Boston University School of Law

Scholarly Commons at Boston University School of Law

Faculty Scholarship

11-30-2022

Comments of the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis

Neil Richards
Cordell Institute for Policy in Medicine & Law

Woodrow Hartzog
Boston University School of Law

Jordan Francis
Cordell Institute for Policy in Medicine & Law

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship

Part of the Consumer Protection Law Commons, and the Internet Law Commons

Recommended Citation

Comments of the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis, Federal Trade Commission Docket No. 2022-0053-1071 (November 30, 2022), https://www.regulations.gov/comment/FTC-2022-0053-1071.

This Regulatory Comment is brought to you for free and open access by Scholarly Commons at Boston University School of Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Scholarly Commons at Boston University School of Law. For more information, please contact lawlessa@bu.edu.

Before the
Federal Trade Commission
Washington, D.C. 20580

In the Matter of		
	)	
Request for Public Comment on the	)	
Prevalence of Commercial Surveillance and	)	Commercial Surveillance
Data Security Practices that Harm Consumers	)	ANPR, R111004

COMMENTS OF THE CORDELL INSTITUTE FOR POLICY IN MEDICINE & LAW AT WASHINGTON UNIVERSITY IN ST. LOUIS

Neil Richards, Faculty Director[*]
Woodrow Hartzog, Fellow[†]
Jordan Francis, Legal Research Fellow[‡]
Cordell Institute for Policy in Medicine & Law[§]
Washington University in St. Louis
One Brookings Drive
Saint Louis, MO 63130

---

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

[‡] The authors would like to thank Patricia Hageman, Cordell Institute Associate Director, and Emily Doster, Cordell Institute Legal Research Fellow, for their significant contributions to these comments.

[§] Founded in 1853, Washington University in St. Louis is an internationally known research university whose mission is to act in service of truth through the formation of leaders, the discovery of knowledge and the treatment of patients for the betterment of our region, our nation and our world. At WashU, we generate, disseminate, and apply knowledge. We foster freedom of inquiry and expression of ideas in our research, teaching and learning. The Cordell Institute is a collaboration between the University's schools of law and medicine, founded to work on legal and other problems at the intersection of law and human information technologies. The Cordell Institute leadership and staff include includes law professors and attorneys who work at the forefront of privacy law, information law, and constitutional civil liberties. Its mission is to advance legal concepts toward a practical policy framework that guides the ethical use of human information to promote health, the protection of individuals, and education of the public. Our scholarship drives policies that reveal how human information can be used appropriately and effectively to build confidence and trust. The opinions offered in these comments are those of the undersigned members of the Cordell Institute in their scholarly capacities, and not necessarily those of Washington University as an institution or those of its constituent schools.

Executive Summary

The Federal Trade Commission—with its broad, independent grant of authority and statutory mandate to identify and prevent unfair and deceptive trade practices—is uniquely situated to prevent and remedy unfair and deceptive data privacy and data security practices. In an increasingly digitized world, data collection, processing, and transfer have become integral to market interactions. Our personal and commercial experiences are now mediated by powerful, information-intensive firms who hold the power to shape what consumers see, how they interact, which options are available to them, and how they make decisions. That power imbalance exposes consumers and leaves them all vulnerable. We all share data concerning ourselves with these platforms, often unwittingly, and we leave ourselves at the risk of their manipulation and control. The Commission envisions "[a] vibrant economy fueled by fair competition and an empowered, informed public."[1] But, this vision cannot be realized in the absence of meaningful consumer trust. Trust is the oxygen necessary for consumer choice to survive. Where trust is present, consumers are empowered to invest in companies and share their data knowing they are not going to be betrayed, manipulated, deceived, or treated unfairly. But where trust is weakened or absent, the marketplace breaks down and becomes a fertile ground for the development of market failures that are contrary to the interests of consumers and competition. Recognizing the importance of trust in digital markets, our comments are organized around three arguments: (i) commercial surveillance is the correct label for the data practices observed in the market; (ii) notice and choice, centered around the fiction of consumer consent, has failed as a regulatory regime; and (iii) the Commission should ground its future data privacy rules in concepts of trust, loyalty, and relational vulnerability.

The harms and benefits of commercial surveillance are wildly imbalanced in favor of commercial actors, with consumers more vulnerable than ever before. This is why we argue in Part I that commercial surveillance is the correct terminology for the practices being observed in digital markets. Humans are increasingly being tracked, identified, classified, and commodified online. This prevalent surveillance borders on the ubiquitous. It manifests in different ways and is driven by different market actors, but its cumulative effect is a corporate surveillance regime which the Commission is correct to label as such. Although commercial surveillance is neither always good nor always bad, some commercial surveillance practices unacceptably harm consumers. They also harm digital markets, namely by eroding trust as consumers increasingly feel betrayed by data practices that contradict their expectations and do not advance their interests. Commercial surveillance also poses significant risks to our mental health, civil rights, and democracy, in contravention of established public policy. Such harms are not outweighed by countervailing benefits to consumers or competition, as the benefits of commercial surveillance disproportionately flow to industry. This is especially true of targeted advertising, where "ad-tech" middlemen pocket the surplus fees generated by targeting and consumers are preyed upon by an advertising leviathan supercharged by prevalent surveillance and behavioral psychology. Industry rakes in profits, giving consumers nothing but risk, dread, and over-hyped, undesired targeted ads.

In Part II we explain why notice and choice has failed to curtail all but the most egregious industry practices. Notice and choice is overwhelming, illusory, and ineffective. Rather than being

[1] FTC STRATEGIC PLAN, *infra* note 7.

empowering, notice and choice has proven overly burdensome on consumers and has legitimized harmful, disloyal commercial surveillance and data security practices. Notice and choice is plagued by cognitive and structural problems which prevent consumers from effectively engaging in privacy self-management. These problems reveal a fundamental problem with notice and choice: rather than giving consumers meaningful choices, notice and choice manufactures consent. True choice means selecting from an array of options knowing that you will be protected from harmful practices no matter which option you choose. Consent is more than merely choosing; it has a moral and legal significance of accepting a certain set of legal arrangements and certain sets of consequences irrevocably. Consent has its place in law, but a number of pathologies which undermine the validity of consent are present in digital market interactions. The increasing prevalence of dark patterns and manipulative design further highlights the failure of notice and choice. Digital environments are entirely constructed, and companies have considerable power to shape user action through the design of their tools and services. Design is being weaponized to undermine consumer choice and nudge consumers into taking actions which are disproportionately beneficial to companies. Notice and choice creates the market incentives which precipitate deceptive and manipulative design. There are situations in which consent can be effective, namely where requests for consent are *infrequent*, the risks to which consumers are being asked to consent are *vivid*, and there are incentives to take each request *seriously*. Meaningful, informed, consent is possible where those conditions hold, but those circumstances are rarely present in digital markets. American privacy must move beyond notice and choice if it is to truly protect the ability of consumers to make voluntary choices and safely interact in markets.

In Part III we explain why the Commission should ground its data privacy rules in concepts of loyalty and relational vulnerability. Modern commercial relationships are uniquely risky for consumers. Modern tech companies are entrenched in our lives and have considerable control over what we see and click, making consumers vulnerable to companies in unprecedented ways. We trust these companies with our data out of necessity, but the law fails to stop them from engaging in self-serving, opportunistic behavior. Not all privacy injuries are caused by disloyal commercial surveillance, but all disloyal commercial surveillance causes substantial injuries. Such practices are the very definition of an unfair trade practice for the digital age, because they leave consumers substantially worse-off, are not reasonably avoidable given consumers' vulnerability, and negate any possible offsetting benefits to consumers or competition by poisoning the marketplace. When companies are free to act in ways disloyal to consumers, they send a message to consumers that they cannot be trusted with people's data and mediated experiences. Instead of healthy competition, companies have strong incentives to generate short-term profits by extracting more data and attention in increasingly harmful ways. Approaching questions of unfairness through the frame of disloyalty and relational vulnerability thus reveals why certain commercial surveillance practices are both unfair and deceptive. Loyalty is what separates harmful commercial surveillance from market intelligence that can benefit everyone. By narrowing the category of commercial surveillance to the subset of those practices which are disloyal, the Commission can craft precise trade regulations which target the most egregious and pressing harms in the marketplace.

These comments identify several trust-preserving rules which the Commission could implement. The first of these is requiring data minimization (or preventing data maximization), which would help bridge the gap between privacy and security. Data minimization is a fundamental element of good data security because unnecessary and disproportionate data

collection worsens the consequences of data breaches and gives fraudsters personal information which can be used to carry out subsequent attacks. Second, the Commission should prohibit the practice of providing third-party access to consumer data when that access elevates the self-interest of the company over that of the consumers, a practice we term as "disloyal gatekeeping." This prohibition would still allow for beneficial third-party access, such as contextual advertising. Third, the Commission should place substantive limits on targeted advertising. This would remove the market incentives that drive disloyal and exploitative commercial surveillance while still preserving the incentives for loyal commercial surveillance, such as personalization and product improvement. Contextual advertising remains a viable alternative that can fuel a free, open internet without relying on corrosive and disloyal surveillance-based targeting. Fourth, the Commission should heed the advice of experts and develop rules regarding the design, implementation, and use of AI systems that are grounded in concepts of loyalty and relational vulnerability. With mounting evidence that these systems create discriminatory outcomes, companies' increased reliance on automated decision-making systems raises grave concerns about their transparency, fairness, and accountability. These opaque systems diminish consumer trust, to the detriment of consumers, companies, and competition. Finally, we argue that the Commission should not see this rulemaking as a binary choice between protecting either (a) children and teens or (b) adults. The Commission's focus on protecting children is laudable, but many of the reasons given for protecting children apply to adults as well. Age is a spectrum, as is the wisdom and maturity that comes with it. Rules and safeguards which follow arbitrary age distinctions can leave gaps in protection. Digital markets are plagued by drastic information asymmetry and power differentials. As demonstrated by the failure of notice and choice and privacy self-management, the same kinds of information asymmetries and overconfidence that are ascribed to children and teenagers frequently apply to adults as well. Thus, rather than promulgating specific data privacy rules for children and teenagers, we believe that the Commission should focus on crafting generally applicable trade regulations which will protect all Americans from harmful commercial surveillance.

We have previously written that "the corporate, commercial, mobile app-driven internet of the early 2020s represents probably the most highly surveilled environment in the history of humanity."[2] Such prevalent surveillance creates individual and social harms, disproportionately benefits certain industry actors, and erodes trust in the market. The commercial surveillance industry may have flourished under a notice and choice regime which serves only the interests of the data hungry companies who hold considerable power of basic aspects of our lives, but human consumers have not. Nothing about this status quo is inevitable, and the Commission is right to ask questions about how these practices affect us and what can be done to mitigate the harms of disloyal commercial surveillance. Substantive limits on commercial surveillance which are nuanced, narrowly tailored, and elevate consumer wellbeing will not irreparably damage the internet or spell the end of the advertising industry. To the contrary, the Commission has an opportunity to pass substantive rules which benefit consumers and companies by fostering trust and enabling human flourishing. We applaud the Commission for its thoughtful approach to these questions of critical importance for the future of our economy, our society, and our democracy.

---

[2] RICHARDS, *infra* note 21, at 83; *see also* Khan, *infra* note 455 (citing RICHARDS, *supra*).

Table of Contents

Executive Summary 1
Introduction 6
I. The Disproportionate Dangers and Meager Consumer Benefits of Commercial Surveillance. 10
A. Commercial Surveillance is the Correct Term for the Data Practices Observed in Digital Markets 10
B. Commercial Surveillance is Prevalent 14
1. Collection 15
2. Personalization 19
3. Gatekeeping 20
4. Influencing 21
5. Mediation 22
C. Commercial Surveillance Causes Substantial Injury to Consumers and Society 23
1. Commercial Surveillance Inflicts Substantial Injuries on Consumers Which Prevent Them from Safely Participating in Markets 24
2. Commercial Surveillance Inflicts Substantial Injuries on Our Mental Health, Civil Rights, and Democracy in Contravention of Established Public Policy 34
D. The Benefits of Commercial Surveillance Disproportionately Flow to Industry 41
1. The Substantial Injuries Inflicted by Targeted Advertising Are Not Outweighed by Countervailing Benefits to Consumers or Competition 42
II. Notice and Choice Has Failed 47
A. Privacy Self-Management Has Proven Ineffective, Untenable, and Undesirable 49
B. Several Well-Known Pathologies Thwart Effective Consent to Commercial Surveillance 51
C. Manipulative Interface Design and Dark Patterns Are Pervasive Barriers to Effective Consent 53
D. Consent Can Be Effective Only in Select Circumstances, None of Which Are Present in Most Digital Transactions 57
III. Fostering Trust in Digital Marketplaces 59
A. Modern Commercial Relationships are Uniquely Risky for Consumers 60
B. Commercial Data Disloyalty as an Unfair Trade Practice 65
1. Concepts of Loyalty and Relational Vulnerability Are Consonant with Section 5 66
2. Loyalty Solves the Consent Dilemma and Has the Added Virtue of Flexibility 68

C. The Commission Should Use Its Rulemaking Authority to Ban Particularly Harmful Unfair Trade Practices That Have the Hallmark of Disloyalty 69

1. Data Minimization Is a Fundamental Element of Good Data Security 70

2. Loyal Gatekeeping Can Curtail Data Broker Access to Consumer Information 72

3. Targeted, Behavioral, and Cross-Contextual Advertising Should Be Limited 73

4. Fairness, Transparency, and Accountability Are Necessary to Combat Due Process Harms of Automated Decision-Making 75

5. Data Privacy Rules Should Protect Children, Teenagers, and Adults 76

Conclusion 79

Appendix 81

Introduction

As the only agency at the national level with a broad consumer protection law enforcement mandate,[3] the Federal Trade Commission was created to prevent unfair and deceptive trade practices, both in enforcement actions and by promulgating trade regulation rules.[4] For nearly three decades the Commission has been the *de facto* data privacy and data security federal regulator in the United States, creating an impressive body of enforcement actions akin to a body of common law.[5] In an increasingly digitized world, the collection, use, and dissemination of data has become integral to consumer experiences in the marketplace. Our personal and commercial experiences are mediated by powerful, information-intensive firms. These firms are endowed with the power to shape what consumers see and can click on.[6] They also determine just how exposed consumers are when using a service. That power imbalance makes consumers vulnerable. We share data concerning ourselves with these platforms, often unwittingly, and we leave ourselves at the risk of their manipulation and control. The Commission envisions "[a] vibrant economy fueled by fair competition and an empowered, informed public."[7] Trust is a critical component of that vision. Where trust is present, consumers are empowered to invest in companies and share their data knowing they are not going to be betrayed, manipulated, deceived, or treated unfairly.[8] This in turn would allow consumers to engage in responsible innovation in the development of new products and services in the interests of both consumers and competition. Unfortunately, that is not the world we have.[9] Without trust, the marketplace breaks down and becomes a fertile ground for the development of market failures that are contrary to the interests of consumers and competition. The public, tired of being betrayed and commodified, deserve rules that compel loyal behavior and put their interests first.[10] If consumers cannot trust the companies they deal with, they cannot meaningfully participate in the marketplace. In such a world, consumers, companies, and competition are all worse off in the long run. The Commission's vision to protect consumers and promote healthy competition thus cannot be achieved in the absence of substantive rules which foster trust by curtailing disloyal data practices.

---

[3] Public Statement, Roscoe B. Starek, III, Protecting the Consumer in the Global Marketplace (June 25, 1997), https://www.ftc.gov/news-events/news/speeches/protecting-consumer-global-marketplace.

[4] *See* Guziak v. FTC, 361 F.2d 700, 703–04 (8th Cir. 1966) ("There appears to be no basis in terms of either history or logic for holding that the Commission may not assert its power until the interstate activity under scrutiny has reached a certain magnitude. In fact, one of the objects of the Federal Trade Commission Act was to prevent potential injury by stopping unfair methods of competition in their incipiency." (citing FTC v. Raladam Co., 316 U.S. 149 (1942); Fashion Originators' Guild of Am. v. FTC, 312 U.S. 457, 466 (1941))).

[5] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

[6] *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018).

[7] FED. TRADE COMM'N, STRATEGIC PLAN FOR FISCAL YEARS 2022 TO 2026 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/fy-2022-2026-ftc-strategic-plan.pdf [hereinafter FTC STRATEGIC PLAN].

[8] *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016).

[9] *See infra* Part I.B.

[10] Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L. J. 985, 1033 (2022).

The time is right for this rulemaking. Industry has repeatedly asked for guidance on what constitutes unfair data practices and data security measures. Consumers likewise need privacy and data security protections now. Every day that passes without substantive rules limiting injurious commercial surveillance and lax data security practices further harms consumers and stifles commerce by leaving companies guessing as to their legal obligations. Although an omnibus federal privacy law might be a useful supplement to or even preferable to agency rulemaking, the Commission should not let this process be deterred by the mere possibility of Congressional action. The FTC has a broad grant of independent bipartisan authority and after all, "Congress envisioned the FTC to *prevent* unfair and deceptive practices."[11] An "unfair trade practice" is a capacious term of art in American law that Congress preferred to a finite, specific, and enumerated list of unfair activities, in large part because substantive unfairness is itself a large category limited only by the ingenuity of unscrupulous merchants.[12] Its flexibility has allowed the Commission to protect consumers from industrial practices in the time of the First World War through to algorithmic decisionmaking in the present. Yet the flexibility of the "unfair trade practices" standard can be buttressed by specificity through this rulemaking. Moreover, it is highly likely (and desirable) that the Commission will engage in rulemaking under a future federal privacy statute. Any progress on rulemaking today will inform both the Commission's present enforcement actions and any future rulemaking strategy. (Q25.)

Congress and the FTC have jointly developed the meaning of unfairness over time, largely through amending the FTC Act and the investigations and cases brought by the FTC and state attorneys general. The Commission should pursue rulemaking tenaciously because it is limited in the ways it can continue to develop the concept of unfairness through complaints and consent orders. The Commission's own enforcement actions show that harmful data practices are prevalent and that these data practices jeopardize our privacy and the security of our data. Limited action on the part of the agency gives oxygen to these harmful practices which are undermining consumer trust. For that reason, although the Commission's case-by-case enforcement strategy has helped and continues to help protect consumers in the marketplace, it is increasingly clear that trade regulation rules are necessary. Clear and substantive rules would go a long way in curtailing the kinds of unfettered data abuses witnessed in the marketplace. Section 18 rulemaking (otherwise known as "Mag-Moss" rulemaking) has the virtue of being "open, iterative, and public."[13] In contrast to a pure enforcement regime, which provides little opportunity for stakeholders to intervene in agency actions,

> proceeding by rulemaking strengthens the democratic legitimacy of agency action by providing greater opportunities for input by regulated parties and regulatory beneficiaries. Public engagement is especially important given Congress's intent

[11] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION: PRIVACY LAW AND POLICY 331 (2016).
[12] *See generally id.*
[13] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273, 51,289 (proposed Aug. 22, 2022) (Statement of Commissioner Rebecca Kelly Slaughter).

> for the agency to update its conceptions of unfairness and deception regularly to keep pace with evolving abuses in the marketplace.[14]

Section 18 rulemaking is further imbued with pro-democratic features such as increased opportunity for public comments and an opportunity to initiate public hearings.[15] By endowing the Commission with this robust rulemaking authority, Congress clearly envisioned the kind of public-led inquiry at hand in this rulemaking. The Commission is asking questions about matters within its expertise, and the public is responding in kind.

These comments are organized around three arguments. The first argument is that the harms and benefits of commercial surveillance are wildly imbalanced in favor of commercial actors, with consumers more vulnerable than ever. This is why we argue that commercial surveillance is the correct terminology for the practices which are being observed in digital markets. Humans are increasingly being tracked, identified, classified, assessed, and commodified online. This prevalent surveillance manifests itself in different ways and is driven by different market actors, but the cumulative effect is a corporate *commercial surveillance* regime which the Commission is correct to label as it has. Commercial surveillance harms consumers and digital markets by eroding trust in those markets as consumers increasingly feel betrayed by data practices that contradict their expectations. These harms are not outweighed by any countervailing benefits to consumers or competition, as the benefits of commercial surveillance disproportionately flow to industry. This is especially true of targeted advertising, where ad-tech middlemen pocket the surplus fees generated by targeting and consumers are preyed upon by an advertising leviathan supercharged by prevalent surveillance and behavioral psychology. Industry rakes in profits, giving consumers nothing but risk, dread, and overhyped undesired targeted ads.

The second central argument of these comments is that notice and choice has failed. Rather than empowering consumers as intended, notice and choice has proven overly burdensome on consumers and has legitimized harmful, disloyal commercial surveillance and data security practices. As such, it has had the opposite effect from the one it was intended to have. There are numerous reasons why notice and choice is ill-suited to promoting good data practices. Notice and choice is plagued by cognitive and structural problems which prevent consumers from effectively engaging in privacy self-management. Consent has its place in American law, but a number of pathologies which undermine the validity of consent are present in digital market interactions. Digital environments are entirely constructed, and corporate design choices undermine consumer choice and nudge consumers into taking actions which are disproportionately beneficial to companies. There are a few situations in which consent can be meaningful and effective, but those circumstances are rarely present in digital markets. American privacy must move beyond notice and choice if it is to truly protect the ability of consumers to make voluntary choices and safely interact in markets.

---

[14] Kurt Walters, *Reassessing the Mythology of Magnuson-Moss: A Call to Revive Section 18 Rulemaking at the FTC*, 16 HARV. L. & POL'Y REV. 520, 526 (2022).

[15] *See* Walters, *supra* note 14,14 at 25–28, discussing the role of informal hearings in Section 18 rulemaking.

Our third argument points toward a solution: to properly deter unfair trade practices, the Commission should ground its data privacy rules in concepts of loyalty and relational vulnerability. Participation in modern society requires consumers to make themselves vulnerable to companies. Modern tech companies are entrenched in our lives and have considerable control over what we see and click.[16] We trust these companies with our data out of necessity, but the law fails to stop them from engaging in self-serving, opportunistic behavior. Such practices are the very definition of an unfair trade practice for the digital age because they leave consumers worse-off, they are not reasonably avoidable given consumers' vulnerability, and they negate any possible offsetting benefits to consumers or competition by poisoning the marketplace. When companies are free to act in ways disloyal to consumers, they send a message to consumers that they cannot be trusted with people's data and mediated experiences. Consumers struggle to differentiate between those companies who have loyal data practices and those who do not, which further bolsters companies engaged in disloyal practices. Instead of healthy competition, companies have every incentive to compete to extract more data and attention in increasingly harmful ways.

Approaching questions of unfairness through the frame of disloyalty and relational vulnerability reveals why certain commercial surveillance practices are both unfair and deceptive. Loyalty is what separates harmful and beneficial commercial surveillance. By narrowing the category of commercial surveillance to the subset of those practices which are disloyal, the Commission can craft precise trade regulations which target the most egregious and pressing harms in the marketplace. Through this focused approach, the Commission can work towards its goal of "[a] vibrant economy fueled by fair competition and an empowered, informed public."[17] We identify several actions the Commission can take to help foster trust in digital markets: (1) requiring *data minimization* by prohibiting companies from engaging in unnecessary and disproportionate data *collection*; (2) prohibiting disloyal *gatekeeping* by prohibiting third-party access to consumer data where that access is not in the consumer's best interest; (3) placing *substantive limits* on targeted, behavioral, and cross-contextual advertising; (4) heeding the advice of AI experts and developing rules regarding the design, implementation, and use of AI systems which increase the *fairness, transparency, and accountability* of these systems; and (5) rather than seeing this rulemaking as a binary choice between protecting children and teens or adults, crafting *generally applicable trade regulations which protect all Americans* from harmful commercial surveillance. (Q30.)

---

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

[17] FED. TRADE COMM'N, STRATEGIC PLAN FOR FISCAL YEARS 2022 TO 2026 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/fy-2022-2026-ftc-strategic-plan.pdf.

I. The Disproportionate Dangers and Meager Consumer Benefits of Commercial Surveillance

A. Commercial Surveillance is the Correct Term for the Data Practices Observed in Digital Markets

To "define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce,"[18] the Commission rightly seeks to use accurate and clear language. "Commercial surveillance" is the correct term to use in this rulemaking because it accurately describes the context in which these practices occur, the prevalence of these practices, the limited visibility of these practices to consumers, and the power disparities that exist between consumers and companies engaging in such commercial surveillance. The Commission's expanded definition of commercial surveillance in the ANPR captures these factors:

> For the purposes of this ANPR, "commercial surveillance" refers to the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information. These data include both information that consumers actively provide—say, when they affirmatively register for a service or make a purchase—as well as personal identifiers and other information that companies collect, for example, when a consumer casually browses the web or opens an app.[19]

This definition clarifies that the Commission is concerned with acts or practices affecting consumer data and that such practices encompass both overt and covert data collection. Concerns that the term is presumptive or value-laden are misplaced, as these comment demonstrate that some kinds of commercial surveillance can be mutually beneficial for consumers and businesses when used in line with consumer expectations and in a way that fosters trust.[20] Commercial surveillance is not always bad, but it is the right term for what is going on here.

The use of the term "surveillance" captures the prevalence of these practices and their invisibility to consumers. Surveillance is a word that can cause unease, conjuring mental images of Orwell's Big Brother and totalitarian societies.[21] Notwithstanding those associations, surveillance is a complex subject that is neither always good nor always bad.[22] Sociologist David Lyon has defined surveillance as "the focused, systemic and routine attention to personal details for purposes of influence, management, protection or direction."[23] Building on this definition, we[24] have previously written:

---

[18] 15 U.S.C. § 57a(a)(1)(B) (2018).
[19] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273, 51,277 (proposed Aug. 22, 2022) (advance notice of proposed rulemaking and request for public comment).
[20] *Infra* Part III.
[21] NEIL RICHARDS, WHY PRIVACY MATTERS 136–137 (2022).
[22] *Id.* at 138.
[23] *Id.* (citing DAVID LYON, SURVEILLANCE STUDIES 18–22 (2007)).
[24] For ease of reading, these comments use the term "we" to refer to the prior writings of any of the authors, whether written jointly or individually.

> Four aspects of this definition are noteworthy, as they expand our understanding of what surveillance is and what its purposes are. First, surveillance is focused on learning information about *individuals*. Second, surveillance is *systematic*, which is to say that it is intentional rather than random or arbitrary. Third, surveillance is *routine*, part of the ordinary administrative apparatus that characterizes modern societies. Fourth, surveillance can have a wide variety of *purposes*—sometimes totalitarian domination, more often subtler forms of influence or control, and sometimes oversight or protection. . . . To Lyon's four features of surveillance, I'd like to add a fifth, which is that surveillance *transcends the public-private divide*. . . . In our world, surveillance is performed by the government, by the private sector, and by a thriving combination of the two.[25]

Viewed through this lens, the Commission's use of the term "surveillance" accurately describes the practices we observe in digital markets and which are under scrutiny in this rulemaking. Commercial surveillance as defined by the Commission focuses on *individual* consumers, which includes human market participants, businesses, and workers.[26] Commercial surveillance is also *systematic*, as consumers are either directly asked to provide information or companies have systems in place which automatically collect personal identifiers and other information concerning consumers. These practices are also *routine*. Prevalent digital tracking methods, such as the use of third-party cookies or cross-device tracking for targeted and behavioral advertising, are commonplace features of the modern internet that are near-ubiquitous. Commercial surveillance also has a wide variety of *purposes*. Some of those purposes further trust and improve the consumer experience, such as the use of cookies to keep a user logged into a portal or when a streaming service provides personalized recommendations. On the other hand, some purposes of commercial surveillance practices are more insidious or outright malicious, such as the use of "stalkerware" to stalk and harass people against their will.[27] Thus, the Commission's own definition of consumer surveillance is precisely the kind of focused, systemic, and routine attention to personal details which the definition of surveillance covers.

Recognizing that surveillance in general *transcends the public-private divide*,[28] the use of the term *commercial* surveillance also demonstrates the Commission's caution and careful use of language to keep the focus of this rulemaking narrow. At issue is the use of human information in

---

[25] RICHARDS, *supra* note 21, at 138.

[26] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273, 51,277 (proposed Aug. 22, 2022) (advance notice of proposed rulemaking and request for public comment).

[27] *Stalkerware: Phone Surveillance & Safety for Survivors*, TECH SAFETY, https://www.techsafety.org/spyware-and-stalkerware-phone-surveillance (last visited Sept. 26, 2022).

[28] *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1958–59 (2013); *see also* BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 64–79 (2015) (describing how we are surveilled by "an amalgam of various national intelligence services, Google, Microsoft, other Silicon Valley firms, Facebook and other social media corporations, private surveillance industry companies and consultants, IT departments everywhere, . . . local police departments, friends, hackers, and curious interlopers").

the flow of commerce, especially as driven by pecuniary interests.[29] As Bruce Schneier has recognized, "[t]he overwhelming bulk of surveillance is corporate."[30] Danielle Citron has written that "[e]very day, all day long, products and services . . . track our bodily functions, health conditions, searches, sexual activities, and correspondence, creating digital archives of our lives at unimaginable scale."[31] This corporate surveillance is ostensibly a bargain between consumers and companies. The incentive for companies is clear: "Companies are maximizing the amount of personal data collected so that they can make money from it. . . . [F]irms amass intimate data to analyze it, share it, and—yes—sell it."[32] Absent any regulations to the contrary, cheap storage costs and plentiful opportunities to monetize consumer data create pressure to engage in rampant collection, storage, and use of our data.[33] The incentive for consumers to not resist this prevalent surveillance is the repeated assurance from tech companies that "they are making our lives better."[34] Companies employ every tactic they can to convince consumers that this arrangement benefits them: "In the astute words of privacy researcher Pinelopi Troullinou, 'seductive surveillance' is the name of the game. Firms tell us that the more they know us, the more they can meet our needs, bring us joy, and simplify our lives."[35] As we discuss below, this is sometimes true and sometimes untrue.[36] Setting aside for now the discussion of which parties benefit from these practices, the Commission is correct in labeling them as *commercial* surveillance.

Another virtue of the term "commercial surveillance" is that it correctly implies the existence and exercise of various forms of power over consumers. As we have written before, "privacy is inevitably about the distribution and exercise of power."[37] Power is key to understanding the significance of commercial surveillance and the ways in which it can substantially injure consumers and competition. Oscar Gandy's discussion of power as a relative measure elucidates this point:

> Randall Bartlett offers a definition of power that may serve us well as we venture into battle with those who would ignore the role that information plays in its use. He defines power as "the ability of one actor to alter the decisions made and/or welfare experienced by another actor relative to the choices that would have been

---

[29] *See generally* Roger McNamee, *A Brief History of How Your Privacy Was Stolen*, N.Y. TIMES (June 3, 2019), https://www.nytimes.com/2019/06/03/opinion/google-facebook-data-privacy.html (detailing the rise of commercial surveillance).
[30] BRUCE SCHNEIER, DATA AND GOLIATH 47 (2015).
[31] DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE 1 (2022).
[32] *Id.* at 1, 5.
[33] *See id.* at 2–3.
[34] *Id.* at 1.
[35] *Id.* at 5 (citing Pinelopi Troullinou, *Exploring the Subjective Experience of Everyday Surveillance: The Case of Smartphone Devices as Means of Facilitating "Seductive Surveillance*," (Dec. 2016) (Ph.D. thesis, Open University), http://oro.open.ac.uk/52613/2/thesis_PT_library_submission.pdf.
[36] *See* Part I.C, discussing the substantial injuries that some commercial surveillance practices inflict upon consumers.
[37] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1737 (2020).

> made and/or welfare that would have been experienced had the first actor not existed or acted." Defined in this way, power is a relative measure. All actors may be seen to have some power. The importance of the question is based in the desire to determine, or to demonstrate . . . that the power of individuals is frequently overwhelmed by the power of bureaucratic organizations. . . . As we explore the political economy of personal information, the relative power of individuals in comparison with that of institutions and organizations becomes highly relevant. . . . [T]he power that the individual is able to exercise over the organization when she withholds personal information is almost always insignificant in comparison with the power brought to bear when the organization chooses to withhold goods or services unless the information is provided.[38]

This intrinsic power inequality is present in the Commission's definition of commercial surveillance, which focuses on actions taken with respect to consumer data, usually by a trusted party, such as collection, aggregation, analysis, retention, transfer, or monetization. This implicit recognition of power inequality tracks the statutory requirements of an unfair trade practice. An act or practice is not unfair "unless the act or practice 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."[39] As Gandy's discussion of power explains, commercial surveillance is perpetuated by companies and is unavoidable by consumers because a consumer's ability to withhold information is insignificant compared to a company's ability to withhold goods or services.

The purpose of this ANPR is to identify only those commercial surveillance practices which are unfair. Although commercial surveillance always involves the exercise or distribution of power, sometimes it can be useful on balance. Similarly, a technology is not necessarily disloyal merely because it benefits its maker.[40] A number of mutually beneficial data practices fall within the Commission's definition of commercial surveillance: When companies mine user data to improve services specifically requested by the user (and share that data with trusted third parties for that purpose), that is a mutually beneficial commercial surveillance practice;[41] digital entertainment services like Netflix, Spotify, etc. utilize data collection and personalization to the benefits of users;[42] and recommendation systems used by companies like Amazon, can benefit users and platforms alike.[43] If all commercial surveillance were presumptively unfair, there would be no need to promulgate an ANPR as comprehensive and nuanced as this. The Commission is trying to identify the small subset of data practices that are *unfair* commercial surveillance under the Section 5 framework. Unscrupulous parties who fear the specter of regulation may decry the use of the term commercial surveillance as being presumptive, but it accurately describes their

---

[38] OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 32–34 (2d ed. 2021) (quoting RANDALL BARTLETT, ECONOMICS AND POWER: AN INQUIRY INTO HUMAN RELATIONS AND MARKETS 30 (1989)).
[39] 15 U.S.C. § 45(n) (2018).
[40] HARTZOG, *supra* note 8, at 106.
[41] *Id.*
[42] *Id.*
[43] *Id.*

practices. This descriptive accuracy is necessary to create clear, effective trade regulation rules. The systematic and routine collection of personal data to influence commercial activity affects the ability of consumers to safely, sustainably, and meaningfully participate in the marketplace. To say the least, the Commission should not shy away from using such accurate language merely because it may cause some companies to engage in uncomfortable introspection about their own business models and their attitudes towards consumer data.

B. Commercial Surveillance is Prevalent

When it comes to privacy and digital commerce, Americans are overwhelmingly aware that they are being surveilled, judged, and nudged constantly by private and public actors. A recent New York Times op-ed recognized that "[t]o exist in 2022 is to be surveilled, tracked, tagged and monitored—most often for profit."[44] But consumers crave—and demand—privacy. According to a recent KPMG survey, ninety-seven percent of respondents said that data privacy is important to them, and eighty-seven percent characterized it as a human right.[45] Despite that clear yearning for greater protections, consumers are not optimistic about the level of protection they receive. That same survey found that: sixty-eight percent of consumers don't trust companies to ethically sell personal data;[46] fifty-four percent don't trust companies to use personal data in an ethical way;[47] fifty-three percent don't trust companies to ethically collect personal data;[48] and fifty-percent don't trust companies to protect personal data.[49] This sense of distrust is prevalent and harmful to digital markets. A 2019 report issued by the Pew Research Center revealed that "roughly six-in-ten U.S. adults say they do not think it is possible to go through daily life *without having data collected about them* by companies or the government."[50] A staggering eighty-one percent of the public "say that the potential risks they face because of data collection by companies outweigh the benefits,"[51] and seventy percent think that their personal data is less secure than it was five years ago.[52] These surveys show just how overwhelmed and powerless consumers feel in the face of commercial surveillance and how much trust has been eroded. And these consumers are correct. The status quo of privacy regulation in America (or lack thereof) has created a commercial surveillance leviathan whose insatiable appetite for data manifests pervasive and harmful surveillance practices. This commercial surveillance "ecosystem" drives product design to create "a monetizable data stream

---

[44] Alex Kingsbury, *We're About to Find Out What Happens When Privacy Is All but Gone*, N.Y. TIMES (Aug. 23, 2022), https://www.nytimes.com/2022/08/23/opinion/apple-internet-privacy-tracking.html.
[45] ORSON LUCAS & STEVEN STEIN, KPMG, THE NEW IMPERATIVE FOR CORPORATE DATA RESPONSIBILITY (2020), https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf.
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. 2 (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf.
[51] *Id.*
[52] *Id.* at 4.

from every buyer,"[53] which in turn erodes trust and hampers the ability of consumers to safely interact in markets.

Jack Balkin concisely summarized the breadth of commercial surveillance when he wrote that "[w]e rely on digital businesses to perform many different tasks for us. In the process, these businesses learn a lot about us—our likes, our dislikes, our habits, our movements, websites we visit, who we communicate with and when we do it, features of our bodies, even how we type on, click, and touch digital interfaces."[54] The prevalence and breadth of commercial surveillance makes it difficult to concisely answer the question, "[w]hich practices do companies use to surveil consumers?" Companies surveil consumers in many different ways, some of which are old and familiar and many of which are novel and have not yet entered the public consciousness. Different companies surveil consumers for different reasons and target different types of data from broad groups of people. For conceptual clarity, we can categorize commercial surveillance practices under the five areas of collection, personalization, gatekeeping, influencing, and mediation.[55] Each of these categories capture different aspects of the relationship between consumers and the companies entrusted with our data, and as we will explain below, each category can point the way towards specific commercial regulations. (Q1, Q3.)

1. Collection

Companies today are creating vast "digital archives" of our lives.[56] Rampant data collection has become a normalized aspect of modern commercial relationships, with new and old technologies being employed in conjunction to "create comprehensive records of our movements through physical space, as well as our interests, likes, desires, needs, and physiological states."[57] Data collection is a core feature of digital commerce. Companies act unfairly when they collect large, unnecessary, sensitive and disproportionate data in ways that inhibit consumers' ability to be safe market participants. There is nothing inevitable or accidental about this.[58] Shoshana Zuboff has explained how commercial surveillance as we know it today (marked by unnecessary and disproportionate data collection) evolved due to market pressures. She recounts how engineers first noticed that interactions with customers produced "data exhaust," significant amounts of information about customer behavior that were a byproduct of normal market interactions. Zuboff further describes how that data was reconceptualized as "behavioral surplus" which could be used to improve the quality of the company's services, benefitting consumers. But crucially, Zuboff

---

[53] Shannon Vallor, *We Used to Get Excited About Technology. What Happened?*, MIT TECH. REV. (Oct. 21, 2022), https://www.technologyreview.com/2022/10/21/1061260/innovation-technology-what-happened.
[54] Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 11 (2020).
[55] *See* Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356, 378–384 (2022) (proposing specific subsidiary rules within information relationships to mitigate these kinds of disloyal behaviors).
[56] CITRON, *supra* note 31,31 at 1.
[57] *See* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 135 (2017).
[58] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 17 (2019) ("Surveillance capitalism is not an accident of overzealous technologists, but rather a rogue capitalism that learned to cunningly exploit its historical conditions to ensure and defends its success."); *see also* McNamee, *supra* note 29.

explains that behavioral surplus had other uses which did not directly benefit the consumers who were generating it, such as monetizing that data to serve targeted advertisements that could be used to influence and manipulate consumer behavior.[59] Comprehensive consumer tracking and data collection thus has significant detrimental effects on consumers and on the trust that is necessary for digital markets to function. Consumers become exposed and vulnerable the moment their data is collected. If that collection is not limited to what is necessary and proportionate to provide the service requested by the consumer, then consumers lose trust and digital commerce as a whole suffers. Moreover, data surreptitiously collected on one set of consumers can be used to influence and manipulate other consumers.[60]

The Commission's definition of commercial surveillance recognizes that data collection includes both information that consumers actively provide (usually at the request of a trusted party) and information that companies collect in ways that are passive or covert to consumers. Often, companies will condition the use of a service or sale of goods on consumers providing personal information. Sometimes that is a practical necessity, such as providing a payment option and shipping address for delivery of goods. Other times, companies present these requests as allegedly voluntary, but they are designed to be so difficult to decline that consumers consent against their desire to do so. Furthermore, there are pervasive information-collecting practices that are invisible to all but the most technology-savvy consumers. Persistent trackers surveil users across the web and compile our browsing history. Third-party cookies have been in use for decades, tracking users across websites, building user profiles, and leveraging that information to provide targeted advertising. Even now, as users find new ways to avoid or circumvent cookies, new persistent tracking methods are being implemented. For more than a decade, devices have been surveilled via digital fingerprinting (also known as device fingerprinting), a process which amasses information about consumer devices, such as IP address, operating system, browser selection, screen resolution, clock settings, font choice, etc., to track an individual computer or device across the web.[61] At the same time, our smartphone apps track our location, contacts, calendar, bookmarks, and search history.[62]

Commercial surveillance and data collection have crept into all aspects of our lives. Schools use AI-empowered tools to scan student social media posts, ostensibly to identify students

---

[59] Richards & Hartzog, *supra* note 16, at 972 (citing ZUBOFF, *supra* note 58,58 at 8, 67–69, 71–75).

[60] *See* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573 (2021) (explaining that "[w]hat makes datafication [—the transformation of information about people into a commodity—] wrong is not (only) that it erodes the capacity for subject self-formation, but instead that it materializes unjust social relations: data relations that enact or amplify social inequality").

[61] Julia Angwin & Jennifer Valentino-DeVries, *Race Is On to 'Fingerprint' Phones, PCs*, WALL ST. J. (Nov. 30, 2010, 11:30 PM), https://www.wsj.com/articles/SB10001424052748704679204575646704100959546.

[62] Kingsbury, *supra* note 44 ("In 2019, Times Opinion investigated the location tracking industry. Whistleblowers gave us a data set that included millions of pings from individual cellphones around daily commutes, churches and mosques, abortion clinics, the Pentagon, even the headquarters of the Central Intelligence Agency. 'If the government ordered Americans to continuously provide such precise, real-time information about themselves, there would be a revolt,' the editorial board wrote." (citing Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html)).

at risk of harming themselves or others, but also to surveil things like student protests.[63] Our cars monitor, log, analyze, and monetize data about our driving habits, including our location history, phone distraction, how quickly we accelerate, how early we apply the brakes, and even our entertainment choices.[64] Employers increasingly monitor their employees, screenshotting the websites they visit, recording their faces and voices, logging keystrokes, tracking their location, and monitoring their calls and texts.[65] Video games collect users' personal information and leverage information asymmetry, design, and known frailties in human cognition to pressure players into microtransactions, such as purchasing "loot boxes."[66] Hungry consumers attempting to simply order a pizza have found themselves being surveilled by session replay tools, software designed to observe and record mouse movement, clicks, and keystrokes so that analysts can monitor consumer behavior and optimize websites.[67] Thousands of "femtech" apps, designed to help users track "menstruation, fertility, pregnancies, menopause, pelvic and uterine health, nursing care, and sexual habits," collect vast amounts of data about their users, including information about "cramps, medications, illnesses, the consistency of their vaginal discharge, sex drive, sexual fulfillment (including whether they orgasmed or not), mood, alcohol use, miscarriages, and use or nonuse of contraception."[68] A new crop of spyware, ominously known as "accountability apps," have cropped up to prevent consumers from viewing "pornographic" images by monitoring everything they see and do and feeding that information to an appointed chaperone, even going so far as to take screenshots and eavesdrop.[69] Virtual reality headsets harvest data about our faces, eye movement, and body language.[70] Smart watches embedded with sensors collect a trove of information about our bodies, including whether someone is ovulating.[71]

---

[63] Ari Sen & Derêka K. Bennett, *Tracked: How Colleges Use AI to Monitor Student Protests*, DALLAS NEWS (Sept. 20, 2022), https://interactives.dallasnews.com/2022/social-sentinel.

[64] Jack Morse, *Your Car Knowns Too Much About You. That Could Be a Privacy Nightmare.*, MASHABLE (Sept. 18, 2021), https://mashable.com/article/privacy-please-what-data-do-modern-cars-collect.

[65] Irina Ivanova, *Workplace Spying Surged in the Pandemic. Now the Government Plans to Crack Down.*, CBS NEWS (Nov. 1, 2022, 10:30 AM), https://www.cbsnews.com/news/labor-board-official-takes-aim-at-workplace-spying.

[66] Daniel L. King & Paul H. Delfabbro, *Predatory Monetization Schemes In Video Games (e.g. 'Loot Boxes') and Internet Gaming Disorder*, 113 ADDICTION 1967, 1967–68 (2018); *see also* Tom Gerken, *Report Blasts "Manipulative" Video Game Loot Boxes*, BBC (May 31, 2022), https://www.bbc.com/news/technology-61594815. The problem of loot boxes is particularly bad for child consumers. Vic Hood, *Are Loot Boxes Harmful to Your Kids? Yes, Says Children's Organization*, TECH RADAR (Oct. 22, 2019), https://www.techradar.com/news/are-loot-boxes-harmful-to-your-kids-yes-says-childrens-organization (citing CHILDREN'S COMM'R FOR ENGLAND, GAMING THE SYSTEM (OCT. 2019), https://www.childrenscommissioner.gov.uk/wp-content/uploads/2019/10/CCO-Gaming-the-System-2019.pdf).

[67] *See, e.g.*, Brandon Vigliarolo, *Papa John's Sued for 'Wiretap' Spying on Website Mouse Clicks, Keystrokes*, REGISTER (Oct. 6, 2022, 8:20 PM), https://www.theregister.com/2022/10/06/papa_johns_spying_lawsuit.

[68] CITRON, *supra* note 31,31 at 14.

[69] Dhruv Mehrotra, *The Ungodly Surveillance of Anti-Porn 'Shameware' Apps*, WIRED (Sept. 22, 2022, 1:00 PM), https://www.wired.com/story/covenant-eyes-anti-porn-accountability-monitoring-apps.

[70] Khari Johnson, *Meta's VR Headset Harvests Personal Data Right Off Your Face*, WIRED (Oct. 13, 2022), https://www.wired.com/story/metas-vr-headset-quest-pro-personal-data-face.

[71] *See, e.g.*, Justin Sherman, Apple Is Using Its Reputation for Protecting Privacy to Invade Your Privacy, SLATE: FUTURE TENSE (Sept. 23, 2022, 8:00 AM), https://slate.com/technology/2022/09/apple-privacy-fertility-tracking-

One major sports team—with financial ties to a nation state[72]—has even developed a "smart scarf," which uses "a PPG sensor, accelerometer, temperature sensor, and an electrodermal activity (EDA) sensor" to track a fan's physiological reactions during games.[73] The increasing presence of interconnected, sensor-enabled, networked devices, known as the "Internet of Things" (IoT), exacerbates this surveillance and data harvesting. These devices "are always on, are always with us and, together, ensure the total surveillance of everyday movements, habits, and intellectual endeavors."[74] (Q1, Q3.)

Many of these collection practices are facilitated by dominant platforms and other well-known actors in the surveillance ecosystem. These companies are not solely responsible for the rise of commercial surveillance, but an inventory of prevalent data collection practices would be incomplete without at least analyzing the role of these companies in furthering the prevalence of commercial surveillance.[75] Meta Platforms, Inc. reportedly gathers, loses[76], and leaks[77] vast amounts of data about consumers, whether they are on Facebook or not.[78] Through its panoply of devices, apps, online services, and website analytics, Google now collects vast troves of personal data, including location information, search history, browsing history, contact information, user IDs, device IDs, usage data, crash and performance data, user content, purchase history, email

---

roe.html (discussing Apple Watch's new ovulation tracking feature, which has the potential to expose people to criminal risk post *Roe v. Wade*).

[72] *See Documents Reveal How Abu Dhabi Fund Manchester City*, MARCA (Apr. 7, 2022, 3:09 PM), https://www.marca.com/en/football/manchester-city/2022/04/07/624f3c69e2704ed0818b45f6.html

[73] Victoria Song, *Manchester City is Making a Smart Scarf*, VERGE (July 27, 2022), https://www.theverge.com/2022/7/27/23280629/manchester-city-smart-scarf-wearables.

[74] BRIDGES, *supra* note 57,57 at 135 (citing Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent*, 93 TEX. L. REV. 85, 85–167 (2014)). Examples of IoT devices include "wearable health and fitness sensors; high-tech baby monitors that can be affixed to infants to track their sleeping habits, and breathing patterns, and heart rates; and 'smart' appliances in homes that can detect residents' daily patterns." BRIDGES, *supra*, at 135.

[75] *See* ZUBOFF, *supra* note 58, at 24 ("My focus in these pages tends toward Google, Facebook, and Microsoft. The aim here is not a comprehensive critique of these companies as such. Instead, I view them as the petri dishes in which the DNA of surveillance capitalism is best examined.").

[76] According to leaked documents, Facebook employees do not understand where much data goes once it enters the company's systems. Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does with Your Data, Or Where It Goes: Leaked Document*, VICE (Apr. 26, 2022, 8:02 AM), https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

[77] *See* Complaint, *In re* Cambridge Analytica, LLC, No. 9383 (July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3107_cambridge_analytica_administrative_complaint_7-24-19.pdf (describing Facebook's role in facilitating Cambridge Analytica's access to user data); Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook (announcing a $5B penalty against Facebook for violating a 2012 FTC order, in part for tactics which "allowed the company to share users' personal information with third-party apps that were downloaded by the user's Facebook 'friends.'").

[78] Kate O'Flaherty, *All the Ways Facebook Tracks You and How to Stop It*, FORBES (May 8, 2021), https://www.forbes.com/sites/kateoflahertyuk/2021/05/08/all-the-ways-facebook-tracks-you-and-how-to-stop-it/?sh=6ebb5dbe5583; RICHARDS, *supra* note 21,21 at 84–85 (describing how Facebook intentionally shifted norms and expectations surrounding privacy through design choice and business strategy).

address, text message content, email content, audio data, product interaction, and so on.[79] Such data is collected across services and devices for different purposes, such as advertising, marketing, analytics, personalization, and functionality.[80] Amazon dominates the smart home market, surveilling consumers through a diverse array of devices including speakers, lightbulbs, refrigerators, thermostats, doorbells, televisions, and so on.[81] Amazon recently released its Halo Rise sleep tracker which senses breathing and movement during sleep.[82] In a move seemingly designed to normalize the pervasive surveillance from which it profits, Amazon recently launched a television show featuring footage recorded on the company's Ring doorbells.[83] These devices listen to us in our most intimate moments, comprehensively track our habits, and map our homes.[84] There are increasingly fewer places where consumers can be shielded from the prying eyes and ears of commercial surveillance, and few if any reasonable steps that they can take to avoid such pervasive commercial surveillance.

2. Personalization

Personalization, the routine and systemic treatment of people differently based on personal information or characteristics, is often exalted as a key feature of the modern internet.[85] Personalization embodies several aspects of commercial surveillance, including collection, aggregation, analysis, retention, transfer, and monetization. Some forms of personalization are relatively obvious to consumers, like first-party product advertisements, streaming recommendations, and algorithmically-curated news feeds.[86] Personalization also happens in ways

---

[79] Matt Burgess, *All The Data Google's Apps Collect About You and How To Stop It*, WIRED (Apr. 5, 2021, 6:00 AM), https://www.wired.co.uk/article/google-app-gmail-chrome-data.

[80] *Id.* Google recently entered into a $391.5 million settlement with 40 state attorneys general. The case concerned Google's allegedly misleading location data settings. Bobby Allyn, *Google Pays Nearly $392 Million to Settle Sweeping Location-Tracking Case*, NPR (Nov. 14, 2022, 2:55 PM), https://www.npr.org/2022/11/14/1136521305/google-settlement-location-tracking-data-privacy.

[81] Katie Schoolov, *Amazon Dominates the $113 Billion Smart Home Market—Here's How It Uses the Data It Collects*, CBNC: TECH (Sept. 28, 2022, 1:23 PM), https://www.cnbc.com/2022/09/28/amazon-dominates-the-smart-home-now-privacy-groups-oppose-irobot-deal.html; *see generally* Chris Gilliard, *The Rise of 'Luxury Surveillance,'* ATLANTIC (Oct. 18, 2022, 7:00 AM), https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772 (describing how Amazon's suite of "ambient intelligence" tech products typify a category of "luxury surveillance" goods which normalize and exacerbate methods of surveillance which historically disproportionately harm Black communities).

[82] Schoolov, *supra* note 8181. Google's upcoming new phone, the Pixel 7, will have a similar feature which detects coughing and snoring. Ivan Mehta, *The Pixel 7 Will Have a Snoring and Coughing Detection Feature*, TECH CRUNCH (Oct. 6, 2022, 10:52 AM), https://techcrunch.com/2022/10/06/the-pixel-7-will-have-a-snoring-and-coughing-detection-feature.

[83] *See* Catherine Thorbecke, *Why 'Ring Nation' May Be the Most Dystopian Show on TV*, CNN: BUS. (Oct. 1, 2022, 8:27 AM), https://www.cnn.com/2022/10/01/tech/amazon-ring-nation-backlash (describing how *Ring Nation* controversially recasts surveillance as entertainment).

[84] Grant Clauser, *Amazon's Alexa Never Stops Listening to You. Should You Worry?*, N.Y. TIMES: WIRECUTTER (Aug. 8, 2019), https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you; Jennifer Pattison Tuohy, *Amazon Bought iRobot to See Inside Your Home*, VERGE (Aug. 5, 2022, 12:08 PM), https://www.theverge.com/23293687/amazon-irobot-acquisition-purchase-smarthome-intelligence-privacy-analysis.

[85] Hartzog & Richards, *supra* note 55, at 380.

[86] *See id.*

that are less obvious to consumers, like default settings and layouts.[87] There are positive, loyal examples of personalization, such as "targeted recommendations for networked connections based upon intentionally revealed data such as where you work or attended high school."[88] Personalization systems also create harm, however, "such as those that wrongfully discriminate or have a disparate impact on protected, marginalized, or vulnerable groups of people."[89] "Personalization" of this sort becomes little more than a euphemism for invidious *discrimination*.

Some practices—masquerading as personalization—are corrosive forms of targeting that "unreasonably exclude people from opportunities, extract their attention and financial resources, and expose them to misinformation."[90] Privacy laws enacted at the state level recognize the potential for this corrosive targeting and have implemented bans on data selling, data sharing, and targeted advertising. For example, California's CCPA grants consumers the right to opt out of cross-context behavioral advertising, which is defined as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."[91] Trade regulation rules prohibiting unfair commercial surveillance practices will thus need to distinguish between beneficial and injurious forms of personalization. (Q1, Q3.)

3. Gatekeeping

The nature of digital markets results in third parties having considerable access to consumer data. Trusted parties who are directly interacting with consumers have "a remarkable ability to facilitate third party access to trusting parties and their data."[92] This happens through "APIs, advertiser portals, fusion centers, and government backdoors."[93] This is a significant source of power for major platforms, and where much of the economic incentive to engage in surveillance comes from. For example, advertisers clamor for user data to deliver targeted advertisements,[94] while AI developers want large data sets for training their latest AI models.[95] These third-party desires, coupled with a duty of profit maximization owed to shareholders, create extreme financial pressures on companies to enable access to consumer data. Third-party access to consumer data can be beneficial and loyal. For example, companies might provide anonymous customer data to an analytics firm for the purpose of improving product quality or to a security firm for increasing security. But third-party access is frequently detrimental, such as when consumer data is sold to scammers who then target a company's users or when a company facilitates a data breach by failing

---

[87] *See id.*
[88] *See id.*
[89] *Id.*
[90] Richards & Hartzog, *supra* note 16,16 at 983.
[91] CAL. CIV. CODE § 1798.140(k) (West 2022) (effective Jan. 1, 2023); s*ee also* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 204(c) (2022) (proposing a right for consumers to opt out of targeted advertising).
[92] Hartzog & Richards, *supra* note 55, at 380.
[93] *Id.*
[94] *Id.*
[95] *Id.*

to properly vet the security practices of its vendors. One prominent example which highlights the importance of gatekeeping is the Facebook-Cambridge Analytica scandal, in which third-party apps on Facebook enabled data analytics company Cambridge Analytica to extract massive amounts of data from tens of millions of Facebook's human customers.[96] Reasonable minds can debate the semantics of whether or not this was a "data breach," but the underlying concern from a consumer perspective is more or less the same: consumers trusted Facebook with their data and that trust was betrayed when Facebook failed to safeguard that data from being extracted and leveraged against consumers in an attempt to manipulate them politically. (Q1, Q3.)

4. Influencing

Influencing is both a goal and an unavoidable consequence of commercial surveillance. Every design choice exerts some degree of influence over consumer behavior. We have written before that

> [t]echnologies are artifacts built to act upon the world. Every single design decision made in the creation of a website or app is meant to facilitate a particular kind of behavior. The structure of digital technologies will affect people's choices even if the effect is not intended by designers. When designers create a drop-down menu, privacy settings, "I agree" buttons, and any other feature that implicates people's privacy, they are influencing them. They can't avoid it.[97]

Intentional and unintentional influencing manifests itself in several ways. As discussed above, all design influences to a degree, but many design choices are innocuous. Of greater concern to the Commission are the manipulative and harmful intentional attempts to influence. For example, consumers are frequently unwitting test subjects in experiments designed by companies to increase engagement and, hence, influence, usually in the form of A/B testing.[98] Unlike test subjects in medical or scientific research by universities, however, these unwitting test subjects have few, if any protections, like Institutional Review Boards and other safeguards for human subjects research. These experiments highlight not only the prevalence of surveillance, but also the inability of consumers to avoid it, as well as the harmful consequences that can arise from such power imbalances.[99]

One of the most prevalent and visible ways in which commercial surveillance manifests as influencing is the set of practices which comprise targeted, behavioral, and cross-contextual advertising. Targeted advertising, which has been defined in one instance as "displaying to an individual or device identified by a unique identifier an online advertisement or content that is selected based on known or predicted preferences, characteristics, or interest associated with the

---

[96] DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 143–46 (2022); *see also supra* note 7777 and accompanying text.
[97] *Id.* at 381; *see also* HARTZOG, *supra* note 840.
[98] Natasha Singer, *LinkedIn Ran Social Experiments on 20 Million Users Over Five Years*, N.Y. TIMES (Sept. 25, 2022), https://www.nytimes.com/2022/09/24/business/linkedin-social-experiments.html (describing LinkedIn's practice of using A/B testing on users over a five year period).
[99] *Id.*

individual or a device identified by a unique identifier,"[100] is little more than a sophisticated attempt to influence consumers. Targeted advertising involves many actors, including consumers, publishers, advertisers, and ad-tech middlemen. It also embodies many aspects of commercial surveillance: It is fueled by data collection, facilitated by gatekeeping, and results in personalization. Contextual advertising, an alternative to targeted advertising in which "an advertisement is displayed based on the content or location in which the advertisement appears and does not vary based on who is viewing the advertisement,"[101] is also an attempt to influence but one which relies far less on commercial surveillance. The important distinction between these practices is the degree of risk they entail for consumers and whether they advance consumers' interests. (Q1, Q3.)

We challenge many of the assumptions underlying the proliferation of targeted advertising in Part I.D of these comments, but it is helpful at this stage to use the lens of influencing to introduce the basic set of assumptions which drives this practice. The logic of targeted advertising, as presented to consumers, is that consumers see only ads which are "relevant"[102] to them, which ostensibly enhances their online experience as an unmitigated good. The logic to advertisers is that this form of targeting is more likely than alternatives, such as contextual advertising, to result in purchases – i.e., a change in human behavior caused by the power of prevalent corporate surveillance.[103] This raises important questions about autonomy, manipulation, potential discrimination, democracy, etc., which we address later in these comments, but it is sufficient to note at this stage that the purpose of targeted advertising is to influence consumers-an exercise of power enabled by the detailed information that commercial surveillance generates.

5. Mediation

Digital environments are necessarily and intentionally *constructed*: The creators of such environments decide how and within what parameters human users will interact with one another. This fact implicates consumer privacy and autonomy in significant and serious ways. For example, in response to partisan accusations of censorship and bias, Google recently launched a pilot program with the goal of preventing political campaign emails from going to users' spam folders.[104] Consumers expect their spam filter settings to empower them to make choices about who communicates with them, what kind of emails land in their inbox, and which are directed to spam. Despite those consumer expectations, Google is ultimately in control of mediation, and it facilitates and hinders user behavior through the design of its tools. Another example is the way

---

[100] American Data Privacy and Protection Act, H.R. 8152, 117th Congress § 30 (2022).
[101] *Id.* ("which is when an advertisement is displayed based on the content or location in which the advertisement appears and does not vary based on who is viewing the advertisement").
[102] Yan Lau, *Economic Issues: A Brief Primer on the Economics of Targeted Advertising*, BUREAU OF ECONOMICS FEDERAL TRADE COMMISSION 3-6 (Jan. 2020), https://www.ftc.gov/system/files/documents/reports/brief-primer-economics-targeted-advertising/economic_issues_paper_-_economics_of_targeted_advertising.pdf.
[103] *Id*.
[104] Ashley Gold, Exclusive: *Gmail Launches Pilot to Keep Campaign Emails out Of Spam*, AXIOS (Sept. 19, 2022), https://www.axios.com/2022/09/19/gmail-pilot-campaign-email-spam.

social media platforms, such as Facebook, algorithmically amplify or diminish certain content.[105] Selling advertising relies on high "user engagement" to justify high advertising prices, so these content-shaping algorithms often promote content that is designed to provoke consumers, such as hate speech or misinformation. Such examples are clear reminders that platforms hold the power to determine what we see, how we use their services, and with whom we interact. (Q1, Q3.)

***

These five practices—collection, personalization, gatekeeping, influencing, and mediation—are features of commercial surveillance and natural consequences of the immense pressure that companies face to monetize consumer data. Whether these practices are good or bad depend on how they are implemented. The duty owed to corporate shareholders to maximize profit coupled with the absence of meaningful trade rules governing data practices creates commercial incentives and business models that lead to lax data security measures and harmful commercial surveillance practices.[106] Unless prohibited from otherwise doing so, companies will continue to find ways to nudge, influence, and manipulate consumers into divulging personal information or "consenting" to technical tracking measures. Companies will invest in methods of circumventing consumer privacy measures, such as the blocking and deletion of tracking cookies. (Q11.)

C. Commercial Surveillance Causes Substantial Injury to Consumers and Society

The Commission is tasked with preventing unfair trade practices—those acts or practices which *cause or are likely to cause substantial injury* to consumers which are not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[107] Commercial surveillance inflicts substantial injuries upon consumers, commerce, and society, but courts and regulators have long struggled to recognize and quantify privacy injuries.[108] This discrepancy arises in part because privacy harms are often small but numerous, involve a future risk of varied injuries, and often affect society in addition to individual consumers.[109] Another challenge is that there are different ways to conceptualize the harms inflicted by commercial surveillance, because industry's insatiable appetite for data, spurred by the absence of meaningful privacy rules, affects our autonomy, dignity, and society in profound (albeit diffuse) ways. As we have written before, "[i]n addition to our attention getting wheedled, manipulated, swindled, or outright taken from us, the appetite for data is producing reduced cognitive skills, reduced personal intimacy and offline interactions, and a corrosion of

---

[105] Jon Evans, *Facebook Isn't Free Speech, It's Algorithmic Amplification Optimized for Outrage*, TECHCRUNCH (Oct. 20, 2019, 8:00 AM), https://techcrunch.com/2019/10/20/facebook-isnt-free-speech-its-algorithmic-amplification-optimized-for-outrage.

[106] Richards & Hartzog, *supra* note 16,16 at 970 ("[P]rivacy 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. 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.").

[107] 15 U.S.C. § 45(n) (2018).

[108] *See generally* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 BOSTON U. L. REV. 793 (2022).

[109] *Id.* at 816–19.

democracy."[110] One can examine the ways in which commercial surveillance undermines human values such as identity, freedom, and protection.[111] Another option is to examine how commercial surveillance enables powerful companies to profile and sort, nudge, and manipulate consumers. These varied examples of harm are important in their own ways, but they do not provide a coherent framework for the Commission to work from. For trust to flourish in digital markets, we need to properly identify the myriad ways in which consumer surveillance substantially injures consumers, including the indirect pecuniary harms which shape consumer behavior. For conceptual clarity, this subsection divides the harms stemming from commercial surveillance into those inflicted upon individuals and those inflicted upon society. (Q4, Q7.)

1. Commercial Surveillance Inflicts Substantial Injuries on Consumers Which Prevent Them from Safely Participating in Markets

There are numerous individual injuries which result from certain commercial surveillance practices. Professors Danielle Citron and Daniel Solove have produced an extremely useful typology of privacy harms which should serve as the starting point for a discussion of privacy harms. In their work, they identify seven basic types of privacy harms: (a) physical harms, (b) economic harms, (c) reputational harms, (d) psychological harms, (e) autonomy harms, (f) discrimination harms, and (g) relationship harms.[112] The case law surrounding these harms (and their often contradictory recognition by courts) is nuanced, but each category illuminates how commercial surveillance causes substantial injury to consumers. In addition to the Citron-Solove typology of harms, these comments identify two broader categories of individual injuries which shed light on how to distinguish beneficial and harmful commercial surveillance: exploitation and the inability to safely interact in markets.

a. Threats of Physical Violence

The improper sharing of personal data promotes, facilitates, and enables *physical violence* such as murder, physical assault, and rape.[113] Commercial surveillance increases the risk of physical harm because it vastly increases the amount of personal data in circulation. This proliferation of consumer data increases the risk of exposure of that data, which in turn makes consumers more susceptible to physical violence. The law recognizes this risk in certain circumstances, as evinced by the fact that "[e]ntities handling personal data have been found liable for negligently, knowingly, or purposefully paving the way for a third party to physically injure someone."[114] The threat of physical violence only grows as practices such as doxing grow in popularity every year.[115] This risk is especially great for people such as women, members of the

[110] Hartzog & Richards, *supra* note 37,37 at 1726.
[111] *See* RICHARDS, *supra* note 21,21 at 109.
[112] Citron & Solove, *supra* note 108,108 at 831.
[113] *Id.*108 at 832–33.
[114] *Id.*
[115] *Id.* at 834.

LGBTQ+ community, and racial, ethnic, and religious minorities who have historically been the victims of discrimination and marginalization.

b. Direct and Indirect Economic Harm

Unnecessary and disproportionate data collection, processing of personal data, and lax data security measures can lead to direct and indirect economic injuries. Consumers suffer financially from identity theft, both the crime itself as well as the time and money spent trying to mitigate risk of an identity thief acting on that data.[116] The Commission has previously brought enforcement actions where companies' data security practices were inadequate, even where there was not a subsequent breach.[117] The Commission has also brought an unfairness enforcement action where a company's misuse of information obtained in violation of one site's user agreement subjected consumers to risk of economic harm.[118] The role of data brokers in facilitating identity theft and other economic harms should not be overlooked. For example, the Department of Justice recently entered a consent decree with data brokers Macromark, KBM, and Epsilon, each of whom compiled lists of people profiled as naïve.[119] These lists of vulnerable individuals (including elderly Americans and people suffering from mental health difficulties), known as "suckers lists," were sold to scammers who fraudulently solicited money from those vulnerable consumers.[120] These scams can have a cascading effect, where a vulnerable consumer is targeted repeatedly and has their wealth siphoned.[121] The loss of important opportunities is a form of indirect pecuniary harm which warrants consideration. Risk of future economic injury, such as when a receipt displays too many digits of a credit card number, can be considered a harm as well,[122] as recognized by the Commission's prior enforcement actions for inadequate security even in the absence of a data breach.[123] (Q9.)

---

[116] *Id.* at 835.
[117] Citron & Solove, *supra* note 108, at 837 (citing (citing Complaint, Microsoft Corp., No. C-4069, FTC File No. 012-3240 (F.T.C. Dec. 20, 2002), https://www.ftc.gov/sites/default/files/documents/cases/2002/12/microsoftcmp.pdf; Complaint, Guess?, Inc., No. C-4091, FTC File No. 022-3260 (F.T.C. filed July 30, 2003), https://www.ftc.gov/sites/default/files/documents/cases/2003/08/guesscomp.pdf; Complaint, Zoom Video Commc'ns, No. C-4731, FTC File No. 192-3167 (F.T.C. filed Jan. 19, 2021), https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint_0.pdf); *see also* Complaint, United States v. Rental Research Services, Inc., FTC File No. 072-3228 (D. Minn. Mar. 5, 2009), https://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrscmpt.pdf.
[118] *See* Complaint for Permanent Injunction and Other Equitable Relief, ¶ 17, FTC v. ReverseAuction.com, No. 00-CV-00032 (D.D.C. Jan. 6, 2000), https://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversecmp.htm
[119] Alistair Simmons, *The Justice Department's Agreement With a Data Broker That Facilitated Elder Fraud*, LAWFARE (Nov. 7, 2022, 8:16 AM), https://www.lawfareblog.com/justice-departments-agreement-data-broker-facilitated-elder-fraud.
[120] *Id.*
[121] *Id.*
[122] Citron & Solove, *supra* note 108, at 836.
[123] *Id.* at 837.

c. Reputational Harms

Reputation and standing in the community are important traits which have long been protected by legal doctrines such as libel and defamation law or the false light privacy tort.[124] Prevalent commercial surveillance and lax data security, however, have increased the chance of harm to reputation and social standing via leaks of personal information. Everyone is only one moment away from virality, and even seemingly innocuous information can be weaponized against us, harming one's reputation.[125] Not only are these injuries in and of themselves, but loss of reputation or community standing can have knock-on effects, such as "lost business, employment, or social rejection."[126] Risk of reputational harm also increases where there are "sloppy, incomplete, and incorrect records."[127] Inaccurate data can be harmful when exposed, but even when not exposed to others there is still the challenge of managing and correcting that data, which is a burden borne by consumers.

d. Psychological Harms

Emotional distress has long been a part of the discussion surrounding privacy harms, going back to Warren and Brandeis's germinal 1890 article *The Right to Privacy*.[128] Psychological harms caused by privacy violations can produce a variety of potential injuries, but the Citron-Solove typology divides them into emotional distress and disturbance.[129] Encompassing emotions such as "annoyance, frustration, fear, embarrassment, anger, and various degrees of anxiety," emotional distress can produce significant harms, as tort law has also recognized for many years.[130] Take for example the emotional harm that Bobbi Duncan suffered when Facebook outed her to her father.[131] The social media platform's default settings allowed users to be added to groups in a public way without their permission, so Bobbi's father received an automatic update when Bobbi was added to the Facebook group for the University of Texas at Austin's Queer Chorus. This digital privacy violation resulted in the two becoming estranged and Bobbi falling into depression.[132] In addition to such reckless or negligent practices, malicious practices such as impersonation, doxing, leaking of intimate images, and threats can create devastating fear.[133] Dealing with identity theft leaves a

---

[124] *Id.* at 837–38.
[125] *See, e.g.*, Maria Luisa Paul, *Couch Guy to West Elm Caleb: Inside the Making of a TikTok 'Villain'*, WASH. POST (Jan. 23, 2022, 7:00 AM), https://www.washingtonpost.com/technology/2022/01/23/west-elm-caleb-tiktok (describing the ease with which a man, dubbed "West Elm Caleb," became an inadvertent villain on TikTok, resulting in harassment).
[126] Citron & Solove, *supra* note 108, at 838.
[127] *Id.* at 839.
[128] *Id.* at 842 (citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197 (1890)).
[129] *Id.* at 841.
[130] *Id.*
[131] HARTZOG, *supra* note 8,40 at 1.
[132] Citron & Solove, *supra* note 108, at 841.
[133] *Id.* (citing DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 35–55 (2014)).

heavy emotional toll.[134] In cases involving privacy torts, courts recognize "feelings of violation, mortification, fear, humiliation, and embarrassment" as cognizable harms.[135] In contrast to Citron and Solove's first category of emotional distress, their second category of disturbance "involves unwanted intrusions that disturb tranquility, interrupt activities, sap time, and otherwise serve as a nuisance."[136] Unsolicited telephone calls and text messages are prototypical examples here.[137] The Commission pursued a similar theory of harm in *FTC v. Accusearch*, where the unconsented-to disclosure of telephone records subjected consumers to emotional harm, including stalking and harassment.[138] A more subtle and insidious form of disturbance is the way in which our attention is getting "wheedled, manipulated, swindled, or outright taken from us" by addictive design decisions which feed industry's insatiable appetite for data.[139] These disturbances waste our time, distract us, and intrude into our private and personal peace.

e. Autonomy Harms

As previously explained, all surveillance exists for the purposes of influence, management, protection, or direction—and commercial surveillance is no exception.[140] When done to achieve disloyal, self-serving ends, commercial surveillance can restrict, undermine, inhibit, or unduly influence people's choices. These threats to consumer autonomy are significant, and in addition to harming individual consumers, they undermine trust in markets when they become prevalent. People want to make choices in accordance with their preferences, but deceptive design and subtle forms of influence prevent them from doing so. Loss of autonomy can be effectuated in different ways, and the Citron-Solove typology also helpfully divides these harms into the six subcomponents of (i) coercion; (ii) manipulation; (iii) failure to inform; (iv) thwarted expectations; (v) lack of control; and (vi) chilling effects.

i. Coercion

A vivid and age-old example of harm to autonomy is coercion, which occurs where there is "a constraint or undue pressure on one's freedom to act or choose."[141] Commercial surveillance can give rise to coercion where consumers are punished for exercising privacy rights or a service (most notably a critical service, like medical treatment) is conditioned on agreeing to provide personal data for purposes unrelated to the service itself.[142]

---

[134] *Id.* at 842.
[135] *Id.* at 843.
[136] *Id.* at 844.
[137] *Id.*
[138] FTC v. Accusearch Inc., 570 F.3d 1187, 1193–94 (10th Cir. 2009).
[139] Hartzog & Richards, *supra* note 37, at 1726.
[140] *Supra* Part I.A.
[141] Citron & Solove, *supra* note 108,108 at 846.
[142] *Id.*

ii. Manipulation

Manipulation is an especially pernicious kind of harm because it is invisible to consumers if done correctly. Definitions of manipulation vary. Danielle Citron and Daniel Solove define manipulation as "undue influence over a person's behavior or decision-making,"[143] In an effort to explain the difference between manipulation, which is harmful, and influence, which is tolerable, Cass Sunstein has written that "an effort to influence people's choices counts as manipulation to the extent that it does not sufficiently engage or appeal to their capacity for reflection and deliberation."[144] Consistent with the concepts of loyalty and relational vulnerability embraced in these comments, Shaun Spencer has defined manipulation as "an intentional attempt to influence a subject's behavior by exploiting a bias or vulnerability."[145] In its policy statement on unfairness, the Commission has itself recognized manipulation (trade practices that prevent consumers from "effectively making their own decisions") as a substantial injury and unfair trade practice, because sellers engaging in manipulation "unreasonably create[ ] or take[ ] advantage of an obstacle to the free exercise of consumer decisionmaking."[146]

We have written before that companies act disloyally when they exploit consumer trust by first profiling and sorting consumers and then nudging them in order to manipulate them to act in accordance with the company's interests.[147] Governments and companies have long used human information to *profile and sort* humans,[148] but commercial surveillance has greatly increased the capacity of powerful organizations to identify, classify, and assess consumers to those consumers' detriment. We have explained that "the mere act of *classification* to more effectively drive purchasing habits is itself an exploitation of data-derived vulnerabilities."[149] This classification has become more potent as commercial surveillance generates vast troves of consumer data, enabling more specific and precise classifications. The human information produced by digital activities may have initially been used only to benefit consumers in the form of improved quality of service (a loyal data practice to be sure), but it is increasingly employed to predict and influence consumers in ways which benefit the company alone.[150] Once consumers have been profiled and sorted, new behavioral science tools, coupled with advances in data science, are deployed to *nudge* consumers into acting in ways which benefit the company but which are not in consumers' best interests.[151] The net effect of these "evil nudges" is manipulation. It is well understood now that "entities who

---

[143] *Id.*
[144] *Id.* at 847 (citing Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MKTG. BEHAV. 213, 216 (2015) (emphasis omitted)).
[145] *Id.* (citing Shaun B. Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959, 990).
[146] *Id.* at 848 (citing FTC, FTC POLICY STATEMENT ON UNFAIRNESS (1980), *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1070, 1074 (1984)).
[147] Richards & Hartzog, *supra* note 16,16 at 970.
[148] *Id.*
[149] *Id.* at 971.
[150] *Id.* (citing ZUBOFF, *supra* note 5859).
[151] *Id.* at 973.

can control how choices are structured can also control, at least at the margins, what decisions humans make."[152] Moreover, in the absence of restrictions on such disloyal practices, competitive market incentives can effectively require companies to leverage choice architecture and behavioral science to manipulate consumers by exploiting their known irrationalities, nudging consumers in ways that promote only the company's financial interests.[153] This can be a vicious cycle. Manipulation facilitates greater extraction of data which provides disloyal companies with ever-more detailed and granular data, enabling more effective profiling and sorting, prediction of consumer behavior, and, ultimately, control.[154]

iii. Failure to Inform

The failure to inform, defined as "failing to provide individuals with information to assist them in making informed choices about their personal data or exercise of their privacy rights," is a substantial injury to consumers and their autonomy because "it limits people's ability to make choices consistent with their preferences."[155] Failure to inform consumers of their rights or to give important information is an autonomy injury because it impedes those consumers' "ability to assert their rights at the appropriate times, to respond effectively to issues involving their personal data, or to make meaningful decisions regarding the use of their data."[156] For example, the Commission has previously found that it was an unfair practice for a company to fail to notify its human customers that "many preexisting files on consumer computers would be designated for public sharing."[157] In that case, *FTC v. Frostwire*, the defendants had configured their application's default settings so that, upon installation, preexisting files on the consumer's device were immediately designated for sharing.[158] Failing to inform consumers of that default setting rendered them unable to effectively protect their files. Where personal data is used to make a decision about a consumer, failure to inform likewise harms consumers because they are left unable to "understand how their data affected a decision," nor are they able to respond.[159] Failure to inform is a serious threat to consumers in modern commercial relationships because online environments are constructed—consumer action is limited to the options given, and consumers rely on design to inform them of what they can do. While the notice and choice regulatory regime was meant to empower consumers by informing them of companies' data practices, this notice largely has

[152] *Id.* at 974–75.
[153] *Id.*
[154] *Id.*
[155] Citron & Solove, *supra* note 108,108 at 848.
[156] *Id.* at 849.
[157] Solove & Hartzog, *supra* note 5, at 642.
[158] Complaint, FTC v. Frostwire, LLC, No. 11-cv-23643 (S.D. Fla. Oct. 12, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf.
[159] Citron & Solove, *supra* note 108, at 849.

proven to be fictitious, leaving consumers unable to make truly informed choices about their personal data.[160]

iv. Thwarted Expectations

Relevant to concepts of loyalty and relational vulnerability, thwarted expectations harms arise where consumers' choices have been undermined, such as when a company breaks its promises made about data practices.[161] Thwarted expectations leave consumers unable to act in accordance with their preferences, which undermines the trust which is necessary for consumers to be safe market participants. The Commission has consistently recognized the harm of thwarted expectations when enforcing violations of privacy policies as deceptive acts and retroactive changes to data practices as unfair trade practices.[162] For example, in *In re Gateway Learning Corp.*, the Commission found that it was unfair for a company to retroactively apply privacy policy changes to personal data they had previously collected from consumers.[163] Remedying thwarted expectations is consistent with the Commission's core mission, because "[t]he market cannot work fairly if people's expectations are completely wrong, if people lack knowledge of potential future uses of their personal data, and if people have no way to balance the benefits and risks of using products or services."[164]

v. Lack of Control

Another autonomy harm resulting from the consciously constructed nature of modern commercial relationships is the lack of control, which "involves the inability to make certain choices about one's personal data or to be able to curtail certain uses of the data."[165] Absent meaningful control, we lose our ability to manage both risk and the peace of mind that comes with such management.[166] At its most extreme, this can entail surreptitious data collection which is invisible to the consumer. The Commission has previously brought enforcement actions under this theory as well. For example, the Commission found that a company acted unfairly when it (i) "installed monitoring software on rented computers and gathered, or caused to be gathered, sensitive personal, financial, and medical information about consumers from those computers," and (ii) "used information improperly gathered from consumers to collect or attempt to collect a debt, money, or property pursuant to a consumer rental contract."[167] Data subject rights such as

---

[160] *See supra* Part II, discussing the failure of notice and choice and the importance of design decisions in empowering and informing consumers; *see also* Citron & Solove, *supra* note 108,108 at 851 ("Many courts fixate on whether plaintiffs have read and relied on the privacy policy of a company, but the privacy policy plays a small role in forming people's privacy expectations. This is especially true because hardly anyone reads privacy policies, and it is not rational to do so given the vast number of organizations collecting data about people.")
[161] *See* Citron and Solove, *supra* note 108,108 at 849.
[162] *See id.* at 852; Solove & Hartzog, *supra* note 5, at 628–30, 640–41.
[163] *In re* Gateway Learning Corp., 138 F.T.C. 443, 445–46, 499 (2004).
[164] Citron & Solove, *supra* note 108,108 at 852–53.
[165] *Id.* at 853.
[166] *Id.*
[167] Complaint, *In re* Aspen Way Enters, Inc., FTC File No. 112-3151, No. C-4392 (F.T.C. Apr. 11, 2013)

rectification or erasure theoretically empower consumers to exert control over how personal data is used, but exercising those rights requires design features which enable or facilitate those actions. Without such protections, control becomes no more than a hollow and pernicious fiction.

vi. Chilling Effects

Commercial surveillance has the potential to create harms well beyond those traditionally thought of as consumer harms and affecting the very fabric of our democracy. Such harms include chilling effects which inhibit consumers from "engaging in certain civil liberties, such as free speech, political participation, religious activity, free association, freedom of belief, and freedom to explore ideas."[168] These chilling effects deter consumers from reading or researching,[169] which "reduce[s] the range of viewpoints expressed and the nature of expression that is shared."[170]

We have written before that privacy not only protects but is essential to enduring human values such as identity and freedom.[171] These are not an exhaustive list of the values which enrich consumers' lives and promote healthy commerce, but examining the chilling effects of the commercial surveillance apparatus on those values paints a morbid picture, one which illuminates some of the ways in which pervasive commercial surveillance substantially harms consumers, commerce, and society. Privacy supplies the space for *identity* development and experimentation, which is necessary for developing "a diversity of interests, opinions, and identities as a society."[172] Harm to identity formation resulting from commercial surveillance manifests itself in different ways. Facebook's "real" name policy, for example, harms consumers by forcing them into one singular identity, preventing exploration and experimentation. Hyper-personalized digital services focused on maximizing engagement can create echo chambers which harm consumers' identities and civic lives by depriving them of information which is new to them; and excessive exposure online drives our identities toward mainstream homogeneity.[173] Because surveillance transcends the public-private divide, commercial surveillance also threatens our political *freedom* in profound and consequential ways. Surveillance stifles our intellectual freedom and chills the exercise of our civil liberties.[174] Our intellectual freedom is harmed by the hyper-personalization and targeting described above. Our physical and legal freedom is implicated as well in increasingly powerful and concerning ways. One sobering example is the threat that pregnant people face in a post-*Roe* world. Collected geolocation data, phone location data, internet searches, and purchase history can

---

[168] *Id.* at 854; *accord* Richards, *supra* note 28,28 at 1935.
[169] Citron & Solove, *supra* note 108,108 at 854 (citing NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 165 (2015)).
[170] *Id.* (citing RICHARDS, *supra* note 169, at 180; Neil M. Richards, *Intellectual Privacy*¸ 87 TEX. L. REV. 387, 419, 419 n.199 (2008); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000)).
[171] *See* RICHARDS, *supra* note 21,21 at 109.
[172] *Id.* at 130.
[173] *Id.* at 111–13, 120–23, 123–25, 125–30.
[174] *Id.* at 131–63; *see also* Richards, *supra* note 2828.

all be used to penalize and prosecute people who seek abortions.[175] More generally, surveillance breeds dangers to political freedom in the form of blackmailing and discrediting, discrimination, and persuasion.[176] Each of these risks chills individuals from fully exercising their civil liberties and taking advantage of the positive aspects of digital markets and the potential of digital democracy.

f. Discrimination Harms

Another category of harm that has disastrous social effects in addition to the substantial injuries inflicted upon individual consumers is discrimination, which "involve[s] entrenching inequality and disadvantaging people based on gender, race, national origin, sexual orientation, age, group membership, or other characteristics or affiliations"[177] Discrimination harms such as those felt by women, members of the LGBTQ+ community, and racial and religious minorities often manifest as other kinds of harms detailed above but with additional harms that are unique to discrimination. For example, discrimination can be an autonomy harm in that it results in the denial of opportunities a consumer would otherwise be afforded.[178] Period tracking apps sharing information with employers and insurance companies can result in raised premiums or denied promotions for the consumers using such apps.[179] Women and minorities face increased risk of physical violence due to online harassment and doxing.[180] Survivors of abuse who have nude photos or embarrassing, intimate information posted online suffer "substantial emotional and reputational harm."[181] But discrimination does more than lessen someone's autonomy or raise the risk of physical violence; it also inflicts different injuries such as "a searing wound of stigma, shame, and loss of esteem that can turn into permanent scars."[182] These effects combine to create a "distinct and distinctly harmful type" of psychological harm wherein affected individuals believe

---

[175] The Commission highlighted this risk in its recent enforcement action against Kochava, a geolocation data broker who was selling data which could be used to identify consumers who have visited an abortion clinic. Complaint, ¶ 25, FTC v. Kochava Inc., No. 22-cv-377 (D. Idaho Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf. *See also* Jennifer Korn & Claire Duffy, *Search Histories, Location Data, Text Messages: How Personal Data Could Be Used to Enforce Anti-Abortion Laws*, CNN: BUS. (June 24, 2022, 4:27 PM), https://www.cnn.com/2022/06/24/tech/abortion-laws-data-privacy/index.html; Kingsbury, *supra* note 44; James Vincent, *Facebook Turns Over Mother and Daughter's Chat History to Police Resulting in Abortion Charges*, VERGE (Aug. 10, 2022, 5:51 AM), https://www.theverge.com/2022/8/10/23299502/facebook-chat-messenger-history-nebraska-teen-abortion-case ("[P]rivate chat messages are only one component in a whole range of digital evidence that is likely to be used by police to prosecute illegal abortions in the United States. Investigators will be able to request access to many data sources, including digital health records, Google search history, text messages, and phone location data.").

[176] *See* RICHARDS, *supra* note 21,21 at 146–62.

[177] Citron & Solove, *supra* note 108,108 at 855.

[178] *Id.*

[179] *Id.* at 856.

[180] *Id.*; *see also supra* Part I.C.1.a.

[181] *Id.* (citing CITRON, *supra* note 133,133 at 54; Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1914–15 (2019)).

[182] *Id.* at 855–56.

that they are viewed as being less worthy of respect.[183] Disloyal commercial surveillance has ample potential to enable or facilitate discrimination, such as where sensitive personal data is collected, where data is processed to further discrimination, or where platforms mediate consumer interaction with services in such a way as to enable harassment and abusive targeting.

g. Relationship Harms

Commercial surveillance has the potential to damage the intimate personal, professional, and organizational relationships in our lives.[184] The ability to withhold and disclose information is essential for maintaining relationships, which in turn requires that parties "trust[] each other to maintain the confidentiality of their information."[185] One example of a personal relationship harm, discussed above, is how Bobbi Duncan was inadvertently outed by Facebook.[186] Facebook's default design choice (without customer permission) to publicize if a customer joined a group outed Bobbi Duncan when she joined Facebook's for the University of Texas at Austin's Queer Chorus group.[187] Bobbi's father saw that his daughter joined this group and the two became estranged.[188] Had Facebook been transparent about its information practices, Bobbi likely would have concealed this information, not only for the sake of her own privacy but to maintain certain relationships.

Privacy violations can also lead to professional relationship harms. In the workplace, persistent and overbroad monitoring of workers is creating a power imbalance and forming a rift between employers and employees. For example, over the last year, Amazon has implemented AI cameras in their driver vehicles, requiring drivers to sign forms consenting to the collection and use of their biometric data to keep their jobs.[189] Further, in Amazon's warehouses, the company uses sensors and tablets to track workers' movements and productivity.[190] A worker can be fired if they are adjudged to be under-productive, which has led to higher rates of employee injury and some workers skipping needed breaks to avoid the risk of losing their job.[191] Not only has this extreme workplace surveillance harmed employees, it has also placed a huge strain on the employer-employee relationship. Intense workplace surveillance creates an environment of distrust that can lead to strained workplace environments. Relationships can thus suffer from both the loss of confidentiality and the loss of trust.[192] This loss of trust is most important to the Commission's core mission of enabling consumers to be safe market participants.

---

[183] *Id.* at 856.
[184] *Id.* at 859.
[185] *Id.*
[186] *See infra* Part I.C.1.h. (citing HARTZOG, *supra* note 8,40 at 1).
[187] *Id.*
[188] *Id.*
[189] Kathryn Zickuhr, *Workplace Surveillance is becoming the New Normal for U.S. Workers*, WASH CTR. FOR EQUITABLE GROWTH (Aug. 2021), https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers.
[190] *Id.*
[191] *Id.*
[192] Citron & Solove, *supra* note 108,108 at 859–60.

h. Inability to Safely Interact in Markets

The injuries detailed above result from a variety of different commercial surveillance practices which affect different consumers in different ways. One underlying theme of these injuries is that they result from disloyal commercial surveillance. Not all privacy injuries are caused by disloyal commercial surveillance, but all disloyal commercial surveillance causes substantial injuries. The net effect of these injuries is a second-order harm which is central to the Commission's mission: the prevalence of disloyal commercial surveillance sabotages the ability of consumers to be safe market participants. Disloyal behavior causes consumers to mistakenly trust companies to their detriment, which prevents consumers from participating in the market because they can no longer trust commercial actors. Due to the unique nature of modern commercial relationships, consumers have no choice but to expose themselves to commercial actors who hold significant power over them;[193] exposing their data is an unavoidable condition of modern commercial participation. Every day consumers make themselves vulnerable when they trust companies with their data and online experiences. Consumers overwhelmingly want companies to take data responsibility seriously and to take the lead in establishing corporate data responsibility,[194] but companies continue to betray those consumers by succumbing to self-serving, opportunistic, and exploitative behavior. Companies collect, aggregate, analyze, retain, transfer, and monetize consumer data and the direct derivatives of that information in ways that conflict with the best interests of those consumers. In this way, disloyal commercial surveillance betrays consumers. Consumers suffer these injuries, they are cognizant that they may be similarly injured again, and having little to no recourse, they are faced with a Hobson's choice of either being left at risk of betrayal or not participating in digital markets at all. The idea that consumers should be able to safely interact in markets is one which the Commission has built out in its prior enforcement actions, separate from financial harm or extreme emotional damage, and is one which is central to the very idea of consumer protection law. (Q8, Q9.)

This lens of disloyalty, betrayal, and relational vulnerability gives the Commission a new way to identify unfair practices in the context of commercial surveillance. The Section 5 unfairness authority is not limitless, and there will be many situations where a commercial surveillance practice is disloyal but does not rise to the level of a substantial injury, even when aggregated across consumers. Nevertheless, a focus on disloyalty will identify a subset of commercial surveillance practices which are so exploitative that the injury caused does warrant enforcement under the Commission's Section 5 powers.[195]

2. Commercial Surveillance Inflicts Substantial Injuries on Our Mental Health, Civil Rights, and Democracy in Contravention of Established Public Policy

In addition to the myriad harms suffered by consumers, commercial surveillance can also impose significant externalities and social harms. The Commission is statutorily empowered to

---

[193] *See infra* Part III.A.
[194] LUCAS & STEIN, *supra* note 45, at 8 (finding that 91% of respondents say companies should take data corporate responsibility seriously and that 91% say that companies should take the lead in establishing corporate data responsibility).
[195] *See infra* Part III.B.

consider established public policies as evidence in determining whether an act or practice is unfair.[196] Any trade regulation rules contemplated by the Commission should take notice of the ways in which pervasive commercial surveillance harms our mental health, civil rights, and democracy.[197]

a. Mental Health

The intense pressure to monetize user data pushes tech companies to design our phones and computers to be addictive, so as to extract ever-increasing amounts of data[198] with no regard to the substantial injuries dealt to "our mental well-being, our social relationships, and even the very nature of what it means to be a human in our modern world."[199] Modern technologies are "designed to be addictive to maximize interaction and data collection."[200] The average person checks their phone over three hundred times *every day*.[201] This compulsive screen usage wreaks havoc on our mental health, especially that of children and teenagers,[202] and is linked with increased anxiety, depression, and related physical ailments.[203] Compulsive social media use creates a sense of FOMO ("fear of missing out"), which in turn leads to negative moods, low levels of life satisfaction, and threatens consumers' mental health.[204] Increased suicide rates for

---

[196] 15 U.S.C. § 45(n) (2018).
[197] Hartzog & Richards, *supra* note 37,37 at 1755–1760.
[198] *Id.*37 at 1756.
[199] *Id.*
[200] *Id.* at 1725.
[201] *Infra* note 382382 and accompanying text.
[202] *See, e.g.*, Georgia Wells, Jeff Horwitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sept. 14, 2021, 7:59 AM), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 (describing how Meta (then Facebook) spent years conducting studies on how Instagram affected its millions of young users and was aware that the app was causes significant harm to the mental health of users, particularly teenage girls); Adam Satariano & Ryan Mac, *Facebook Delays Instagram App for Users 13 and Younger*, N.Y. TIMES (Oct. 27, 2021), https://www.nytimes.com/2021/09/27/technology/facebook-instagram-for-kids.html (describing how Meta delayed launching Instagram Kids in response to criticism over how the platform affects the mental health of young users); Matt Richtel, *A Teen's Journey Into the Internet's Darkness and Back Again*, N.Y. TIMES (Sept. 9, 2022), https://www.nytimes.com/2022/08/22/health/adolescents-mental-health-technology.html (using one teen's personal struggles with mental health to examine the broader context of mental health harms posed by excessive screen time and social media use); *see also* Alvaro Bedoya, Comm'r, Fed. Trade Comm'n, "Who is being left behind?": Enforcement Priorities for a Tech Consumer Protection Agenda (Aug. 9, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/who_is_being_left_behind_-_naag_presidential_summit.final_.public_version.pdf ("[A] growing body of evidence suggests that teenagers, particularly teenage girls, who spend more than two or three hours a day on social media, suffer from increased rates of depression, anxiety, and thoughts of suicide and self-harm.").
[203] *The Social Dilemma: Social Media and Your Mental Health*, MCLEAN HOSP. (Jan. 21, 2022), https://www.mcleanhospital.org/essential/it-or-not-social-medias-affecting-your-mental-health (discussing the effects of social media and excessive internet use on mental health as well as ways in which users can better protect themselves); Catherine Price, *Putting Down Your Phone May Help You Live Longer*, N.Y. TIMES (Apr. 24, 2019), https://www.nytimes.com/2019/04/24/well/mind/putting-down-your-phone-may-help-you-live-longer.html (discussing how smart phone usage contributes to increased stress and higher levels of cortisol in the body that can be detrimental to human health).
[204] ZUBOFF, *supra* note 58,59 at 463.

teenagers, especially teenage girls, have been linked to increased screen time.[205] Content promotion algorithms which elevate incendiary, polarizing, hateful, and abusive content for the sake of increased engagement stimulate outrage and increase the likelihood that those hateful messages will find their intended targets.[206] (Q13, 14, 15, 16, 17)

Mental health harms are not limited to addictive social media and engagement juicing. Targeted advertising can inflict substantial injuries to mental health as well. Traumatic life experiences can be perpetuated when advertisements related to that trauma haunt users around the web, suffocating any chance at healing or escape.[207] Consumers worrying about (and hence searching for information about) infertility are met with constant ads for period products, which serve as a constant reminder of their fears.[208] One woman, for example, was inundated with tombstone ads after her mother's death from cancer.[209] People who are exploring their sexual or gender identities can reasonably fear that related "relevant" ads may out them to their families on terms not of their choosing.[210] People who have or are recovering from eating disorders can be subjected to ads regarding diets or meal supplements, perpetuating their harmful conditions and impeding their recoveries. Targeted advertisements take our most intimate details and leverage that vulnerability to try and sell us goods and services, sometimes to traumatic and tragic ends. In one harrowing example, journalist Gillian Brockell was barraged with baby-related advertisements for months after learning her baby would be stillborn.[211] A personal tragedy—one which should have been subject to an intimate mourning period— instead became a wound that was reopened

---

[205] *See* Alice G. Walton, *Phone Addiction Is Real – And So Are Its Mental Health Risks*, FORBES (Dec. 11, 2017, 10:53 AM), https://www.forbes.com/sites/alicegwalton/2017/12/11/phone-addiction-is-real-and-so-are-its-mental-health-risks;*see also* Melissa G. Hunt, Rachel Marx, Courtney Lipson, & Jordyn Young, *No More FOMO: Limiting Social Media Decreases Loneliness and Depression*, J. SOC. & CLINICAL PSYCH. 37:10 751-768 (2018), https://doi.org/10.1521/jscp.2018.37.10.751 (discussing a study conducted with college students where some reduced the time spent on social media while other did not, with results being that those that spent less time online decreased feelings of loneliness and depression); Jean M. Twenge, Thomas E. Joiner, Megan L. Rogers & Gabrielle N. Martin, *Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time*, 6 CLIN. PSYCH. SCI. 1 (Jan. 2018), https://journals.sagepub.com/doi/10.1177/2167702617723376.

[206] *See* Luke Munn, *Angry by Design: Toxic Communication and Technical Architectures*, HUMANITIES & SOC. SCI. COMM'C'NS 7:53 (July 2020), https://doi.org/10.1057/s41599-020-00550-7 (discussing how "hate-inducing architectures" amplify hate online, leading to "real world" harms).

[207] *See generally* Rae Nudson, *When Targeted Ads Feel a Little Too Targeted*, VOX (Apr. 9, 2020, 10:20 AM), https://www.vox.com/the-goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus ("When someone has experienced a trauma or is struggling with something — and is perhaps searching for answers online — these ads can become an unwelcome reminder. The best many can hope for is that these ads are unnoticeable or mildly annoying. For others, though, they can cause real harm to mental health.").

[208] *Id.*

[209] *Id.*

[210] *Id.*

[211] Lauren Feiner, *A Woman Shared Her Tragic Story of How Social Media Kept Targeting Her With Baby Ads After She Had a Stillbirth*, CNBC (Dec. 12, 2018, 4:32 PM), https://www.cnbc.com/2018/12/12/woman-calls-out-tech-companies-for-serving-baby-ads-after-stillbirth.html.

with every digital interaction. Gillian's experience is clearly not atypical, as self-help guides have sprung up to help similarly situated people try to escape the trauma of pervasive pregnancy ads following a loss.[212] (Q13, 14, 15, 16, 17.)

b. Civil Rights

Commercial surveillance also threatens our civil rights. Social media facilitates anonymous speech by making speech seemingly costless and consequence-free. This might hypothetically be a good thing in some circumstances,[213] but it also leads in practice to "harassment, bile, and abuse . . . largely against women, people of color, and other marginalized and vulnerable populations."[214] Algorithms which elevate and amplify incendiary and divisive content can cause substantial injuries to mental health.[215] By pushing hateful and incendiary content, those same algorithms can chill activities and drive users from platforms. Platform optimization therefore implicates our "cyber civil rights" by reducing the equal ability of all people to make use of those platforms.[216]

There are also "technological due process" concerns raised by the pervasive and opaque use of algorithms to make decisions about "people's health, finances, jobs, ability to travel, and other essential life activities."[217] Such systems shape our lives in powerful ways and have the ability to amplify and perpetuate age-old discrimination.[218] Modern data discrimination, the product of from targeted advertising and automated decision-making, manifests itself in a variety of harmful practices, including "digital redlining, differential pricing, racist search results, and social media filter bubbles."[219] Earlier this year, the United States Government Accountability Office prepared a report urging Congress to consider enhancing protections around scores used to rank consumers.[220] Consumer scoring can lead to unfair and discriminatory outcomes when done without transparency. This problem is amplified when scoring is automated and applied at scale. To combat these issues, society needs (1) algorithmic accountability centered around fairness,

---

[212] *See, e.g.*, *How to Stop Pregnancy Ads Following You After a Loss*, TOMMY'S (Jan. 14, 2021), https://www.tommys.org/about-us/charity-news/how-stop-pregnancy-ads-following-you-after-loss.
[213] *See* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1995) (predicting that the internet would reduce the costs of distributing speech and, hence, foster democracy by expanding the reach of diverse voices).
[214] Hartzog & Richards, *supra* note 37,37 at 1758.
[215] *Supra* Part I.C.2.a.
[216] Hartzog & Richards, *supra* note 37,37 at 1758 (citing CITRON, *supra* note 133, at 56–72, Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 65–66 (2009), Woodrow Hartzog & Evan Selinger, *Increasing the Transaction Costs for Harassment*, 95 B.U. L. REV. ANNEX 47, 47–51 (2015)).
[217] *Id.*
[218] *See* Chris Gilliard, *Friction-Free Racism*, REAL LIFE MAG. (Oct. 15, 2018), https://reallifemag.com/friction-free-racism (describing how "[s]urveillance capitalism turns a profit by making people more comfortable with discrimination").
[219] Dr. Nathalie Maréchal, *Targeted Advertising Is Ruining the Internet and Breaking the World*, VICE (Nov. 16, 2018, 12:54 PM), https://www.vice.com/en/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world.
[220] U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-104527, CONSUMER PROTECTION: CONGRESS SHOULD CONSIDER ENHANCING PROTECTIONS AROUND SCORES USED TO RANK CONSUMERS (2022).

transparency, and similar values and (2) data privacy rules which limit the unfettered, exploitative access to personal data which these algorithms rely upon.[221] (Q65, Q69, Q70, Q71.)

c. Democracy & Discourse

Like the mass medias of the twentieth century before it, the internet creates unique opportunities and challenges for democracy. People have greater access to information and opportunities to engage with one another, which could in turn boost political accountability and constructive debate. On the other hand, increased interconnectivity, data processing, and pervasive commercial surveillance have enabled new forms of "electoral interference, voter suppression, and demagoguery."[222] Richard Hasen has chronicled how the economics of cheap speech have "undermined mediating and stabilizing institutions of American democracy including newspapers and political parties, with negative social and political consequences," replacing problems of media scarcity with new-age challenges like "fake news" and the devastation of the business model of journalism.[223] Matthew Crain has concisely captured the threats commercial surveillance poses to democracy:

> The race to commercialize the Internet is over, and advertising is the big winner. This is excellent news if you are an executive or major shareholder of one of the handful of companies that dominate the $600 billion global digital advertising economy. For almost everyone else, advertising's good fortunes have meant the erosion of privacy, autonomy, and security, as well as a weakening of the collective means to hold power accountable. This is because the industry's economic success is rooted in its virtually unrestrained monetization of consumer surveillance. Digital advertising technologies are widely distributed but largely operate under the control of a few giant companies whose monopoly-like market power has, among other ills, unleashed a wave of manipulative communication and deepened a revenue crisis among the nation's most important journalism outlets. For the ownership class of Silicon Valley, digital advertising has been a gold mine of epic proportions. For democratic society, it is gasoline on a fire.[224]

---

[221] *Id.*; *see infra* Part III.C.4.
[222] Hartzog & Richards, *supra* note 37,37 at 1759.
[223] Richard L. Hasen, *Cheap Speech and What It Has Done (to American Democracy)*, 16 FIRST AMEND. L. REV. 200 (2017); *accord* RICHARD L. HASEN, CHEAP SPEECH: HOW DISINFORMATION POISONS OUR POLITICS—AND HOW TO CURE IT (2022); Jeff Kosseff, *Confronting Misinformation in the Age of Cheap Speech*, LAWFARE (May 10, 2022, 3:49 PM), https://www.lawfareblog.com/confronting-misinformation-age-cheap-speech (reviewing Rick Hasen's new book and discussing the problem of misinformation online).
[224] Matthew Crain, *How Capitalism—Not a Few Bad Actors—Destroyed the Internet*, BOSTON REVIEW (Aug. 3, 2022), https://www.bostonreview.net/articles/how-capitalism-not-a-few-bad-actors-destroyed-the-internet [hereinafter Crain, *How Capitalism Destroyed the Internet*]; *accord* MATTHEW CRAIN, PROFIT OVER PRIVACY: HOW SURVEILLANCE ADVERTISING CONQUERED THE INTERNET (2021) [hereinafter CRAIN, PROFIT OVER PRIVACY]; *see also* Maréchal, *supra* note 219.

Trade regulation rules governing commercial surveillance methods should thus be cognizant of the ways commercial surveillance facilitates sophisticated voter manipulation, amplifies rage and hate online, and isolates consumers into "echo chambers."

i. Commercial Surveillance Facilitates Sophisticated Voter Manipulation

Up to this point, these comments have analyzed manipulation as individual injuries, but consumer and citizen manipulation inflicts substantial injuries on society as well.[225] Commercial surveillance supercharges the ability to influence and manipulate voters on a massive scale.[226] For example, the 2012 and 2016 United States presidential elections were marked by the use of data analytics (by both major parties) in driving voter turnout, each of which had a profound effect upon our democracy.[227] Matthew Crain has detailed how "corporate spying," digital advertising, and commercial surveillance harmed our democracy by allowing malicious foreign actors to easily spread misinformation and enabling the corrosive targeting of specific voter groups by both Republicans and Democrats to try and dissuade select Americans from voting.[228]

This voter-manipulation ecosystem—a subset of commercial surveillance's corrosive targeting practices—is highly sophisticated. Opaque voter-profiling systems, fed by a "vast voter data-mining ecosystem" comprising "political consulting, analytics, media, marketing and advertising software companies," allow political campaigns to target and manipulate narrow audiences.[229] For the 2020 presidential election, the travel patterns of tens of millions of Americans were analyzed to develop "Covid concern" scores, which were then used to identify "persuadable Republicans" who campaigners thought might be persuaded to vote Democrat on the basis of pandemic concern.[230] For the 2022 midterm elections, even more voter profile categories were being developed and utilized. Some of the categories identified include "gun owner," "pro-choice," "Trump 2024," "racial resentment," "trans athletes should not participate," and "U.F.O.s distrust government."[231] Such scoring systems, relying on information about consumers such as "demographic profile, socioeconomic status, online activities and offline interests," enable political campaigns to predict voter beliefs and likelihood of voting, and then to try and manipulate

---

[225] Citron & Solove, *supra* note 108,108 at 847.
[226] *See* Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335 (2014).
[227] Hartzog & Richards, *supra* note 37,37 at 1759
[228] CRAIN, PROFIT OVER PRIVACY, *supra* note 224, at 2–3 (citing Issie Lapowsky, *Facebook Exposed 87 Million Users to Cambridge Analytica*, WIRED (Apr. 4, 2018, 5:43 PM), https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica; Alex Stamos, *An Update on Information Operations on Facebook*, FACEBOOK NEWSROOM (Sept. 6, 2017), https://about.fb.com/news/2017/09/information-operations-update; Indictment, United States v. Internet Research Agency LLC, No. 18-CR-00032, 2018 WL 914777 (D.D.C. Feb. 16, 2018), https://www.justice.gov/file/1035477/download; Scott Shane, *LinkedIn Co-Founder Apologizes for Deception in Alabama Senate Race*, N.Y. TIMES (Dec. 26, 2018), https://www.nytimes.com/2018/12/26/us/reid-hoffman-alabama-election-disinformation.html); *see also* Crain, *How Capitalism Destroyed the Internet*, *supra* note 224 (discussing how the techlash against Facebook over its role in these scandals reflected the deeper complaint that "the pervasive consumer surveillance at the heart of the Internet's advertising business model was out of control").
[229] Natasha Singer, *Why Am I Seeing that Political Ad? Check Your 'Trump Resistance' Score*, N.Y. TIMES (Oct. 23, 2022), https://www.nytimes.com/2022/10/23/technology/voter-targeting-trump-score.html.
[230] *Id.*
[231] *Id.*

voters into acting in a particular way. Some of the information used in these profiles comes from public databases, but the data which enable the most detailed and narrow forms of targeting, such as browsing habits, shopping records, or location history, come from commercial actors such as data brokers.[232] This politically motivated micro-targeting and manipulation becomes more effective each passing year as data science methods improve and commercial surveillance makes ever-increasing amounts of granular consumer data available. These profiles represent a threat to our privacy, autonomy and democracy—at least to the extent that we think that democratic elections should be about issues and character rather than which candidates can hire the best data and behavioral scientists.

These dangers extend beyond the mere manipulation of individual voters through targeting. As the Supreme Court of North Carolina explained in *Harper v. Hall*, commercial surveillance and modern data analytics facilitate extraordinarily effective gerrymandering:

> While partisan gerrymandering is not a new tool, modern technologies enable mapmakers to achieve extremes of imbalance that, "with almost surgical precision," undermine our constitutional system of government. Indeed, the programs and algorithms now available for drawing electoral districts have become so sophisticated that it is possible to implement extreme and durable partisan gerrymanders that can enable one party to effectively guarantee itself a supermajority for an entire decade, even as electoral conditions change and voter preferences shift.[233]

This surgically precise level of gerrymandering, which undermines the right to vote, is enabled by commercial surveillance and the lack of substantive limits on the uses of consumer data.

ii. Engagement-Juicing Precipitates Violence and Undermines Discourse

Social media companies optimize their algorithms to maximize engagement.[234] Not only does this "engagement juicing" threaten our mental health, it also promotes the most hateful, vitriolic content on platforms, creating "hate-spiralling algorithms."[235] Such algorithms can lead to distressing ends. For example, Amnesty International has accused Facebook of fueling ethnic cleansing in Myanmar via its content-shaping algorithm.[236] The Mozilla Foundation found

---

[232] *Id*.
[233] Harper v. Hall, 868 S.E.2d 499, 509 (N.C. 2022).
[234] Maréchal, *supra* note 219.
[235] Dell Cameron & Mack DeGeurin, *Meta's Toxic Algorithm 'Substantially Contributed' to Ethnic Cleansing in Myanmar: Amnesty International*, GIZMODO (Sept. 28, 2022, 9:47 PM), https://gizmodo.com/meta-s-toxic-algorithm-substantially-contributed-to-eth-1849594683; *see also* Jeremy B. Merrill & Will Oremus, *Five Points for Anger, One for a 'Like': How Facebook's Formula Fostered Rage and Misinformation*, WASH. POST (Oct. 26, 2021, 1:04 PM), https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm (describing how Facebook's ranking algorithm favors controversial posts, leading to more misinformation, toxicity, and low-quality news).
[236] Cameron & DeGeurin, *supra* note 235235 (describing how Facebook's "content-shaping algorithms" directly fueled ethnic cleansing of Myanmar's Rohingya and how Meta "profited off the swell of divisive, hateful content that aided Myanmar's government in laying the groundwork for a military-led ethnic cleansing campaign").

evidence that TikTok contributed to the spread of disinformation, incendiary rhetoric, lies about candidates, and calls for ethnic violence in the lead up to Kenya's presidential election.[237] In a case to be heard in the Supreme Court, a family is suing Google over the death of Nohemi Gonzalez, who was killed in an ISIS terrorist attack, alleging that Google assisted ISIS by recommending ISIS videos to its human customers.[238] These rage- and hate-producing algorithms are part and parcel of the commercial surveillance ecosystem because they are designed to keep consumers engaged for the purpose of harvesting and exploiting their data.[239] An ad-based company makes more money, after all, when its human customers spend more time engaging with the site, and watch more ads.

In addition to harming our mental wellbeing through the design of addictive services, personalization practices such as curated social media feeds and targeted advertisements also undermine our democracy by isolating us from each other. Personalization creates digital spaces that conform only to that consumer's political and ideological commitments. Such "echo chambers" lessen a consumer's ability to engage with ideologically opposed or different people.[240] As detailed above, consumers are being scored and sorted into increasingly granular voter profiles for the purpose of more "surgical" political message delivery.[241] This kind of "nano-targeting" exacerbates political polarization as consumers are faced with radically different facts and messaging based on how they are targeted.[242]

These individual and social harms detailed above underscore the necessity for privacy and meaningful privacy regulation. Privacy is necessary for human flourishing, whether we conceptualize these humans as consumers or citizens. Any reasonable conceptualization of human flourishing needs to include not only autonomy and dignity harms to the individual, but also the broader mental and social wellbeing implicated by interactions online.

D. The Benefits of Commercial Surveillance Disproportionately Flow to Industry

The individual and social injuries exacted by commercial surveillance are not outweighed by countervailing benefits to consumers or to competition. Commercial surveillance propagandists argue that their practices result in beneficial personalization which outweighs any harms inflicted by those practices. That argument overstates the benefits of personalization and misinterprets how the cost-benefit weighing should be applied, but it gains traction in the broader policy discussion because there is lack of agreement on how to weigh the harms and benefits of commercial surveillance. The Commission needs a conceptual lodestone to identify and examine the

---

[237] Drew Harwell & Taylor Lorenz, *Sorry You Went Viral*, WASH. POST (Oct. 21, 2022, 5:00 AM), https://www.washingtonpost.com/technology/interactive/2022/tiktok-viral-fame-harassment/ (citing Neha Wadekar, *Why Dangerous Content Thrives on Facebook and TikTok in Kenya*, WASH. POST (July 31, 2022, 6:00 AM), https://www.washingtonpost.com/world/2022/07/31/kenya-meta-tiktok-facebook-disinformation.
[238] Rebecca Kern, *SCOTUS to Hear Challenge to Section 230 Protections*, POLITICO (October 3, 2022, 2:57 PM), https://www.politico.com/news/2022/10/03/scotus-section-230-google-twitter-youtube-00060007.
[239] Maréchal, *supra* note 219 (describing how democracy has been harmed by "targeted advertising, which stole journalism's lunch money and used it to sustain platforms whose driving logic isn't to educate, to inform, or to hold the powerful to account, but to keep people "engaged'").
[240] BRIDGES, *supra* note 57,57 at 137.
[241] Singer, *supra* note 229.
[242] *Id.*

countervailing benefits of commercial surveillance under the Section 5 unfairness test. We would submit that loyalty can be that guiding concept. Loyalty fits well into our existing consumer protection scheme because it inherently considers the relative benefits to consumers and industry.

1. The Substantial Injuries Inflicted by Targeted Advertising Are Not Outweighed by Countervailing Benefits to Consumers or Competition

Any discussion about the relative costs and benefits of commercial surveillance must discuss the assumptions that underlie the proliferation of targeted, behavioral, and cross-contextual advertising. Targeted advertising, discussed above as an example of both personalization and influencing, is a much-debated and critically important example of commercial surveillance, given its role in the rise of prevalent digital tracking. The basic logic offered to defend targeted advertising, as explained above, is that consumers see more "relevant" ads, advertisers benefit from higher sales, publishers fund their content through higher ad sales, and everyone benefits from a free and accessible internet. Such axioms have long justified the spread of increasingly sophisticated targeting online. In reality, however, things are more complicated.

a. Ad-tech Middlemen Disproportionately Benefit Relative to Advertisers and Publishers

While advertising generally may be procompetitive, it does not necessarily follow that targeted advertising is procompetitive. For such an omnipresent practice, one would expect strong empirical justifications to prove the value that this service provides to consumers, platforms, and the digital economy as a whole. The reality is that advertisers sell advertising, and the benefits of targeted, behavioral, and cross-contextual advertising have been exaggerated at best and fabricated at worst.[243] Digital advertising is a huge industry, with some estimates placing the current market value at $350–600 billion.[244] But the benefits of that industry disproportionately flow to a select few industry actors, leaving consumers and publishers left wondering how this arrangement benefits them.[245] Accountable Tech, in its petition to the Commission calling for rulemaking to

---

[243] *See* Sam Biddle, *Facebook Managers Trash Their Own Ad Targeting in Unsealed Remarks*, INTERCEPT (Dec. 24, 2020, 9:00 AM), https://theintercept.com/2020/12/24/facebook-ad-targeting-small-business (describing how internal Facebook documents cast doubt on the reliability of the platform's ad targeting, especially as it relates to small businesses); Andrew Hutchinson, *New Study Finds Facebook's Interest Targeting Is Inaccurate Around 30% of the Time*, SOCIAL MEDIA TODAY (Mar. 28, 2022), https://www.socialmediatoday.com/news/new-study-finds-facebooks-interest-targeting-is-inaccurate-around-30-of-t (describing the results of a study which found that "around 30% of Facebook's inferred interests are inaccurate or irrelevant).

[244] ReportLinker, *Global Digital Advertising and Marketing Market to Reach $786.2 Billion by 2026*, GLOBE NEWS WIRE (May 4, 2022, 8:19 AM), https://www.globenewswire.com/news-release/2022/05/04/2435674/0/en/Global-Digital-Advertising-and-Marketing-Market-to-Reach-786-2-Billion-by-2026.html (predicting global advertising spending near $350 billion); Ethan Cramer-Flood, *Worldwide Ad Spending 2022*, INSIDER INTELLIGENCE (May 18, 2022), https://www.insiderintelligence.com/content/worldwide-ad-spending-2022 (predicting $600 billion digital ad spend by 2022).

[245] According to some estimates, ad-tech middlemen pocket 50% of all money spent on digital advertising. Dr. Augustine Fou, *Billions Spent On Digital Ads, And You're Not Sure?*, FORBES (Jan. 31, 2021, 12:18 PM), https://www.forbes.com/sites/augustinefou/2021/01/31/billions-spent-on-digital-ads-and-youre-not-sure ("How much of your digital ad dollar goes towards showing ads? . . . Sometimes that is hard to determine due to the complexity of the programmatic supply chain. There are many middlemen taking their cut whether they add any

prohibit surveillance advertising, detailed many of the ways in which commercial surveillance and targeted advertising disproportionately benefit a select number of actors (the dominant surveillance advertising firms) in the advertising industry, to the detriment of advertisers, publishers, consumers, and commerce itself.[246] Advertisers are harmed by platforms and publishers who inflate metrics and defraud advertisers.[247] Publishers have perverse incentives to increase traffic and juice ad impressions however they can, including by buying "rewarded inventory" on mobile games.[248] Publishers also suffer under this system. Dominant platforms have superior targeting capabilities—they possess vast "user bases" and can use their control over choice architecture to extract vast amounts of human information from those human "users."[249] That superior targeting capacity enables those platforms to siphon profits from digital advertising, leaving little value added for publishers.[250] According to one recent study, publishers may only see as little as a 4% increase in value added from cookies and behavioral advertising, roughly $0.00008 per advertisement.[251] That shocking disparity between the ever-increasing value of the digital advertising industry and the value added to publishers demonstrates how the commercial benefits of commercial surveillance disproportionately flow to a small handful of actors. This outcome, where profits grow year over year but those gains are realized only in an increasingly small subset of actors, is not good for consumers, competition, or commerce. (Q40.)

---

value or not. What IS known is that at least half of your dollar goes to such ad-tech middlemen, instead of to the publisher for showing ads. . . . Three industry-wide studies since 2016 have all confirmed that at least 50% of every dollar goes into middlemen's pockets and not to the publisher for showing ads. What's worse is that on average 15% of the dollars 'went missing.'"); *see also* Gilad Eldelman, *Ad Tech Could Be the Next Internet Bubble*, WIRED (Oct. 5, 2020, 8:00 AM), https://www.wired.com/story/ad-tech-could-be-the-next-internet-bubble (citing Alex Barker, *Half of Online Ad Spending Goes to Industry Middlemen*, FIN. TIMES, (May 5, 2020), https://www.ft.com/content/9ee0ebd3-346f-45b1-8b92-aa5c597d4389); *see generally* TIM HWANG, SUBPRIME ATTENTION CRISIS (2020).

[246] *See generally* Accountable Tech, *Accountable Tech Petitions FTC to Ban Surveillance Advertising as an 'Unfair Method of Competition'* (Sept. 28, 2021), https://accountabletech.org/media/accountable-tech-petitions-ftc-to-ban-surveillance-advertising-as-an-unfair-method-of-competition.

[247] ACCOUNTABLE TECH, PETITION FOR RULEMAKING TO PROHIBIT SURVEILLANCE ADVERTISING 6 (Sept. 2021), https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf; *see also* HWANG, *supra* note 245245 (describing the ways in which powerful digital advertising intermediaries inflate metrics and resist third-party auditing).

[248] *See, e.g.*, Ryan Barwick & Jen Brice, *Major Publishers Are Buying Ads in Mobile Games Like 'Subway Surfers' to Juice Traffic*, MKTG BREW (Aug. 11, 2022), https://www.marketingbrew.com/stories/2022/08/11/major-publishers-are-buying-ads-in-mobile-games-like-subway-surfers-to-juice-traffic.

[249] *See supra* Part I.B.2, describing how profiling and sorting can be combined with nudges to enable manipulation which facilitates even greater data collection and control.

[250] ACCOUNTABLE TECH, *supra* note 247247.

[251] Veronica Marotta, Vibhanshu Abhishek & Alessandro Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis* (May 2019) (unpublished manuscript), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf ("Our analysis finds that, after accounting for other factors (including those that may be used for non-behavioral forms of targeting, such as visitors device information or geolocation), when the user's cookie is available publisher's revenue increases by about 4%. The increase is significant from a statistical perspective. Nevertheless, from an economic perspective, the increase corresponds to an average increment of just $ 0.00008 per advertisement.").

Just because benefits flow disproportionately to industry, it does not follow that these are benefits to commerce. In fact, many scholars have demonstrated that digital platforms are characterized by a lock-in effect. Dominant platforms lock-in consumers, extract data, cultivate extensive profiles on those consumers, aggregate behavioral insights, develop "hyper-personalized content" that optimizes engagement, and then repeat the cycle.[252] This lock-in effect leads to degradation of products, as ads become more prevalent and consumers have less control over the products they use, enabling dominant platforms to increase costs on advertisers and publishers.[253] Through the introduction of substantive limits on data collection and targeted advertising, the Commission can break this vicious cycle, enhance competition, and improve the quality of digital services. (Q27, Q40, Q41, Q42.)

b. Targeting Threatens Consumer Autonomy, Imposes Costs in Terms of Data and Attention Extraction, and Harms Society

The proliferation of targeted, behavioral, and cross-contextual advertisements online has largely been premised on two alleged benefits to consumers: (1) the ads that consumers see are more "relevant" to them, which in turn improves their user experience; and (2) targeted advertisements enable a "free" internet to exist, saving consumers from paying subscription fees for every item of content they wish to enjoy. Both of these alleged benefits are problematic, and neither stand up to close scrutiny. Both of these alleged benefits are framed in ways which minimize or erase the direct and indirect harms which can flow from targeted advertising to consumers.

The idea that consumers benefit from seeing more "relevant" ads fails to account for the direct harms that consumers suffer from this kind of precise targeting. Targeting creates risks of loss of agency and autonomy. Consumers understand that their data will be tracked when they are online, but they often do not grasp the extent to which their data is being collected and utilized to profile, sort, and manipulate them. When companies create detailed behavioral profiles about consumers, exploit cognitive biases, and effectively deploy targeted advertisements to influence them, those companies gain an economic advantage. [254] This gives companies a strong incentive to collect as much data as they can.[255] One study found that ninety-one percent of Americans feel they have lost control over how their data is being collected and used by companies.[256] That loss of control reflects the injury that targeting inflicts on consumer autonomy. As documented above, tracking facilitates powerful behavioral interventions which diminish consumer choice.[257] Another

---

[252] ACCOUNTABLE TECH, *supra* note 247,247 at 20; *see generally* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017) (describing how Amazon's successful use of the lock-in effect has undermined competitors and increased consumer retention).
[253] ACCOUNTABLE TECH, *supra* note 246,247 at 20.
[254] *See generally* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).
[255] Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 113 HARV. L. REV. 497 (2019).
[256] Maurice Stucke & Allen Grunes, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, ANTITRUST SOURCE (APR. 2015), https://ir.law.utk.edu/cgi/viewcontent.cgi?article=1777&context=utklaw_facpubs (citing Mary Madden, PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 3 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf).
[257] *See supra* Part I.B.2; ACCOUNTABLE TECH, *supra* note 246,247 at 6.

issue with the assumption that showing consumers more "relevant" ads is necessarily a good thing for them is that it is not clear what everyone means when we talk about showing consumers more "relevant" ads. To whom are these ads are more relevant? We would submit that these ads are more relevant to advertisers rather than to consumers. Ads are only more relevant to consumers if they get at what those consumers actually want, (or, maybe more accurately, what is in a consumer's calmly calculated actual benefit rather than feeding their id), not what consumers can be manipulated into agreeing to. One way in which companies influence consumers through targeting is price discrimination, a tactic companies use to offer a product at various prices depending on the individual consumer.[258] Companies track consumer spending habits and offer "special offers" to consumers whom the companies have determined will buy a product if those consumers believe they are getting a good deal. Although that arrangement provides benefits to consumers in select transactions, the tradeoffs are not worthwhile in the long run. We have built an all-encompassing, comprehensive, always-on surveillance network just to get people to click more.[259] Companies infringe on our privacy for financial gain, manipulating consumers and the market with little to no ability from consumers to pushback or avoid these outcomes.[260] Trading privacy preferences for a company's ability to target consumers directly is not worth it for the consumer, especially when alternative advertising methods can be utilized to keep company profits where they are, while affording consumers the privacy protections they require.

The second supposed benefit of targeted advertising from a consumer perspective is that targeted advertising fuels a "free" internet, saving consumers from having to pay subscription and access fees to enjoy the majority of digital content.[261] Reducing socioeconomic barriers to internet access is an extremely important goal and we should not lose sight of that, but policymakers must also account for the myriad ways in which targeted advertising imposes costs on consumers and the alternatives which would be implemented in lieu of targeted ads, such as contextual ads. As Chris Hoofnagle and Jan Whittington explain, digital content is not "free"[262]: although there may not be a monetary fee to access content, consumers pay for these services and content with their personal data, attention, and time.[263] These companies extract personal data, ignore consumer privacy preferences, and command their attention.[264] Not only do consumers pay for internet use in the form of attention and data, targeted advertising imposes costs on publishers and advertisers as well. Companies using targeted advertising hope to benefit from higher sales, an increased consumer base, and lower marketing and advertising costs by focusing their spending on relevant consumers. However, there is evidence that targeted advertising is less cost-efficient than alternatives such as contextual advertising. The cost of targeted advertising may be greater where

---

[258] Yan, *supra* note 102, at 7.
[259] *See* HWANG, *supra* note 245. Ethan Zuckerman, *The Internet's Original Sin*, THE ATLANTIC (Aug. 2014), https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041.
[260] Calo, *supra* note 254. Ethan Zuckerman, *The Internet's Original Sin*, THE ATLANTIC (Aug. 2014), https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041.
[261] *See generally* Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price,* 61 UCLA L. REV. 606 (2014).
[262] *Id.*
[263] Hoofnagle & Whittington, *supra* note 261; *accord* ACCOUNTABLE TECH, *supra* note 247, at 6.
[264] ACCOUNTABLE TECH, *supra* note 247,247 at 6–7.

companies rely on third-party firms, such as data brokers, to buy consumer data or distribute their ads on platforms who charge a higher premium for targeted ads.[265] While some companies may see decreased ad spending by using leveraging data tactics, many are likely to see an increase if they are not already paying to track user data and distribute targeted ads themselves due to firms having increased market power in this area.[266]

c. Contextual Advertising is a Viable Alternative for Companies and Consumers

Targeted advertising is not the only option companies have to reach consumers. Contextual advertising—which matches advertisements with the content of the page rather than the viewer of the advertisement[267]—is a trust-preserving form of targeting which has withstood the test of time. Contextual advertising benefits consumers, publishers, and advertisers without betraying consumer trust and without resorting to prevalent commercial surveillance. As Jack Balkin points out, contextual advertising does not require "an elaborate digital dossier about [you] to be effective."[268] Instead, organizations pay to have their ads displayed on various pages relevant to what they are advertising. Contextual advertising was an important advertising tool prior to the rise of the information economy and commercial surveillance, and it has made a resurgence in recent years as discussions of online privacy have become more common. Another virtue of contextual advertising relative to targeted and behavioral advertising, in addition to preserving consumer trust, is that it is more cost-efficient for advertisers.[269] Critics have argued that contextual advertising is not viable in select circumstances, such as where brand integrity would be damaged by the content of a news article. It is not clear that this will be the case. For example, consumers are likely to understand that contextual ads target a particular publisher's readership rather than the content of specific stories.[270] Furthermore, different advertisers have different tolerances when it comes to brand integrity. (Q42.)

With contextual advertising as a viable alternative to targeting, substantive limits on targeted, behavioral, and cross-contextual advertisements are not an existential threat to either the advertising industry or the notion of a "free" internet. Consumers can still receive relevant ads while also enjoying stronger privacy protections that are more consistent with their preferences. Industry members, including publishers, advertisers, and ad-tech middlemen, can still create value-generating advertising campaigns which are potentially more cost-efficient than targeting.

---

[265] Yan, *supra* note 102, at 5.
[266] *See generally* Calo, *supra* note 254.
[267] Brook Shepard, *The New Rise of Contextual Advertising*, FORBES (July 22, 2021, 7:20 AM), https://www.forbes.com/sites/forbesagencycouncil/2021/07/22/the-new-rise-of-contextual-advertising.
[268] Balkin, *supra* note 54,54 at 28.
[269] GUMGUM HQ, UNDERSTANDING CONTEXTUAL RELEVANCE AND EFFICIENCY: A COMPARISON OF CONTEXTUAL INTELLIGENCE VENDORS AND BEHAVIORAL TARGETING (2020), https://insights.gumgum.com/hubfs/DAN%20Research%20Study/GumGum%20Contextual%20Research%20Paper-1.pdf.
[270] *See* Jenn Chen, *Fostering Advertising with Greater Integrity*, ASS'N. NAT'L ADVERT. (Sept. 22, 2022), https://www.ana.net/miccontent/show/id/ii-2022-09-fostering-advertising (describing how contextual advertising presents an opportunity for advertisers to "finance diverse voices, reward publishers who uphold high journalistic standards and move beyond an era of advertising driven by personal data often collected without consumer consent").

Policymakers are already taking notice of the value of contextual advertising as an alternative. For example, California's CCPA grants consumers the right to opt out of cross-contextual behavioral advertising, defined as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."[271] California's substantive restrictions on cross-contextual advertising serve both as evidence that alternative advertising methods are viable and that industry has had ample time to begin preparing for a post-targeting world. (Q42.)

***

Commercial surveillance is a complex phenomenon, involving a diverse range of market actors, business practices, and individual and social harms. Despite that challenge, the Commission is correct both to label these practices as commercial surveillance and to treat them as a fitting subject for investigation and potentially regulation. Commercial surveillance accurately describes the power dynamic that shifts between the platforms, companies, and merchants employing these practices and the vulnerable, trusting humans who are left exposed. These practices are highly prevalent, and consumers undoubtedly experience the real and substantial injuries they inflict. Commercial surveillance results in disproportionate dangers and meager benefits for consumers. In contrast, the profits of this surveillance economy flow to a small subset of market actors. Consumers crave—and demand—privacy. But no protection will come so long as market incentives push companies to maximize data harvesting, at the expense of their vulnerable, trusting human customers. Consumers need substantive rules which go beyond mere procedural protections, and the Commission's Section 5 authority is the appropriate vehicle with which to consider providing such protections. This is particularly the case because, as we explain in the next section, the default "notice and choice" model of privacy regulation used to date has failed to protect consumers.

II. Notice and Choice Has Failed

For nearly five decades, privacy regulation in the United States has come largely in the form of "notice and choice."[272] These bedrock elements of the venerable Fair Information Practices (FIPs) are often implemented and enforced weakly in practice, leading to fictitious notice and illusory choice. But even zealous adherence to the FIPs would fail to fully protect consumers because the FIPs are largely procedural. Unfairness, in contrast, is a substantive issue. Rights of "notice, access, and consent regarding the collection, use and disclosure of personal data" theoretically allow people to decide for themselves how to weigh the costs and benefits of commercial surveillance, something Daniel Solove has termed "privacy self-management."[273] Empowering individuals to make decisions about how to manage their data is a laudable goal, but

---

[271] CAL. CIV. CODE § 1798.140(k) (West 2022) (effective Jan. 1, 2023); s*ee also* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 204(c) (2022) (proposing a right for consumers to opt out of targeted advertising).

[272] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882 (2013) (tracing the origins of notice-and-consent to the advent of the Fair Information Practices in 1973).

[273] *Id.* at 1880.

experience has taught that this is a futile endeavor when it is the sole regulatory effort. This is particularly the case in the complex modern digital marketplace in which consumers may have relationships with dozens or hundreds of platforms, companies, and merchants. Privacy control as an ideal is illusory, overwhelming, and myopic.[274] No matter what reservations we have or what care we take, there is no way to get things done in the digital age without exposing our data to third parties; "[n]o other way to reserve the hotel room or seat on the plane, to file the IRS form, to recall the library book, or to send money to our loved one in prison."[275] Failures of human psychology and design choices by companies offer the seductive illusion of control in theory where none exists in reality. Consumers interact with a staggering number of apps and websites on a daily basis. Exercising meaningful control over privacy with all of those services would occupy literally all of a consumer's time and willpower. Finally, an individual's privacy choices impose externalities on others which are ignored under a "control" theory. The Commission should evaluate the effectiveness of notice and choice by the reality which has evolved under this regime: the prevalence of harmful data practices, unfettered commercial surveillance, and "privacy nihilism" experienced by consumers. Measured against those effects, it becomes apparent that notice and choice is an abject failure as a result of its many structural, psychological, and legal defects. (Q73.)

Before delving into the failures of notice and choice, it is important to clarify that a rejection of notice and choice is a rejection of the *overreliance* on consent as a legal mechanism rather than a rejection of either notice or consumer choice as elements of a properly functioning consumer market. Companies need to continue providing notice of their data practices because transparency is critical for trust to flourish in markets, even if any individual consumer is unlikely to be able to understand what is actually going on. Nevertheless, recognizing the value of notice and choice and individual concepts does not justify relying on notice and choice as the sole or most prominent privacy regulatory measure. Opponents of regulation glorify the empowering nature of notice and choice and decry criticisms of that regime as a rejection of consumer choice and free agency. But in reality, moving on from notice and choice offers the only chance of truly empowering people to freely interact in a marketplace. The difference lies in the distinction between choice and consent. Choice is less consequential than consent. Choice can mean the ability to elect among a range of reasonable options in an interface, such as selecting a dinner

---

[274] *See* Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423 (2018), https://papers.ssrn.com/abstract_id=3299762; ACLU of Massachusetts, *Rise of the Surveillance State*, FREEDOM UNFINISHED (Sept. 26, 2022), https://www.freedomunfinished.com/1983514/11374637 (statements of Woodrow Hartzog, who is one of the authors of these comments); *see also* Thomas Germain, *I Said No to Online Cookies. Websites Tracked Me Anyway.*, CONSUMER REPORTS (Sept. 29, 2022), https://www.consumerreports.org/electronics-computers/privacy/i-said-no-to-online-cookies-websites-tracked-me-anyway-a8480554809 [hereinafter Germain, *I Said No to Online Cookies*] (describing how companies may still be showing targeted advertisements even after a consumer opts out of tracking on their websites); Thomas Germain, *Apple Is Tracking You Even When Its Own Privacy Settings Say It's Not, New Research Says*, GIZMODO (Nov. 8, 2022, 4:20 PM), https://gizmodo.com/apple-iphone-analytics-tracking-even-when-off-app-store-1849757558 [hereinafter Germain, *Apple is Tracking You*] (describing how Apple—a company who has built a market reputation as being privacy friendly—surveils consumers despite clear promises to enable consumers to opt out of sharing device analytics).

[275] HARCOURT, *supra* note 28, at 14.

option from a menu. Choice can mean selecting between competitors in a marketplace. In that sense, choice flourishes with competition. Consent is different from choice because consent is more than merely choosing; consent is legally consequential whereas choice is not. Consent has a moral and legal significance of accepting a certain set of legal arrangements and certain sets of consequences irrevocably. Consent changes your legal status and orders relationships in ways that are potentially legally and economically significant. As Daniel Solove explains, "Consent legitimizes nearly any form of collection, use, or disclosure of personal data."[276] When companies talk about notice and choice, therefore, what they really mean is notice and consent, because failure to object to using a service can become legal consent for the consequences which come with it. In contrast to that consent-based status quo, these comments envision a better market in which consumers have a range of choices within a trustworthy, largely loyal environment. To truly safeguard choice, consumers need to be protected from disloyal, opportunistic, and exploitative behavior no matter what choices they make. The goal is to maximize consumer choice and then provide a network of protection. Consent does the opposite because consent is a legal mechanism that changes a consumer's legal status based on the choices that they make.

A market that demands consumers grant consent is entirely different from one that merely offer choices. Free, unfettered choice of the sort that industry voices laud can only happen where there is trust—meaningful trust backed up by legal consequences for distrustful and disloyal behavior. The goal should to get to a place that is similar to the fictitious world that companies portray our world as being, one in which consumers are in a vibrant market and can just pick and choose the products and services which will make them happy without fear of betrayal. But that world is not achievable so long as consumers have to keep one hand on their wallets out of fear of being mugged. Only when consumers trust the marketplace can you have the kind of free, unfettered, meaningful, wonderful choice that everyone wants. In the absence of trust, choice is fraught with peril: *caveat emptor*.

A. Privacy Self-Management Has Proven Ineffective, Untenable, and Undesirable

Opt-out choices have not proved effective in protecting against commercial surveillance. Despite strong empirical evidence that consumers desire privacy protections,[277] few consumers read privacy notices on a regular basis, opt out of disagreeable data practices, or adjust their privacy settings online.[278] Daniel Solove has identified several well-known defects that prevent consumers from meaningfully exerting control over their data via privacy self-management and opt-out choices. First, severe cognitive problems undermine privacy self-management, which prevent consumers from making "rational" choices regarding their data.[279] Privacy notices are long and difficult for consumers to understand, yet efforts to make such notices more comprehensible can ultimately reduce how informative they are.[280] Consumers also operate under "woefully incorrect

---

[276] Solove, *supra* note 272,272 at 1880.
[277] LUCAS & STEIN, *supra* note 45 and accompanying text.
[278] *Id.* at 1884, 1886–87.
[279] *Id.* at 1883–88.
[280] *Id.* at 1885.

assumptions about how their privacy is protected."[281] This problem is further compounded by well-known cognitive biases, which companies exploit to nudge consumers into "consenting" to data practices.[282] (Q5, Q73, Q80.)

Second, there are significant structural barriers that render privacy self-management impracticable.[283] These barriers include the vast number of entities collecting and using personal data, as well as the inability of users to weigh costs and benefits because privacy harms often result from the aggregation of data over time rather than discrete moments of collection tied to specific actions. To use the parlance of Silicon Valley, notice and choice cannot scale. Consumers deal with hundreds of online entities per day. The frequency with which they are asked to consent to data practices is overwhelming and exhausting even to the most privacy conscious and well-resourced consumers. The overwhelming demands of such cognitive labor leads consumers to acquiesce to data practices they otherwise would not freely choose, undermining the effectiveness and validity of consent. Furthermore, the problem of scale raises the question of whether it is even economically desirable for consumers to undertake the significant labor and expense of reading and contemplating scores of privacy policies. Such labor at ordinary scale would take literally weeks of full-time labor for every consumer; one 2008 study for example estimated that "it would cost $781 billion in lost productivity if everyone were to read every privacy policy at websites they visited in a one-year period."[284] Given society's increased digitization in the intervening years, that number has unquestionably grown significantly since then. The notice and choice regime therefore leads to different undesirable outcomes. Either consumers are not actually engaging in privacy self-management, which begs the question of why we persist with that fiction at all, they are trying to manage their privacy but at a significant social cost, or they are stuck somewhere in between with the worst of both worlds. (Q5, Q73, Q80.)

Another structural problem with privacy self-management that raises issues of both scale and opacity is the problem of data brokers. A vast array of data brokers and other "reservoirs" of data exist which traffic in consumer data in opaque and often invisible ways.[285] That entire industry embodies the failures of notice and choice, as consumers are both largely unaware of the existence of these entities and also lack any reasonable means of avoiding their ability to collect, use, and disseminate their personal information.[286] Then there is the problem of aggregation, i.e., that

---

[281] *Id.* at 1886.
[282] *Id.* at 1887–88.
[283] *Id.* at 1888–93.
[284] *Id.* at 1889 (citing Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 564 (2008)).
[285] *Id.* at 1889 (citing Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 243–51 (2007)).
[286] In one salient example, geolocation data broker Copley Advertising, LLC delivered anti-abortion advertisements to pregnant persons in reproductive care clinics. Justin Sherman, *The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics*, LAWFARE (Sept. 19, 2022, 8:31 AM), https://www.lawfareblog.com/data-broker-caught-running-anti-abortion-ads%E2%80%94-people-sitting-clinics. The Massachusetts attorney general preemptively obtained a settlement with Copley Advertising under the state's UDAP statute. *Id.* This kind of surveillance is invasive: "Citizens do not reasonably have any knowledge of third-party companies that quietly surveil their locations and then monetize the data on the open market. . . . Even if consumers were aware this was

disclosing information might reasonably seem innocuous at the time of disclosure but become harmful as a critical mass of data is aggregated later in time.[287] Modern data analytics enables companies to "deduce extensive information about a person" from such seemingly innocuous data points.[288] This possibility further undermines the premise of privacy self-management, because consumers are unable to assess the risks and benefits involved with revealing a piece of information (or agreeing to vague and buried terms relating thereto) without knowing how that information might be combined with past and future disclosures.[289] Related to the problem of aggregation is the timeframe in which consumers are asked to make these decisions. Immediate benefits of using a particular service are salient, whereas risks of collection, use, or disclosure of data often occur far off into the future and in ways which are less apparent to consumers.[290] These effects combine to direct consumers into agreeing to data practices which may not be in their actual rational interest. (Q5, Q73, Q80.)

A final challenge with relying on privacy self-management that we would like to highlight is that, due to its overly myopic focus on individual privacy decisions, it fails to internalize important social benefits and costs of privacy. Privacy is essential to our cultural development, as "[s]tunting individual creativity and intellectual development impoverishes society at large."[291] Privacy from both the state and private actors is necessary for intellectual freedom and the development of new ideas.[292] These larger social values are implicated by infringements on individual privacy, but privacy self-management does not account for these broader social consequences. (Q73, Q80.)

B. Several Well-Known Pathologies Thwart Effective Consent to Commercial Surveillance

In addition to the general flaws of privacy self-management identified above, digital consents can be faulty and ineffective in a number of well-documented ways. These "pathologies of consent,"[293] further demonstrate the ways in which opt-out choices have not repeatedly proven ineffective in protecting against commercial surveillance despite strong consumer preferences for meaningful privacy. Each of these pathologies, which are pervasive in digital environments, removes either the "knowing" or "voluntary" dimensions of meaningful consent. (Q73, Q80.)

---

happening, it does not mean they understand how companies and other actors are using their data—and it does not change the fact that those companies and actors can use the data to harm people." *Id.*

[287] Solove, *supra* note 272,272 at 1889–91.

[288] *Id.* at 1889–90.

[289] *See* CITRON, *supra* note 31, at 3 ("Companies have convinced us to give away out intimate data without strong privacy commitments. They wield formidable powers of persuasion and seduction, so individuals end up sharing far more personal data than they realize. Companies know that people can't appreciate the potential perils because the risks from data collection often materialize in the future.").

[290] *Id.* at 1891.

[291] *Id.* at 1892 (citing Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1918 (2013)).

[292] *Id.* at 1892–93 (first citing Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008); then citing Richards, *supra* note 28,28 at 1946, 1951).

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

The first of these pathologies is the problem of *unwitting consent*, which occurs where consumers do not "know what data practices are possible, what they have agreed to, or what the informational risks of the transactions are."[294] Unwitting consent can take several forms. Consumers can "fail to understand the *legal agreement* governing the information relationship they now have with the company," which can occur where the agreement is too long, uses confusing language, is too technical, or is too vague.[295] Consumers also may not adequately understand the *technology* which mediates their relationship with the company, such as when consumers overestimate the security of telecommunications systems or consent is "manufactured through obfuscation, abstraction, and sleight of hand via a user interface."[296] Consumers might also fail to understand the *consequences* or risks of the informational relationship.[297] Humans generally struggle to assess future risks created by present decisions,[298] and this problem is only worsened in the context of data practices. A person asked to consent to the collection of biometric data is unlikely to foresee the downstream risks of harassment, stalking, or discrimination—much less the creation of prevalent or ubiquitous facial recognition tools.[299] Data analytics and advertising surveillance also entail risks which are hard to foresee, such as the generation of inferences (and subsequent targeting) based upon sensitive characteristics.[300] Notice and choice advocates argue that unwitting consent can be remedied by greater information disclosure. This argument fails to understand the insights raised in Solove's critique of privacy self-management—namely that making notices more comprehensible either makes them less informative or more burdensome to read and that truly reading and engaging with notices would be extremely wasteful.[301] Greater information disclosure is also undermined by the pervasiveness of dark patterns, where companies use choice architecture and the insights of behavioral science to prey on consumers' predictable cognitive biases.[302] (Q73, Q80.)

A second pathology of consent comes in the form of *coerced consent*, which occurs where a consumer's choice is not truly voluntary.[303] Coercion underlies the failure of notice and choice in several ways, such as "mediated environments that manufacture consent" which are coercive in

---

[294] *Id.* at 1478.
[295] *Id.* at 1479–80 (emphasis added).
[296] *Id.* at 1480–81. Facebook's lack of clear boundaries between its own site and third-party apps is a salient example of consumers being unable to appreciate the risks at hand. *Id.* at 1482–84. Another prominent example is third-party tracking via advertising technology, which involves complex real-time processing of personal data to serve ads personalized on the basis of that data. *Id.*
[297] *Id.* at 1484.
[298] *Id.* (first citing Caroline Beaton, *Humans Are Bad at Predicting Futures That Don't Benefit Them*, ATLANTIC (Nov. 2, 2017), https://www.theatlantic.com/science/archive/2017/11/humans-are-bad-atpredicting-futures-that-dont-benefit-them/544709; then Kate Morgan, *Why You're So Bad at Predicting the Future*, MEDIUM (Jan. 3, 2019), https://medium.com/s/2069/why-youreso-bad-at-predicting-the-future-68e14a5f41a4; then Bruce Schneier, *Why the Human Brain is a Poor Judge of Risk*, WIRED (Mar. 22, 2007), https://www.wired.com/2007/03/security-matters0322).
[299] *Id.* at 1485.
[300] *Id.* at 1485–86.
[301] *See supra* Part II.A.
[302] *See infra* Part II.C.
[303] Richards & Hartzog, *supra* note 293, at 1486–90.

"manipulative and subtle ways."[304] As a starting point, it bears repeating that presence on the internet is a prerequisite for participation in modern society;[305] the internet is a vital means of participating in commerce, communicating with fellow humans, and even utilizing vital government services. Furthermore, consumers often lack meaningful choice over which companies to interact with, especially at the ISP and platform levels.[306] Choice and bargaining are extremely limited for consumers in digital environments. This problem is further compounded by the rise of dark patterns. Digital environments are entirely constructed and mediated by platforms.[307] Under a notice and choice regime, designers have strong incentives to craft interfaces which shape and influence consumer decision-making in privacy-invasive ways. Discussed in greater detail below,[308] these interfaces are used to "coerce, wheedle, and manipulate people to grant [consent]."[309] (Q73, Q80.)

Finally, there is *incapacitated consent*, which involves situations where consent is not traditionally possible as a matter of law.[310] Children are a great example of where consent is unavailable due to incapacity under the law. The Commission's COPPA Rule recognizes this and requires operators to "[o]btain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children" under the age of 13.[311] Despite the COPPA Rule's narrow focus on children under the age of 13, many of the Rule's justifications are equally true of children aged 13–18 (and, as we argue below, adults as well). The age of contractual consent in the US is 18, yet paradoxically we allow teenagers to "consent" to data practices. This raises questions about the effectiveness and desirability of consent in those situations. (Q18, Q73, Q80.)

C. Manipulative Interface Design and Dark Patterns Are Pervasive Barriers to Effective Consent

The relationships between design, choice, and consent are significant enough to warrant their own discussion. Design, defined broadly to include "the work of engineers as well as other designers such as those who do product design, graphic design, user interface and user experience design,"[312] is critical to the consumer experience. Design encompasses "how a system is architected, how it functions, how it communicates, and how that architecture, function, and communication affects people."[313] Design choices "channel user choice," "shape user expectations,"[314] and can make people vulnerable to both companies as well as other users.[315] One of the reasons design is important is because it determines both the default settings and the range

---

[304] *Id.* at 1486.
[305] *Id.* at 1487.
[306] *Id.*
[307] *See supra* Part I.B.1 discussing influence as a category of commercial surveillance methods.
[308] *See infra* Part II.C.
[309] Richards & Hartzog, *supra* note 293,293 at 1489.
[310] *Id.* at 1490–91.
[311] 16 C.F.R. § 312.3(b) (2022); Richards & Hartzog, *supra* note 293,293 at 1490.
[312] HARTZOG, *supra* note 8,97 at 11.
[313] *Id.* at 12.
[314] *Id.* at 5.
[315] *Id.* at 13.

of choices available to us. For example, "[s]imply moving around a city with a cell phone or other digital device may produce lots of information about us."[316] It is well understood now that "entities who can control how choices are structured can also control, at least at the margins, what decisions humans make."[317] Design tricks and psychological engineering are nothing new, but these tactics have grown more sophisticated and harmful in the context of modern commercial relationships.[318] Digital environments are constructed and shaped by companies, giving them increased control over choice architecture. Consumers also struggle to differentiate between apps and software which are secure and privacy-protective and those which are not.[319] Recognizing this power, "[m]any companies design their interfaces to facilitate and encourage the disclosure of information, including information we may not even be aware we are disclosing. . . . They also use algorithms to monopolize our attention and keep us fixed to the site so that we will disclose even more information."[320] User interfaces can be designed in such a way as to create unwitting consent by obfuscating what it is consumers are consenting to or hiding the option to decline.[321] Sometimes, controls are outright deceptive and fail to do what they promise.[322] Consistent with this observation, the Commission's recent report on dark patterns is replete with examples of manipulative design practices which extract copious amounts of user data.[323] (Q73.)

Placing the onus of privacy protection on consumers rather than requiring software and hardware makers to respect privacy in the design of their products ignores the ways in which popular digital tools are designed to expose people and manipulate consumers into disclosing personal information. Under a notice and choice regime, "there are overwhelming incentives to design technologies in a way that maximizes the collection, use, and disclosure of personal information."[324] Whether known as "malicious design," "dark patterns," or something else, design choices of this type exemplify the ways in which notice and choice fails to protect consumers from exploitative data practices.

---

[316] Balkin, *supra* note 54,54 at 12 (citing Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html).
[317] Richards & Hartzog, *supra* note 16,16 at 974–75.
[318] FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT 1 (2022).
[319] Richards & Hartzog, *supra* note 16,16 at 974–75.
[320] Balkin, *supra* note 54,54 at 12.
[321] Richards & Hartzog, *supra* note 293,293 at 1480–81.
[322] Germain, *I Said No to Online Cookies*, *supra* note 274274 ("The websites and their advertising partners were tracking me for targeted ads even though I'd taken the time to tell them not to—using the tools the companies themselves had provided."); Germain, *Apple is Tracking You*, *supra* note 274 ("Tommy Mysk and Talal Haj Bakry, two app developers and security researchers at the software company Mysk, took a look at the data collected by a number of Apple iPhone apps—the App Store, Apple Music, Apple TV, Books, and Stocks. They found the analytics control and other privacy settings had no obvious effect on Apple's data collection—the tracking remained the same whether iPhone Analytics was switched on or off."). Apple's deceptive tracking practices are already the subject of a class action lawsuit. Thomas Germain, *Apple Sued for Allegedly Deceiving Users With Privacy Settings After Gizmodo Story*, GIZMODO (Nov. 11, 2022, 8:09 PM), https://gizmodo.com/apple-iphone-privacy-analytics-class-action-suit-1849774313.
[323] *See generally* FED. TRADE COMM'N, *supra* note 318318.
[324] HARTZOG, *supra* note 8,40 at 5.

At a time when the effects of social media on our mental health—especially the mental health of children and teenagers—is under exacting scrutiny,[325] popular social media app TikTok provides a useful example of the power of design to exploit consumer vulnerabilities. With over one billion average monthly users, TikTok has become a major social media platform and rival to many of the industry's biggest actors.[326] TikTok's precise tracking of consumer viewing habits enables it to deliver highly personalized content, but this is not the only design feature that makes TikTok addictive.[327] Beyond the app's powerful content recommendation algorithms, the company's explosive growth is tied to its manipulative user experience design, which "is built to trigger compulsive use, especially in more impressionable audiences such as teenagers."[328] The "For You" page, which immediately immerses a consumer in a feed of tailored videos, is a stark contrast to the kind of network-based content of other social media such as Facebook.[329] The use of full portrait mode, the near lack of a progress bar or other similar indicators, and the autoplay "endless scroll" are all designed to create "full immersion and the optimization for maximal consumption."[330] Videos are commonly filmed and displayed as vertical-video monologues, imitating the intimate experience of video chatting with someone directly.[331] Consumers using TikTok are also prohibited from scrolling quickly and bypassing several videos at once—the interface is consciously designed so that they must scroll through each video in their feed.[332] Even the culture of the app, revolving around micro-trends, encourages constant engagement and involvement.[333] These design features achieve their goal: TikTok boasts over one billion users, and the average American viewer watches 80 minutes of TikTok per day.[334] (Q17.)

TikTok also relies on now commonplace design features, such as the use of likes and subscribers to capture consumer attention via dopamine hits or intermittent reinforcement loops, to keep people addicted to its service.[335] Beyond its efforts to keep people as engaged and addicted as possible, TikTok also "uses deceptive design to make users share more data than they would do if that had more information." For example, during the sign-up process TikTok asks the compound

---

[325] Alvaro Bedoya, Comm'r, Fed. Trade Comm'n, "Who is being left behind?": Enforcement Priorities for a Tech Consumer Protection Agenda (Aug. 9, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/who_is_being_left_behind_-_naag_presidential_summit.final_.public_version.pdf.

[326] *I Was on TikTok for 30 Days: It Is Manipulative, Addictive and Harmful to Privacy*, PRIVACY WHISPERER (Luiza Jarovsky), July 28, 2022, https://theprivacywhisperer.substack.com/p/i-was-on-tiktok-for-30-days-it-is [hereinafter Jarovsky, *I Was on TikTok for 30 Days*]. *See generally* Drew Harwell, *How TikTok Ate the Internet*, WASH. POST (Oct. 14, 2022, 5:00 AM), https://www.washingtonpost.com/technology/interactive/2022/tiktok-popularity (detailing TikTok's rise from "sill dance-video fad" to "one of the most prominent, discussed, distrusted, technically sophisticated and geopolitically complicated juggernauts on the internet").

[327] This tracking includes "what you are seeing and how many seconds you stop on each video." *Id.*

[328] *Id.* (emphasis omitted).

[329] *Id.*

[330] *Id.*

[331] Harwell & Lorenz, *supra* note 237237.

[332] Jarovsky, *I Was on TikTok for 30 Days*, *supra* note 326326.

[333] *Id.*

[334] Harwell, *supra* note 326326.

[335] Jarovsky, *I Was on TikTok for 30 Days*, *supra* note 326326.

question, "Are you over 18 and do you allow TikTok to show personalized ads?"[336] Any lawyer who has taken a deposition knows how duplicitous a question like this is. Users who are over 18 and want the content algorithm to treat them as such may feel compelled to consent to personalized ads in this situation. There are other, subtler elements of deception. The "Yes" button is emboldened, whereas the "No" is in a lighter font—a classic dark pattern. The prompt "Confirm you are above 18 and allow personalized ads" is broken up onto two lines, burying the request for personalized ads under the question about being 18. TikTok registrants—no doubt eager to click through to start using the app—will see the top line, gloss over the rest, and accept to confirm their age, not realizing that they are agreeing to more. These features highlight the importance of design for consent, privacy, and consumer wellbeing. TikTok is in control of what its customers see, how they navigate content, and how they interact with one another. TikTok leverages that control to spur compulsive use, optimizing and personalizing their service in order to "steal as much attention as it can."[337]

TikTok's addictive design decisions directly precipitate substantial injuries to consumers. As children globally "spend an average of 75 minutes per day on TikTok,"[338] there is increasing evidence that social media has an especially harmful effect on the mental wellbeing of children and teenagers.[339] There are also significant concerns regarding TikTok's privacy policies and practices. TikTok has been accused of spying on keystrokes[340] and engaging in "aggressive data harvesting."[341] Lingering concerns remain regarding "surveillance, spying and censorship from China."[342] Finally, children and teenagers are exposed on the app in several different ways. "Sharenting," where parents excessively document their child's life on social media, is rife on the app as parents trade their child's privacy for the potential of fleeting moments of virality.[343] This exposure increases the risk of identity fraud, child predation, or cyberbullying, and it often occurs without meaningful consent.[344] Children and teenagers on TikTok (as well as other social media platforms) unintentionally expose themselves to "malicious individuals and predators online."[345]

---

[336] *Id.*
[337] *Id.*
[338] *Id.*
[339] Alvaro Bedoya, Comm'r, Fed. Trade Comm'n, *"Who is being left behind?": Enforcement Priorities for a Tech Consumer Protection Agenda* (Aug. 9, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/who_is_being_left_behind_-_naag_presidential_summit.final_.public_version.pdf (citing
[340] Jarovsky, *I Was on TikTok for 30 Days*, *supra* note 326326 (citing Zak Doffman, *Warning—Apple Suddenly Catches TikTok Secretly Spying on Millions of iPhone Users*, FORBES (June 26, 2020, 1:46 AM), https://www.forbes.com/sites/zakdoffman/2020/06/26/warning-apple-suddenly-catches-tiktok-secretly-spying-on-millions-of-iphone-users).
[341] Data harvesting involves asking for more permissions than is necessary for the app to function, solely to collect more personal data concerning users. *Id.* (citing Rafqa Touma, *TikTok Has Been Accused of 'Aggressive' Data Harvesting. Is Your Information at Risk?*, GUARDIAN (July 19, 2022), https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk).
[342] *Id.*
[343] *Id.*; *see also* Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689 (2013) (describing the perils of "frictionless sharing" and overexposure online).
[344] Jarovsky, *I Was on TikTok for 30 Days*, *supra* note 326.
[345] *Id.*

To be clear, the foregoing discussion is not offered moral condemnation of TikTok. It is offered instead as an example of the practices which naturally evolve in response to the market incentives to monetize consumer data under a notice and choice regime. Like most social media platforms, TikTok makes money from delivering targeted advertisements and sponsored consent.[346] TikTok is also joining the e-commerce industry, attempting to "create a closed loop where TikTok handles each and every step from a user discovering something to actually purchasing it—instead of directing them to an Amazon listing or a Shopify Inc.—powered web store."[347] Both TikTok's ability to addict and enthrall consumers and the substantial injuries that TikTok customers suffer illustrate the inadequacies of notice and choice as the basic data privacy regime in the United States. For better or worse, TikTok has become a center of culture and creativity online. Many people, especially children and teenagers, feel compelled to be on the service, lest they risk social alienation. Platforms like TikTok which embed themselves in the social and cultural fabric of society should not have carte blanche to exploit consumer data under the flimsy guise of notice and choice. We should not pretend that TikTok users have any meaningful understanding of how the app's algorithms and design decisions entrap them, nor that these consumers have any meaningful control over these data practices, whether they are children or adults.

Deceptive, manipulative, and exploitative design decisions are prevalent in digital markets today. The Commission's own staff report on this issue makes a compelling case for acting to prevent companies from using design to exploit consumer trust. Persisting with a notice and choice regime would only further encourage design choices that work to circumvent user choice and manufacture flimsy consent.

D. Consent Can Be Effective Only in Select Circumstances, None of Which Are Present in Most Digital Transactions

All of this is not to say that consent can never be effective. Consent has long been an integral element of American law.[348] In select situations consent is justified, such as where parties have equal bargaining power, parties have significant resources, and parties knowingly and voluntarily agree to assume legal obligations.[349] The hallmarks of informed consent are that it is "freely given, specific, informed, and unambiguous," as well as voluntary and revocable. [350] For data practices, however, there are additional problems with consent beyond its form or substance. For consent to be effective in the context of data practices, there are heightened conditions that must be met. Termed "gold standard" consent, this idealized form of consent can meaningfully enhance autonomy and self-determination, but only if the circumstances and structure under which consent is sought and received are correct.

---

[346] Zheping Huang, *TikTok Has a Few Main Ingredients for Making Money*, BLOOMBERG (June 28, 2022, 5:45 AM), https://www.bloomberg.com/news/newsletters/2022-06-28/how-does-tiktok-make-money-app-relies-on-a-few-main-ingredients.
[347] *Id.*
[348] Richards & Hartzog, *supra* note 293,293 at 1467–76.
[349] *Id.* at 1462–63.
[350] *Id.* at 1492.

We have written before that there are "three circumstances necessary for an ideal environment for effective consent."[351] First, requests for consent must be *infrequent*. In a world rampant with decision fatigue, constant consent requests are a drain on consumer's time and cognitive load.[352] In contrast to situations where informed consent is required, such as medical treatment or scientific research, data subjects are "ceaselessly bombarded with requests for consent."[353] Making requests infrequent, which requires prioritizing certain consent requests over others, is necessary for consent to be effective.[354] Second, risks must be *vivid* (i.e., easy to envision).[355] Threats to bodily integrity or damage to liberty or property are easy to envision, but downstream risks of data practices are abstract.[356] Risk accrues incrementally as information is accumulated bit by bit.[357] Data harms also often stay hidden even after they have occurred.[358] Finally, there must be *incentives to take each request seriously*.[359] People will not take a request for consent seriously absent an incentive to do so, and such an incentive comes from "the magnitude of the stakes involved and the close relationship between the consent and those stakes."[360] Incentives of this sort are absent where the stakes appear insignificant, where the relationship between the consent and the risks is too remote, or when people feel powerless—i.e., under the typical circumstances in which consumers are asked to make online privacy decisions.[361] There are two additional aspects of data consent that further reduce the incentives for a consumer to take each request seriously. Consent to data practices is dispersed, with thousands of small, incremental disclosures that are not front of mind for a consumer faced with atomized data consent requests.[362] That leads to consumers making "transaction-rational" decisions and consenting to data practices which are harmful in the aggregate.[363] Furthermore, there are considerable externalities of consent. One individual's consent to data practices provides data which helps refine and empower those practices, leading to more sophisticated targeting of other individuals.[364] These circumstances—infrequency, vivid risks, and proper incentives—are all critical to effective consent, but they are also fraught with problems in the context of data practices and digital commerce. The absence of even one of these circumstances is fatal to effective consent. (Q74, Q78, Q84.)

---

[351] *Id*.
[352] *Id*. at 1493.
[353] *Id*. at 1493.
[354] *Id*. at 1494.
[355] *Id*.
[356] *Id*. at 1495.
[357] *Id*.
[358] *Id*.
[359] *Id*. at 1496.
[360] *Id*.
[361] *Id*.
[362] *Id*. at 1497–98.
[363] *Id*. at 1498.
[364] *Id*.

***

The well-documented failings of both notice and choice as concepts in privacy self-management combine to form an unwelcome and undeniable reality: consumers in digital markets have little notice nor any meaningful choice when it comes to commercial surveillance and data security. Further attempts to resuscitate the long-dead corpse of notice and choice would not only be a waste of the Commission's limited time and resources but also a disservice to consumers and companies alike. To protect consumers from unfair data practices and foster trust in digital markets, something more is needed: We need substantive limits on harmful data practices.

III. Fostering Trust in Digital Marketplaces

The evidence we have presented up to this point paints a bleak picture for consumers, competition, and digital markets. Prevalent commercial surveillance and lax data security practices have wrought significant individual and social harms and eroded public trust in digital markets. Consumers are eager to reap the benefits of the internet but face unprecedented information asymmetries and power differentials. Digital businesses learn a lot about us, but "we do not know a lot about them—their operations, what kinds of data they collect, how they use this data, and who they share it with."[365] This relational vulnerability leads to consumer exploitation as companies leverage commercial surveillance to profile, nudge, and manipulate consumers into acting in ways which do not benefit them. Rather than empowering consumers as promised, our notice and choice regime has failed to curtail all but the most simple and egregious violations of consumer expectations, and it has enabled a host of insidious data practices that prey upon consumer vulnerabilities. It is clear that something more is needed if we are to realize the promises of the early internet and produce the essential trust that is necessary for humans and companies mediated by technology to get along with each other for everyone's mutual benefit.

Jack Balkin has highlighted that "digital companies hold themselves out as trustworthy enterprises; they insist that our data is safe with them and that our privacy and our safety is their central concern. They encourage us to trust them so that we will entrust them with our data, indeed, with our digital lives."[366] It is time that we hold them to those representations with substantive protections for consumers, rather than merely procedural ones. To fully realize the innovative and transformative promise of digital markets, we need more than just data protection: we need human protection.[367] This requires implementing a framework which both examines the relationships between consumers and the companies with which they interact and places trust "at the center of our digital approach to consumer protection."[368] What we need are rules that focus on human relationships and vulnerabilities rather than on data, and rules that are substantive rather than merely procedural. The sections which follow expand on the themes of trust, loyalty, and relational vulnerability identified above; first by making the case that modern commercial relationships are uniquely risky for consumers; second, by establishing how commercial data disloyalty is an unfair trade practice consonant with the elements of Section 5; and third by identifying specific practices

---

[365] Balkin, *supra* note 54,54 at 11.
[366] *Id.* at 12.
[367] Hartzog & Richards, *supra* note 37,37 at 1736.
[368] *Id.*

or categories of commercial surveillance which are ripe for trade regulation rules grounded in concepts of loyalty and relational vulnerability.

A. Modern Commercial Relationships are Uniquely Risky for Consumers

Modern information relationships are exceptional in ways that the existing regulatory regime fails to fully recognize. Consumers are extremely vulnerable to digital companies who "repeatedly invite end users to trust them" despite knowing that "end users are mostly unaware of the dangers."[369] The current U.S. approach, characterized by *caveat emptor* and the decay of contract law around boilerplate, has facilitated the failed "notice and choice" approach to privacy.[370] Procedural protections and watered down application of the FIPs continue to ignore how companies betray the people who trust them with their data and online experiences every day.[371]

We have written before that "[e]ven if it might have been rational for lawmakers and judges to ignore information relationships in the past, our modern ongoing involvement with the companies providing the apps and websites we use every day demands more scrutiny."[372] The affordances of modern platform-consumer relationships are important and dangerous because of their "speed, immanence, automation, and scale."[373] These affordances and the business models motivated by them should be central to lawmakers' approach to modern privacy problems. Concepts of loyalty accurately reflect how the remarkable affordances of digital technologies result in wildly imbalanced relationships which go far beyond the standard understandings of arms-length dealings between merchants and customers in which parties with relatively equal bargaining power act competently in service of their own self-interest.[374] While the default presumption in

---

[369] Balkin, *supra* note 5454, at 26.

[370] *See generally* MARGARET RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012); NANCY KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS (2013); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587 (2007); Woodrow Hartzog, *Website Design As Contract*, 60 AM. U. L. REV. 1635, 1636 (2011); Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405 (2010); Richards & Hartzog, *supra* note 293293.

[371] Hartzog & Richards, *supra* note 3737; Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017).

[372] Hartzog & Richards, *supra* note 10,10 at 993.

[373] *See* Julie E. Cohen, *Scaling Trust and Other Fictions*, LAW AND POLITICAL ECONOMY (LPE) PROJECT (May 19, 2019), https://lpeproject.org/blog/scaling-trust-and-other-fictions (arguing that information fiduciary proposals fail to reckon with these problems).

[374] *See, e.g.*, Gen. Assur. of Am., Inc. v. Overby-Seawell Co., 893 F. Supp. 2d 761, 780–81 (E.D. Va. 2012), *aff'd*, 533 F. App'x 200 (4th Cir. 2013) ("a fiduciary relationship is not created 'between mutually interdependent businesses with equal bargaining positions who dealt at arms-length.'…Indeed, "[o]nly when one party figuratively holds all the cards—all the financial power or technical information, for example—have North Carolina courts found that the special circumstance of a fiduciary relationship has arisen.") (citations omitted); WEST'S TAX L. DICTIONARY *Arms Length* § A2960 (2021) ("Status of a transaction by unrelated parties, each acting in its own self interest. The term means a transaction made in good faith by parties with independent interests."); 4C LARY LAWRENCE, ANDERSON ON THE UNIFORM COMMERCIAL CODE § 2A-108:31 (3d. ed. 2021) ("The comparative bargaining power of the lessor and lessee is significant in determining whether the contract made by them is unconscionable….When a contract is negotiated at arm's length in good faith between parties of equal bargaining

market transactions is that parties are operating at arms-length, when one party has significant power over the other and an incentive to abuse that power, lawmakers often create duties and restraints within these imbalanced relationships to protect vulnerable parties. These power imbalances can manifest in several different ways, including large disparities in information or knowledge, reliance on expertise or promises, and discretion and control over that which is entrusted to one party in the relationship.[375] Modern commercial relationships are thus more akin to our intimate relationships with people that we trust with deeply personal experiences, information, and our personal safety than to the ones we have with ordinary merchants like automobile or furniture dealers.[376] Digital technologies have insinuated themselves to be an increasingly invisible part of the fabric of people's everyday lives and they have an outsized effect on their wellbeing. When policymakers treat all interactions between people and companies that offer online services as arms-length relationships, they ignore the role that structure and scale play in creating relational vulnerabilities.

Modern commercial relationships present many challenges, not all of which can be solved by loyalty alone. But our next generation of privacy rules will never be complete until it treats information relationships as imbalanced and capable of great abuse by the dominant party. This is one of main privacy problems addressed by loyalty. Rather than treating all kinds of information relationships as equal and fungible, it should increase obligations and restrictions on dominant parties as they amass power. The more power a company has in a relationship, the more protective and loyal it must be. A duty of loyalty would add an additional layer to data privacy law. Privacy would no longer be primarily about the data; instead it would have to consider the relationships between people and the companies they expose themselves to.[377] Such a change in focus would, perhaps surprisingly to some, mean that our consumer protection law would become even more focused on *protecting consumers*.

Although the ongoing interactions between people and digital technologies perhaps might not seem like a meaningful "relationship" in the traditional sense of the word, these relationships give rise to the same relational dynamics and abuses that trust rules are meant to address. At the outset, the interactions between people, platforms, and digital businesses are firmly established as legal relationships. Courts consistently bind people who use websites and apps to the terms of use and service agreements imposed by companies.[378] Yet technologically-mediated relationships between people and companies are more than mere legal formalities, even if they are different

---

power and contains no unusual provisions, the contract will not be regarded as unconscionable merely because one of the parties is disappointed with it."); N. Shipping Funds I, LLC v. Icon Cap. Corp., 921 F. Supp. 2d 94, 104 (S.D.N.Y. 2013) ("Generally, no fiduciary duties arise where parties deal at arm's length in conventional business transactions.") (quoting Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 592 F.Supp.2d 608, 624 (S.D.N.Y.2009)).

[375] *See, e.g.*, Daniel B. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, OXFORD HANDBOOK OF FIDUCIARY LAW 7-9 (Evan J. Criddle, Paul B. Miller, & Robert H. Sitkoff eds., 2019).

[376] *Id.*

[377] *See, e.g.*, Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection Law?*, 4 EUROPEAN DATA PROTECTION LAW REVIEW 1 (2020).

[378] Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1636 (2011); Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405 (2010).

from the meaningful relationships we have with our friends, advisors, and employers. These relationships involve far more interplay, exposure, and personalization than standard commercial services and contracts for widgets.

The relationships that people have with brick-and-mortar merchants and providers of services in a pre-digital era bear little resemblance to the relationships between people and modern commercial services. Critics of a duty of loyalty have asserted that treating platforms the same as a doctor strips away the affordances of the platform and the realities of scale.[379] But it is the precise affordances of hardware and software that make the relationship between people and platforms both highly imbalanced and novel in ways that compel relational rules grounded in concepts of loyalty. There are at least five traits of the relationship between people and digital technologies that, when combined, make these relationships highly imbalanced and worthy of intervention at the relational level: they are *ongoing*, high *frequency* relationships that occur within an *interactive* environment that is completely *constructed* for the individual and *responsive* to the individual by the dominant party.[380] Let's break these traits apart.

Ongoing. When people buy chairs, or ages ago when they bought CD-ROMs containing software, they typically engaged in discrete transactions. Although Office Depot or Adobe hoped customers would return, barring returns or malfunctions, the relationship between customer and manufacturer or software developer typically had some distance and downtime. Those days are long gone.[381] Platforms leveraging browsers, apps, and cloud computing, however, have obliterated the concept of discrete one-time interactions. Virtually every interaction requires an account creation with an intention of an always-evolving delivery of services; one the often auto-renews every month or every year. A platform's ideal scenario is that once a person signs up for service, they regularly visit and never leave. Systems are, to use the parlance of Silicon Valley, "optimized for engagement." Accounts remain updated, data and attention continue to be given, and patches and updates continue to be delivered with no planned end date. This is even true of non-platform websites. When you purchase an item online, you typically create an account (or, at the very least, provide an email address or phone number), install an app or visit a website, any of which give that company access to your data. Even merely visiting a website creates an ongoing

---

[379] *See, e.g.*, Cohen, *supra* note 373 ("The information fiduciaries proposal abstracts speed, immanence, automaticity, and scale away from that encounter and then assumes they never mattered in the first place. In the process, it both sacrifices the fiduciary arrangement's most essential characteristics and fails to reckon adequately with the characteristics of the platform-consumer relationship that are most problematic."); Khan & Pozen, *supra* note 255, at 514–520.

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

[381] *See* Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 198 (2020) ("The ideal of the one-off consumer transaction is dead. Instead of selling or licensing goods and services to consumers, firms today seek to build ongoing, evolving relationships with consumers based on constant contact. This trend is likely to continue, as the always-on devices that comprise the Internet of Things proliferate and cover an increasing number of everyday objects.").

relationship as you are then tracked across the web and fed targeted advertisements whose purpose is to lure you back to that site and tempt you into a purchase. This never-ending story justifies rules designed to foster long term, sustainable relationships between people and platforms.

Frequent. In addition to wanting to be with you forever, digital companies want to be with you *constantly*. People may go shopping in physical stores at most once or a few times a week. They might take occasional advantage of an offline service like babysitting or dry cleaning. But on average people interact with apps and websites over three hundred times *every day*.[382] Popular apps often get checked multiple times within the same hour or minute. While we may commonly use the same tool tens or hundreds of times a day (think how often you pick up a pen, sit in a chair, or drink from a cup), we might think it strange to browse the aisles of a store or call our financial advisor ten times a day, every day, for years on end. But how many times have you checked your phone today? For Facebook, Amazon, Google, Twitter, TikTok, and a host of other dominant platforms, failure to check in regularly is seen as a problem, and constant interaction from the user is a rewarded metric. This is true of other digital companies as well, such as news sites, that aim to keep users either purchasing products or bringing in advertisement revenue by capturing their attention.

Constructed. Companies leveraging their surroundings to influence their customers and clients is nothing new. Grocery stores place milk and eggs at the opposite side of the store from the entrance to encourage people to walk the aisles. Office designers make conference rooms totally transparent, for when you want everyone to see who you're meeting with, or completely opaque, for when you don't. It happens online as well. As Joel Reidenberg noted in his foundational article *Lex Informatica*, companies leverage information technologies to create policy rules that affect people.[383] But the extent to which tech companies control mediated environments is so great that it deserves sustained scrutiny. Our dealings with companies online occur *entirely* on their terms.[384] They control *who* has access, *what* they see and can do, *when* they see it and can

---

[382] *The New Normal: Phone Use is Up Nearly 4-Fold Since 2019, According to Tech Care Company Asurion*, ASURION (June 1, 2022), https://www.asurion.com/connect/news/tech-usage (describing how Americans reach for their phones an average of 352 times a day, or roughly once every two minutes and forty-three seconds, up nearly 4-fold since Asurion's 2019 study); *see also* LEE RAINIE & KATHRYN ZICKUHR, PEW RSCH. CTR., AMERICANS' VIEWS ON MOBILE ETIQUETTE 12 (2015), https://www.pewresearch.org/internet/2015/08/26/chapter-1-always-on-connectivity (noting that 94% of smartphone owners carry their phone with them "frequently," 82% "never or rarely turn their phones off," 59% "use apps on their phones at least several times a day," and 27% use apps "continuously"); *Average Time Spent Daily on Social Media (Latest 2022 Data)*, BROADBAND SEARCH, https://www.broadbandsearch.net/blog/average-daily-time-on-social-media (last visited Oct. 20, 2022) ("On average, people spend 147 minutes, or two hours and twenty-seven minutes, on social media daily."); Gabrielle Pickard-Whitehead, *66% of Americans Check Phone 160 Times a Day, Here's How Your Business Can Benefit*, SMALL BUS. TRENDS (Mar. 3, 2020), https://smallbiztrends.com/2020/03/2020-mobile-phone-usage-statistics.html (describing how "[t]he savviest of small businesses exploit America's love affair with their mobile phones to their advantage").

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

[384] *See, e.g.*, HARTZOG, *supra* note 840; Calo, *supra* note 254, at 1000–03.

take action, *where* they receive signals and can make choices, and *why* particular people see specific things and are given pre-constructed options. In non-mediated relationships, people have a degree of flexibility to work within a structured environment. They can choose from an endless array of physical actions, social interactions, and even change the structure of the environment themselves. But online, people can only click on the options they are given or address the audience they have been presented in the format that has been provided. Our ability to interrogate, analyze, ask questions, tinker, learn and otherwise calibrate our dealings with companies online is virtually non-existent. As consumers using these services, we are essentially powerless. Data subject rights of access, rectification, and deletion like those offered by the GDPR theoretically empower us a little, but they require us to take action in order to be protected. In practice these rights are difficult to exercise at scale, and, since they are limited only to personal data, data subject rights do very little to improve our agency within constructed environments outside of personal data transparency and management.

Interactive. When people consume legacy media like newspapers, magazines, television, or radio, they are essentially passive. There is no give and take between the mind and the medium; the flow of information is one-way. It would be a stretch to call these "relationships," even when we have subscription contracts with them.[385] But by contrast, the relationships between people and digital services are highly interactive. We create detailed accounts and profiles, search, amass networked connections, post pictures and status updates, press buttons, tweak settings, adjust sliders, arrange layouts, and project information streams that we don't even know about. And, of course, all of this interactivity can be quantified, optimized, and used to benefit the platform. Platforms best instantiate interactivity, but this phenomenon is not limited to platforms alone. Even certain legacy media companies, such as the New York Times, are adapting to provide increasingly interactive (and responsive) content.[386] E-commerce sites, empowered by cheap storage and improved data analytics, encourage us to provide information about ourselves so that they can mathematically match our tastes with their products. Prior to the information economy, these interactions occurred on a smaller scale and were ephemeral.

Responsive. The final twist that makes modern information relationships unique is that the *ongoing*, *frequent*, *constructed* and *interactive* nature of digital technologies enables companies to design their mediated environment to be acutely *responsive* to people's choices and profiles. News feeds and suggested products and information change on the fly according to your previous clicks and profiles created from personal data accumulated over time. Our mediated environments are tweaked based on individual data and up-to-the-second wisdom from constant A/B testing to maximize engagement and keep our eyes glued to the screen.[387]

---

[385] *See, e.g.*, Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405 (2010).
[386] *See, e.g.*, Liz Spayd, *A 'Community' of One; The Times Gets Tailored*, N.Y. TIMES (Mar. 18, 2017), https://www.nytimes.com/2017/03/18/public-editor/a-community-of-one-the-times-gets-tailored.html (describing how the New York Times planned to "customize the delivery of news online by adjusting a reader's experience to accommodate individual interests").
[387] *See, e.g.*, Calo, *supra* note 254.

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

The features and affordances of modern commercial relationships thus present unique dangers. It would be a mistake to treat modern commercial relationships as arms-length, even if they are scaffolded by consumer protection and data protection public governance rules. They are too one-sided and involved to tolerate an arms-length fiction. Loyalty is not sufficient to solve all our privacy problems, but it is necessary so long as the affordances of the tools, incentives for self-dealing, and legal contracting status of the parties places people in danger every time they create an account online. In this way, a surprising virtue of a loyalty approach is that it reveals how modern commercial relationships are not anything approaching arms-length transactions. Once lawmakers patch this bug and embrace the relational turn in privacy law, a number of different possibilities open up, including supporting public governance, new substantive rules, and a more collective and systematic approach to privacy.

B. Commercial Data Disloyalty as an Unfair Trade Practice

The Commission should ground its unfair trade practice data privacy rules in concepts of loyalty and relational vulnerability. Commercial surveillance is an accurate, descriptive label for the data practices which the Commission has observed in digital markets. While many commercial surveillance practices are or have the capability of being unfair trade practices,[388] not all commercial surveillance practices are unfair. Loyalty is what separates harmful and beneficial commercial surveillance. Approaching questions of unfairness through the frame of loyalty, trust, and relational vulnerability sheds a great deal of light on why certain trade practices that fall within the broad umbrella of commercial surveillance are both unfair and deceptive. Concepts of loyalty and relational vulnerability will help the Commission identify the exploitative practices and business models which are injurious to consumers. Disloyal practices—those self-serving, exploitative practices where a company acts contrary to a trusting consumer's best interests and causes substantial unavoidable harm— are unfair as a general matter, and it is almost impossible to imagine a disloyal practice that would satisfy Section 5. By narrowing the category of commercial surveillance to the subset of those practices which are disloyal, the Commission can craft precise trade regulations which target the most egregious and pressing harms in the marketplace. Through this focused approach, the Commission can work towards its goal of "[a] vibrant economy fueled by fair competition and an empowered, informed public."[389]

---

[388] *See supra* Parts I.B. & I.C.

[389] FED. TRADE COMM'N, STRATEGIC PLAN FOR FISCAL YEARS 2022 TO 2026 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/fy-2022-2026-ftc-strategic-plan.pdf.

1. Concepts of Loyalty and Relational Vulnerability Are Consonant with Section 5

Concepts of loyalty and relational vulnerability are fully consonant with the three elements of Section 5—substantial injury, unavoidability, and the absence of countervailing benefits. Under a theory of loyalty, betrayal is itself an injury. Betrayal damages the integrity of a relationship and diminishes trust. This has the secondary effect of diminishing a consumer's ability to safely and meaningfully participate in a marketplace. Absent a general duty of loyalty, betrayal is still a helpful lens through which injuries can be identified. Corporate opportunism and self-dealing leads to profiling and sorting, nudging, and manipulation. These prevalent practices undermine the fiction of consumer choice and impose substantial costs on consumers.

Two primary benefits of applying concepts of loyalty and relational vulnerability are that they naturally speak to the "reasonably avoidable" and "countervailing benefits" prongs of Section 5. Disloyal data practices are not reasonably avoidable by consumers because it is impossible to participate in modern society without entrusting personal data with companies, it is difficult for consumers to distinguish between trustworthy and untrustworthy companies, and digital experiences are constructed and mediated by companies. In contrast to traditional relationships between consumers and merchants, consumers can only click the options with which they are presented. There is no room for negotiation or true, meaningful control. Complicated arrays of privacy options give the appearance of control, but in reality these options are illusory and overwhelming. Consequently, consumers have no choice but to trust platforms with their personal data and mediated experiences. When these companies engage in self-serving, exploitative design and personal data processing, consumers are therefore powerless to prevent those actions. These practices are opaque, and consumers are left only with the all-or-nothing proposition of choosing whether or not to use a particular service. This problem is compounded by the difficulty that consumers face in trying to discern whether a company is trustworthy. As for the third prong, countervailing benefits, a disloyal action by definition cannot have a countervailing benefit to consumers because it is not in a consumer's best interest. It is also difficult to imagine how the disloyal betrayal of consumers could somehow benefit competition. The Commission's unfairness enforcement actions have long relied on notions of consumer expectations to identify and prosecute unfair practices. A duty of loyalty would provide greater clarity to companies and consumers about what constitutes an unfair practice, as a duty of loyalty will be informed both by preexisting legal precedents as well as the additional betrayal criterion.

Loyalty and relational vulnerability have been implicit themes of the Commission's prior enforcement actions. In its complaint against Zoom, the Commission alleged that Zoom made deceptive claims regarding the use of end-to-end encryption, the level of encryption, and the secure storage of Zoom meeting recordings, that Zoom unfairly circumvented a third-party privacy and security safeguard, and that Zoom deceptively deployed the ZoomOpener web server.[390] These privacy and security failings were significant given that consumers rely on videoconferencing technology in their daily lives and consumers share sensitive information during such meetings, including "financial information, health information, proprietary business information, and trade

[390] *Zoom Video Communications, Inc.*, 171 F.T.C. 31 (2021).

secrets."[391] The Commission's recognized the importance of trust and relational vulnerability in guiding the Commission's enforcement when it explained that, "[o]ur goal is a safe and secure Zoom that can continue to provide essential services to enable Americans to conduct business, engage in learning, participate in religious services, and stay connected."[392] Consumers made themselves vulnerable when they trusted Zoom to adequately safeguard their data, and Zoom betrayed that trust. This was a disloyal act, which was also an unfair trade practice, and understanding Zoom's acts in terms of disloyalty helps to clarify why those acts were unfair as a matter of law.

The Commission's recent enforcement actions against Kochava Inc. and Drizly, LLC further evince the Commission's focus on enabling consumers to safely interact in markets. In its complaint against Kochava, the Commission alleged that Kochava unfairly acquired and sold consumers' precise geolocation data in a format which allows entities to "track the consumers' movements to and from sensitive locations, including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at risk populations, and addiction recovery."[393] This data, if released, could lead to "stigma, discrimination, physical violence, emotional distress, and other harms."[394] Investigating Kochava's sale of sensitive precise geolocation data reinforces the principle that consumers must be free from disloyal commercial surveillance if they are to have the freedom to safely interact in markets. All-encompassing geolocation data tracking chills consumer behavior. Likewise, the Commission's recent enforcement action against Drizly, LLC and the resulting proposed settlement are also pertinent. Following a 2020 data breach, Drizly, an alcohol delivery e-commerce platform, was accused of failing to employ reasonable security measures and of making deceptive security statements.[395] In its proposed order, the Commission focused not only on Drizly's security failings, but also on the company's unnecessary data collection, which created additional risks for consumers.[396] Imposing data minimization and data retention limits on Drizly signifies that a company's commercial surveillance practices should not unnecessarily expose consumers to risk. Data minimization means, among other things, that companies have a duty to collect only that personal data that is necessary to provide a service to consumers that serves their best interests. By contrast, the collection of personal data that is unnecessary to serve such best interests is self-serving at best

---

[391] *Id.* at 33.
[392] *Id.* at 58 (majority statement of Chairman Joseph J. Simons, Commissioner Noah Joshua Phillips, and Commissioner Christine S. Wilson).
[393] Complaint, *FTC v. Kochava Inc.*, No. 22-cv-377 (D. Idaho Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.
[394] Press Release, Fed. Trade Comm'n, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.
[395] Complaint, Drizly, LLC & James Cory Rellas, FTC File No. 202-3185, https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf.
[396] Order, Drizly, LLC & James Cory Rellas, FTC File No. 202-3185 https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf.

and disloyal at worst, particularly if such data collection is used in a way that is self-serving, exposes the consumer to additional risk in case of a data breach or secondary data use, or is used to the detriment of consumers. Taken in combination, these enforcement actions reinforce the Commission's underlying goal of ensuring that consumers can be safe market participants.

2. Loyalty Solves the Consent Dilemma and Has the Added Virtue of Flexibility

The predominant virtue of loyalty-based rules is that they foster trust, enabling consumers to safely interact in markets. Loyalty has many additional virtues which we have detailed at length in our prior work: Loyalty focuses on relationships, achieves what a duty of care (avoiding unreasonable harm) alone cannot, prioritizes human values, and can be both flexible and clear.[397] For the purpose of this rulemaking, two important virtues of applying concepts of loyalty worth highlighting are that (1) loyalty solves the consent dilemma and (2) loyalty offers a flexible standard to promote ethical and consumer-protective data practices.

Consent has long plagued data privacy.[398] The FIPs idealize principles of notice and choice, but the thin procedural protections which are hallmarks of the dominant U.S. regime of notice and choice fail to give consumers meaningful control over their data. Consumers have a preference for greater data privacy but face a dilemma. Basic participation in modern society requires consumers to entrust other parties with their data, but consumers struggle to differentiate between loyal and disloyal companies and often face the all-or-nothing decision between using a service and consenting to whatever data practices are imposed or not using the service at all. This places consumers in the unenviable position of having to accept the risk that their data will be exploited even if their preference is for greater privacy and protection. To have true choice and autonomy, consumers need to be protected from exploitative data practices no matter what choice they make. This is one of the chief virtues of loyalty: it solves the consent dilemma. As we have written before,

> Trust-based protections would require parties in information relationships to protect the data placed in their care and to treat each other fairly and with deference. They would prohibit entrusted entities from asking for consent to practices that would make people unreasonably vulnerable. Lawmakers looking to embrace trust and minimize the pathologies of consent could leverage rules concerning the design of technologies and legal prohibitions on consent such as unconscionability to shift the policy conversation in a way that values both consent and privacy, and protects the millions and millions of human beings to whom these rules apply.[399]

Another important virtue of grounding data privacy rules in concepts of loyalty and relational vulnerability is that loyalty is flexible and adaptable across contexts, cultures, and time. Not only will this result in greater clarity over time,[400] but it also obviates any concerns about obsolescence. Flexible, standards-based frameworks like negligence, reasonableness (whether in negligence or in reasonable expectations of privacy), and unfairness, have long been applied in

---

[397] *See generally*, Hartzog & Richards, *supra* note 1010.
[398] *See generally* Solove, *supra* note 272272.
[399] *Id*.
[400] Richards & Hartzog, *supra* note 10,16 at 1013.

American law. That flexibility enables a loyalty-based framework to be "responsive to bigger structural power concerns and emergent problems driven by the affordances of new tools."[401] (Q95.)

Concepts of loyalty and relational vulnerability have much to offer the Commission as a conceptual lodestar in this rulemaking, in its future enforcement strategy, and in any future rulemaking under a federal privacy statute. Loyalty recognizes the unique nature of modern commercial relationships. Loyalty fosters trust, allowing consumers to safely interact in a healthy, vibrant marketplace. Loyalty solves the consent dilemma by shifting the risk of exploitative data practices from consumers to the companies which might act disloyally. Finally, loyalty offers a flexible, adaptable approach which is capable of withstanding the test of time. Loyalty will not solve all the problems stemming from society's digital transformation, but it can be a critical component of a nuanced, multilayered strategy which animates a just and fair digital future and promotes human flourishing. It might just be the key element of such a successful strategy.

C. The Commission Should Use Its Rulemaking Authority to Ban Particularly Harmful Unfair Trade Practices That Have the Hallmark of Disloyalty

The Commission should use its Section 18 rulemaking authority define as unfair trade practices select commercial surveillance practices which bear the hallmark of disloyalty, targeting "specific areas where trusted parties have an incentive to engage in self-dealing."[402] We have written before that "[s]ome data practices might be so dangerous that they should be taken off the table entirely."[403] Even without couching these rules within an umbrella duty of loyalty, concepts of loyalty and relational vulnerability can act as an important animating force and interpretive guide that would bring more coherence, flexibility, and accountability to the enforcement of these rules.[404] By crafting narrow rules which apply concepts of loyalty, the Commission can proscribe specific harmful practices while still preserving the benefits of safe and sustainable information exchanges. As a starting point, these comments recommend that the Commission consider rules pertaining to data minimization, targeted advertising, gatekeeping, and automated decision-making. This section also outlines how privacy protections for children and teenagers fit in with concepts of loyalty as we have explained them so far.

Before delving into the disloyal practices that we have identified as ripe for rulemaking, we wanted to clarify that any trade regulation rules promulgated by the Commission should be relatively agnostic about particular categories of data. While sensitive data is a useful proxy to address particularly harmful kinds of practices, advances in data analytics have enabled companies to use even seemingly innocuous types of non-sensitive data in order to infer the same kinds of vulnerabilities for which sensitive data can be a proxy. A better approach than focusing primarily on the nature of data is focusing on the nature of relationships. Rather than focusing primarily on the sensitivity of data, the Commission should focus on the vulnerability of relationships, because

---

[401] *Id.*10 at 1015; *accord* Richards & Hartzog, *supra* note 16,16 at 1013–14.
[402] *See* Hartzog & Richards, *supra* note 55, at 378.
[403] Hartzog & Richards, *supra* note 37,37 at 1737.
[404] Hartzog & Richards, *supra* note 55, at 378.

it is in vulnerable relationships that the opportunities for unfairness and deception are most pronounced and hardest for consumers to avoid harm through reasonable strategies of harm avoidance. (Q10, Q68, Q91.)

1. Data Minimization Is a Fundamental Element of Good Data Security

"[T]he relationship between privacy and security is vitally important and increasingly frayed."[405] A schism between security and privacy has formed,[406] which has resulted in data security "being treated as a distinct area centered around safeguards and notification."[407] That overly narrow view of data security misses the important role that front-door protection plays in data security.[408] Poor privacy undermines even the best data security practices. Put another way, data that is never collected in the first place cannot be exposed in a data breach. To help bridge this gap within companies, the Commission should define unnecessary and disproportionate data collection as an unfair trade practice.[409] Data minimization is a fundamental element of good data security. The Commission has recognized as such in its prior enforcement actions, notably in the recent *CafePress*[410] and *Drizly*[411] cases, where the companies were ordered to implement data minimization procedures. Following the Commission's fiftieth data security settlement in 2014, the Commission emphasized that companies should "limit the information they collect and retain based on their legitimate business needs so that needless storage of data does not create unnecessary of unauthorized access to the data."[412] Companies have thus been on notice for many

---

[405] SOLOVE & HARTZOG, *supra* note 96, at 145.
[406] *Id.* at 133–37.
[407] *Id.* at 137.
[408] *Id.* at 137–39.
[409] These comments refer specifically to a duty of data minimization, but the Commission should also consider a complementary limit on data retention for many of the same reasons. (Q44.)
[410] Residual Pumpkin Entity, LLC, the former owner of CafePress, and PlanetArt, LLC, which bought CafePress in 2020, were both investigated by the FTC regarding security failings which led to multiple data breaches. In a joint settlement, both entities were ordered to implement comprehensive information security programs, which included minimizing the amount of data they collect and retain. *See* Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover; Residual Pumpkin Entity, LLC, 173 F.T.C. 845 (2022), 2022 WL 2355555 (requiring Residual Pumpkin Entity to design, implement, maintain, and document safeguards relating to privacy, security, confidentiality, or integrity of personal information, including "[p]olicies and procedures to minimize data collection, storage, and retention, including data deletion or retention policies and procedures"); PlanetArt, LLC, 173 F.T.C. 874 (2022), 2022 WL 2355707 (likewise requiring PlanetArt to design and implement "[p]olicies and procedures to minimize data collection, storage, and retention, including data deletion or retention policies and procedures").
[411] *See* Press Release, *Fed. Trade Comm'n, FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers* (Oct. 24, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million. The recent proposed order against the online alcohol marketplace Drizly and its CEO Rellas goes further than the CafePress settlements in its requirements. The proposed order includes mandated deletion and data minimization as well as data retention limits. *See* Complaint, Drizly, LLC & James Cory Rellas, FTC File No. 202-3185, https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf.
[412] Public Statement, Fed. Trade Comm'n, *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

years that they increase the risk and severity of potential data breaches when they collect and retain data unnecessarily.[413] Unnecessary data collection creates vast repositories of data whose mere existence incentives hackers to breach systems. As Commissioner Slaughter has helpfully explained, "[H]ackers cannot steal data that companies did not collect in the first place; requirements that limit what data can be collected, used, and retained could meaningfully foil and deter data security breaches."[414] Data breaches are to some extent inevitable, and unnecessary and disproportionate data collection makes breaches more damaging than they otherwise might have been. Rampant data collection also threatens data security because it gives fraudsters additional information that can be weaponized against users to carry out later data breaches, i.e. by facilitating phishing attempts.[415] (Q43, Q47.)

The Commission should promulgate a trade regulation rule providing that it is an unfair practice to collect, process, or transfer data which is not reasonably necessary and proportionate to provide or maintain a specific product of service requested by the individual to whom the data pertains. A data minimization requirement would help bridge the gap between privacy and security by ensuring that companies implement sufficient front end protections on data collection. The Commission should also consider enumerating select "permitted purposes" which would allow companies to collect, process, or transfer personal data so long as the company's purpose is consistent with one of those permitted purposes. There are many detailed data minimization proposals from which the Commission could craft a more detailed and nuanced rule, such as the Electronic Privacy Information Center's proposal from earlier this year.[416] (Q76.)

One of the greatest challenges in implementing substantive limits on appropriate collection and use of data is determining contextually what data collection is reasonably necessary and proportionate. This is another area in which concepts of loyalty and relational vulnerability can add value to the Commission's work. Grounding a data minimization requirement in concepts of loyalty can add important clarity to the rule. Data loyalty provides a normative vision for the boundaries of data minimization by introducing "a value-laden baseline that not only requires an examination of the purpose of the collection but also elevates the interests of those affected by the collection."[417] This loyalty-based minimization requirement would consider the type of data collected and the context of collection relative to the nature of the trusted relationship and the consumer's exposure to the trusted party.[418]Applying this concept, collection generally would shift

---

[413] SOLOVE & HARTZOG, *supra* note 96,405 at 146–47.
[414] Statement of Commissioner Rebecca Kelly Slaughter (Oct. 21, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Statement-of-Commissioner-Slaughter-Regarding-Drizly-FINAL.pdf.
[415] For that same reason, software primarily designed to invade privacy without sufficient legitimate uses also poses a threat to security and should be targeted for enforcement. SOLOVE & HARTZOG, *supra* note 96,405 at 149.
[416] Press Release, Elec. Privacy Info. Ctr., *EPIC and Consumer Reports Urge the FTC to Initiate a Data Minimization Rulemaking* (Jan. 26, 2022), https://epic.org/epic-and-consumer-reports-urge-the-ftc-to-initiate-a-data-minimization-rulemaking.
[417] Hartzog & Richards, *supra* note 10,10 at 1025–26.
[418] *Id.* at 1026.

from gathering as much data as possible to collecting data for "improv[ing] the quality of service in the loyal customer's interest."[419] (Q45.)

Data minimization is not possible without proper data governance. There are a number of privacy practices related to data minimization which the Commission should consider in developing its data minimization framework, such as data mapping and accounting. Operationalizing a data minimization obligation can lessen the risk of organizations losing track of what personal data is collected or where that data is kept.[420] These are just a few examples of how a data minimization rule would improve data security practices and potentially help bridge the gap that often exists between privacy and security compliance within companies. Companies should only be able to collect and retain data that is adequate, relevant, and necessary, as interpreted through concepts of loyalty.[421] Such a limit on collection would better align with consumer expectations, protect users from downstream security failings, and foster trust in commerce. Data security and privacy can thus be mutually reinforcing, and a data minimization requirement would be a powerful step in achieving both aims. (Q43, Q47.)

2. Loyal Gatekeeping Can Curtail Data Broker Access to Consumer Information

Under the current status quo, companies have strong financial incentives to give third parties access to trusting parties and their data. This financial pressure breeds disloyalty, which has manifested itself in a number of high-profile incidents, such as Cambridge Analytica's Facebook data exfiltration.[422] An increasingly important example is the geolocation data broker industry, who aggregate data from third-party apps and surveil the private lives of millions of individuals on behalf of law enforcement and private companies.[423] Disloyal gatekeeping is substantively unfair: it causes substantial injury to consumers, it is not reasonably avoidable by consumers, and it does not have countervailing benefits to consumers and competition. It is unfair to consumers for companies to implement APIs, advertiser portals, third-party SDKs, fusion centers, and government backdoors that facilitate third-party access in ways which conflict with trusting parties' best interests. This access invades consumers' privacy in opaque ways, it exposes them to unavoidable harm, and it leaves them with little recourse. To protect consumers, the Commission should prohibit disloyal gatekeeping, the practice of providing third-party access to consumer data when that access elevates the self-interest of the company over that of consumers. A gatekeeping requirement could be styled in a number of different ways, such as a duty of care

---

[419] *Id.*

[420] *See supra* note 76 and accompanying text (discussing how Facebook employees do not understand where much data goes once it enters the company's systems); *supra* note 77 and accompanying text (describing Facebook's role in the Cambridge Analytica scandal).

[421] *See supra* note 417 and accompanying text. The proposed ADPPA conceives of data loyalty as a robust data minimization rule. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 101 (2022) (placing data minimization under the "Duty of Loyalty").

[422] *See supra* note 77 and accompanying text.

[423] *See* Bennett Cyphers, *Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police*, EFF (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police; Complaint, FTC v. Kochava Inc., No. 22-cv-377 (D. Idaho Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.

and confidentiality, a duty of reasonable gatekeeping, or a duty of reasonable protection. How the Commission frames and articulates the duty will of course have substantive consequences. But regardless of how the Commission might choose to frame a duty of loyal gatekeeping, this duty should still allow for beneficial third-party access, such as contextual advertising or protocols for interoperability. The Commission should also consider an outright prohibition on the nonconsensual sale of consumer data. (Q52, Q76.)

3. Targeted, Behavioral, and Cross-Contextual Advertising Should Be Limited

Advertising is baked into the current business model of the internet.[424] This rulemaking will not change that, but the Commission should explore loyalty-based rules limiting targeted, behavioral, and cross-contextual advertising. The commercial surveillance ecosystem is driven largely in part by the advertising industry's perceived need to profile, sort, and influence consumers. Rampant, unfettered data collection enables companies to build comprehensive user profiles which, when leveraged with data science and behavioral science, enables advertisers to exploit consumer vulnerabilities.[425] Consumers are in the unenviable position of having to entrust companies with their data, knowing that these companies are harvesting as much data as possible to facilitate targeted advertising. But consumers are in no position to assess ex ante whether a company will target them in a loyal or disloyal way (or whether their data will be sold to a third party who will unfairly target them down the line). Some uses might be beneficial, such as loyal personalization and first-party advertising. Some uses might be manipulative, however, like attempts to dissuade that consumer from voting.[426] Furthermore, the benefits of targeted advertising disproportionately flow to a small subset of actors in the ad-tech industry, to the detriment of consumers, publishers, and often advertisers themselves.[427] Data minimization and loyal gatekeeping mandates, as detailed above, are substantive limits which would indirectly curtail the most egregious and trust-eroding forms of targeting by drying up the data streams which enable the surveillance advertising industry. The Commission can further reinforce those measures by placing substantive limits on targeted, behavioral, and cross-contextual advertising. Doing so will remove the market incentives which drive the kinds of rampant, reckless, and disloyal data collection that expose consumers to risk of harm. (Q76, Q81.)

As Jack Balkin has pointed out, not all targeted advertising is inherently abusive or inconsistent with the best interests of end users.[428] In fact, "much of modern advertising is based on increasing efficiencies in locating and reaching interested audiences."[429] The challenge is finding the dividing line between those targeting practices which are exploitative, rising to the level of an unfair trade practice, and those which are not. This is where concepts of loyalty and relational vulnerability, as a normative baseline to guide substantive rules, can be informative: "we should ask what practices of advertising, targeted at end users, do not betray their trust or operate

---

[424] *See generally* CRAIN, PROFIT OVER PRIVACY, *supra* note 224224.
[425] *See supra* Parts I.B and I.C.
[426] *See supra* Part I.C.2.c.ii.; *see also* CRAIN, PROFIT OVER PRIVACY, *supra* note 224.
[427] *See supra* Part I.C.
[428] Balkin, *supra* note 54,54 at 27.
[429] *Id.*

against their interests."[430] One important distinction we can draw is between first- and third-party targeted advertising. Trust cannot flourish when consumers are inundated with online advertisements that are selected by third parties based on known or predicted interests or traits associated with that consumer. Such targeting by third parties poses serious risks of unavoidable injury to consumers.[431] In contrast, it would not be unfair for a company to process first-party data as necessary (consistent with any data minimization obligations) for the purpose of advertising that company's own products or services to a consumer. A consumer who seeks out a particular company or webpage will not feel a sense of betrayal from first-party advertising because it aligns with their expectations and does not involve unnecessary exposure to a third party with whom the consumer does not have a relationship.

There are existing legal limits on targeted advertising from which the Commission should take inspiration. California's CCPA draws a distinction between "cross-context behavioral advertising" and "nonpersonalized advertising." Cross-context behavioral advertising encompasses "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."[432] Companies subject to the CCPA are required to provide an option for consumers to opt out of having their personal information sold or shared for cross-context behavioral advertising.[433] Nonpersonalized advertising, in contrast, encompasses "advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business with the exception of the consumer's precise geolocation."[434] Nonpersonalized advertising is not restricted under the CCPA so long as "the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business."[435] This kind of first-party advertising would be consistent with the notion of loyalty as we articulate it here. (Q42, Q80, Q82.)

Introducing reasonable, substantive limits on targeted advertising would not mean the death of online advertising. Some forms of targeted advertising could continue if pursued in a transparent and loyal manner. This could result where consumers give truly informed and voluntary consent to opt-in to such targeting, giving them true control over how their data is used, in contrast to the fictitious control perpetuated by the current notice and choice regime. As discussed above, there is also an opportunity for first-party targeting. Contextual advertising is a trust-preserving form of targeting which has withstood the test of time.[436] Displaying

---

[430] *Id.* at 28.
[431] *See supra* Part I.C.1.
[432] CAL. CIV. CODE § 1798.140(k) (West 2022) (effective Jan. 1, 2023).
[433] CAL. CIV. CODE § 1798.185(a)(19)(A)(vi)(III) (West 2022).
[434] CAL. CIV. CODE § 1798.140(t) (West 2022) (effective Jan. 1, 2023).
[435] CAL. CIV. CODE § 1798.140(e)(4) (West 2022) (effective Jan. 1, 2023) (describing nonpersonalized advertising as a "business purpose" for which service providers and contractors may use consumers' personal information); CAL. CIV. CODE § 1798.185(a)(11).
[436] *See supra* Part I.D.1.c.

advertisements based on the content in which that advertisement appears, rather than who is viewing that advertisement, can benefit consumers, publishers, and advertisers without betraying consumer trust. As Balkin identifies, contextual advertising does not require "an elaborate digital dossier about [you] to be effective."[437] Critics have argued that contextual advertising is not viable in select circumstances, such as where brand integrity would be damaged by the content of a news article. It is not clear that this will be the case. For example, consumers are likely to understand that contextual ads target a particular publisher's readership rather than the content of specific stories.[438] (Q41, Q42.)

4. Fairness, Transparency, and Accountability Are Necessary to Combat Due Process Harms of Automated Decision-Making

Companies' increased reliance on automated decision-making systems, coupled with mounting evidence that these systems create discriminatory disparate outcomes,[439] raises grave concerns over the fairness, accountability, and transparency of these systems. As we have argued before, platform optimization threatens our "cyber civil rights," and algorithmic or automated decision-making in key aspects of people's lives, such as health, finance, jobs, travel, and other essential life activities, raises important concerns about due process.[440] Therefore, "[a]ny approach to data privacy that does not incorporate algorithmic accountability will be incomplete."[441] The Commission should heed the advice of AI experts and develop rules regarding the design, implementation, and use of AI systems which are grounded in concepts of loyalty and relational vulnerability. The Commission could prohibit the use of algorithms which have an unreasonable risk of producing disparate outcomes for marginalized communities. Procedural safeguards such as algorithmic impact assessments will not perfectly eliminate the risk of disloyal, exploitative, and biased algorithms, but they could help curtail such algorithms by increasing the likelihood that

---

[437] Balkin, *supra* note 54,54 at 28.

[438] *See* Jenn Chen, *Fostering Advertising with Greater Integrity*, ASS'N. NAT'L ADVERT. (Sept. 22, 2022), https://www.ana.net/miccontent/show/id/ii-2022-09-fostering-advertising (describing how contextual advertising presents an opportunity for advertisers to "finance diverse voices, reward publishers who uphold high journalistic standards and move beyond an era of advertising driven by personal data often collected without consumer consent").

[439] *See, e.g.*, Joy Buolamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, TIME (Feb. 7, 2019, 7:00 AM), https://time.com/5520558/artificial-intelligence-racial-gender-bias (describing the "exclusion overhead," the costs incurred when technological systems fail to take into account the diversity of humanity); Olga Akselrod, *How Artificial Intelligence Can Deepen Racial and Economic Inequities*, ACLU (July 13, 2021), https://www.aclu.org/news/privacy-technology/how-artificial-intelligence-can-deepen-racial-and-economic-inequities (describing the ways in which AI has worsened discriminatory practices); *U.S. Warns of Discrimination in Using Artificial Intelligence to Screen Job Candidates*, NPR (May 12, 2022, 5:04 PM), https://www.npr.org/2022/05/12/1098601458/artificial-intelligence-job-discrimination-disabilities; Charlene Chu, Kathleen Leslie, Rune Nyrup & Shehroz Khan, *Artificial Intelligence Can Discriminate on the Basis of Race and Gender, and Also Age*, CONVERSATION (Jan. 18, 2022, 11:11 AM), https://theconversation.com/artificial-intelligence-can-discriminate-on-the-basis-of-race-and-gender-and-also-age-173617 (describing how AI can exacerbate ageism); Andrew Burt, *How to Fight Discrimination in AI*, HARV. BUS. REV. (Aug. 28, 2020), https://hbr.org/2020/08/how-to-fight-discrimination-in-ai. (Q53.)

[440] Hartzog & Richards, *supra* note 37,37 at 1758.

[441] *Id.*

disparate impacts are detected and mitigated. Even though it lacks an express duty of loyalty, the White House's recent AI Bill of Rights is an informative source from which the Commission can take inspiration.[442] The Commission should also examine the ways in which other jurisdictions, such as the EU, have attempted to mitigate the risks of algorithms producing disparate outcomes.[443] (Q56, Q60, Q62, Q67, Q89.)

5. Data Privacy Rules Should Protect Children, Teenagers, and Adults

When it comes to the important responsibility of protecting children, the Commission does not face a binary choice between strengthening privacy protections for Americans either under or over the age of eighteen. To the contrary, many of the methods for protecting the most vulnerable consumers are applicable to the protection of all consumers, and vice versa. The general agreement across stakeholders about the importance of protecting children in digital environments actually illustrates a broader point about problems of commercial surveillance, loyalty, and the data economy which is true for all consumers. While there is much evidence to indicate that children and other highly vulnerable populations need protection, the imbalance of the relationship between all consumers and commercial surveillance companies is so drastically skewed that the most desirable concepts for preventing unfair practices against children should be applied to the general population as well.[444]

In the past few decades, a general consensus has emerged regarding the need to protect children from the risks and harms which result from being online. Concerns over the privacy and wellbeing of children lead to the enactment of one of the few data protection laws in the US, the Children's Online Privacy Protection Act. Despite COPPA's notable successes in protecting young children online, it has are obvious gaps. Children over the age of thirteen are excluded. The law predates the advent of modern social media and is ill-equipped to deal with the mental health crises spurred by these platforms. States are stepping in to fill the gaps, as California has done with its recent enactment of the California Age-Appropriate Design Code Act.[445] There are also new

---

[442] *See generally* WHITE HOUSE, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

[443] *See, e.g.*, Council Regulation 2016/679, arts. 4(4), 22, recitals (71), (72), General Data Protection Regulation, 2016 O.J. (L 119) 14, 33, 46. If the Commission is looking to practices in other jurisdictions, it should also consider the proposals in the EU's new Digital Services Act. *See, e.g.*, Council Regulation 2022/2065, Digital Services Act, 2022 O.J. (L 277); THE DIGITAL SERVICES ACT: ENSURING A SAFE AND ACCOUNTABLE ONLINE ENVIRONMENT, EUROPA, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en (last visited Nov. 21, 2022). One benefit of drawing from EU law is that, by bolstering a US data privacy regulatory regime with elements of EU law, the Commission could help the US obtain an adequacy judgment and thus facilitate transatlantic data transfers under the GDPR.

[444] *See, e.g.*, Lindsey Barrett, *Ban Facial Recognition Technologies for Children—and for Everyone Else*, 26 B.U. J. SCI. & TECH. L. 223 (2020) (arguing that "children's heightened vulnerability to privacy violations and discrimination from the use of facial recognition technologies doesn't diminish the severity of the harms that other groups and the population at large experience.").

[445] *See* California Age-Appropriate Design Code Act, A.B. 2273, 2021-2022 Reg. Sess. (Cal. 2022).

federal laws being proposed every year, such as the Kids Internet Design and Safety (KIDS) Act.[446] The Commission devotes a substantial number of questions in the ANPR to addressing the effects of commercial surveillance on the wellbeing of children and teenagers, and there is considerable support amongst the commissioners for additional privacy rules protecting children and teenagers. As Commissioner Wilson has recently highlighted,

> [r]ecent research reveals that platforms use granular data to track children's online behavior, serve highly curated feeds that increase engagement, and (in some instances) push kids towards harmful content. More broadly, the research reveals a "catastrophic wave of mood disorders (anxiety and depression) and related behaviors (self-harm and suicide)" among minors, and particularly teenage girls, who spend a significant amount of time on social media daily.[447]

Commissioner Bedoya has likewise emphasized the plight faced by children and teenagers online, calling for greater scrutiny of product design and more aggressive enforcement of children's privacy standards.[448] The Commission "has a long history of intervening in the marketplace to protect children,"[449] reflecting a general consensus that children and teenagers are in need of protection online.

Arguments for protecting children and teenagers online generally coalesce into broad points about their lack of information, naiveté, autonomy, and decision-making skills. Having less decision-making experience than adults, children and teenagers have less information about potential risks of consenting to different data practices. That same lack of life experience leads children (and especially teenagers) to be overconfident about their ability to make decisions. This lack of information and experience manifests itself in different ways, such as underdeveloped media literacy which leads children and teens struggling to distinguish between sponsored content and news articles.[450] There is also evidence that certain injuries resulting from disloyal data practices disproportionately affect children and teenagers. Teens self-report high percentages of online use, with forty-six percent stating they are online "almost constantly" and ninety-seven

---

[446] Many of the proposals in the KIDS Act, such as prohibitions on manipulative marketing, amplification of harmful content, and damaging design features would substantially benefit all consumers if broadly implemented, not just children and teens. *See* Press Release, Sen. Ed Markey, Senators Markey and Blumenthal, Rep. Castor Reintroduce Legislation to Protect Children and Teens from Online Manipulation And Harm (Sept. 30, 2021), https://www.markey.senate.gov/news/press-releases/senators-markey-and-blumenthal-rep-castor-reintroduce-legislation-to-protect-children-and-teens-from-online-manipulation-and-harm (describing how the KIDS Act can make the digital design more ethical).

[447] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273, 51,299 (proposed Aug. 22, 2022) (Dissenting Statement of Commissioner Christine S. Wilson).

[448] Cristiano Lima & Aaron Schaffer, *The FTC's Newest Member Wants to Scrutinize How Tech May Harm Kids*, WASH. POST (Aug. 25, 2022, 9:01 AM), https://www.washingtonpost.com/politics/2022/08/25/ftc-newest-member-wants-dial-up-scrutiny-kids-online-safety.

[449] HOOFNAGLE, *supra* note 11,11 at 193.

[450] Wayne D'Orio, *What Is Media Literacy? What Parents Need to Know*, U.S. NEWS (Mar. 31, 2022, 9:09 AM), https://www.usnews.com/education/k12/articles/what-is-media-literacy-what-parents-need-to-know.

percent stating they are online daily.[451] Research shows that while both adults and children receive a boost of dopamine from social rewards online, these feelings are heightened by children and teens as they are more likely to attach their sense of self to the opinions of their peers and others online.[452] Taken together, these justifications make a compelling argument for increased privacy protection.

The Commission's focus on protecting kids is laudable, but the Commission should not lose sight of the fact that many of the reasons given for protecting children also apply to adults. There are some meaningful differences between the decision-making capabilities of children and adults. There are also meaningful differences in the way that privacy harms may affect children versus adults. For example, there is evidence that time on social media affects adults differently than it does young people.[453] Despite those differences, it is not clear whether these distinctions are very meaningful from a policy perspective. Questions abound about whether there is a good reason that privacy protections for children cease at age thirteen rather than eighteen. But there is also nothing magical about eighteen as a dividing line. As any college professor or parent of young adults will tell you (something we can also speak to from personal experience), nineteen-year-olds are only marginally wiser and more mature than eighteen-year-olds, and undergraduate students, many of whom are also living away from home for the first time, generally struggle under the strain of commercial surveillance and the overwhelming demands of notice and choice. Age is a spectrum, as is the wisdom and maturity that comes with it. Rules and safeguards that follow arbitrary age distinctions fail to see the forest for the trees and leave meaningful gaps in protection. Adults suffer many of the same harms as children and teens. Adults are similarly ill-equipped to protect themselves in the face of these platforms. Digital markets are plagued by stark information asymmetries and power differentials. As discussed above in the analysis of the failure of notice and choice, the same kinds of information asymmetries and overconfidence that are ascribed to children and teenagers apply to adults as well. Pointedly, if notice and choice is overwhelming, illusory, and ineffective for adults, then parental consent cannot be an efficacious way of ensuring child online privacy.[454] The ANPR asserts that teenagers may be characteristically less capable of anticipating reputational harms than adults, but adults routinely overestimate their ability to self-manage their own privacy. The general agreement across stakeholders about the importance of protecting children in digital environments actually illustrates a broader point about problems of commercial surveillance, loyalty, and the data economy which is true for all consumers. Commercial surveillance is so prevalent, powerful, and opaque that we are all rendered powerless before this data hungry leviathan, regardless of how young or old we are. Rather than promulgating specific data privacy rules for children and teenagers, the Commission should focus on crafting

---

[451] Emily A. Vogels, Risa Gelles-Watnick, and Navid Massarat, *Teens, Social Media and Technology 2022*, Pew Research Center (Aug. 10, 2022).
[452] Zara Abrams, *Why Young Brains are Especially Vulnerable to Social Media*, AM. PSYCH. ASS'N (Feb. 2022), https://www.apa.org/news/apa/2022/social-media-children-teens.
[453] Alvaro Bedoya, Comm'r, Fed. Trade Comm'n, "Who is being left behind?": Enforcement Priorities for a Tech Consumer Protection Agenda (Aug. 9, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/who_is_being_left_behind_-_naag_presidential_summit.final_.public_version.pdf.
[454] *See supra* Part II.

generally applicable trade regulations which will protect all Americans from the harmful practices detailed above. The best protections that the Commission can offer children and teens are the kinds of generally applicable rules detailed above, especially data minimization, loyal gatekeeping, and an end to corrosive targeting. (Q12, Q13, Q18, Q19, Q79.) All consumers deserve protection from disloyal data practices, and consumer protection should mean much more than the digital *caveat emptor* that is far too frequently the world that consumers of digital goods and services face.

Conclusion

The status quo of privacy regulation in the United States cannot continue. We have previously written that "the corporate, commercial, mobile app-driven internet of the early 2020s represents probably the most highly surveilled environment in the history of humanity."[455] This prevalent, even ubiquitous surveillance creates individual and social harms, disproportionately benefits certain industry actors, and erodes trust in the market. "[P]rivacy is inevitably about the distribution and exercise of power,"[456] and commercial surveillance enables certain market actors to leverage unreasonable and unavoidable power over consumers, to the detriment of both consumers and competition. Commercial surveillance has certainly flourished under a notice and choice regime which serves only the interests of the data hungry companies who hold considerable power of basic aspects of our lives. Consumers—human beings—have not. It is important to recognize, however, that there is nothing inevitable about this current state of affairs. These disloyal, exploitative data practices are everywhere, but they *came to be* everywhere.[457] There is nothing natural, unavoidable, or inevitable about modern commercial relationships. Furthermore, neither consumers nor voters really chose this outcome. Advertisers and advertising middlemen, driven by market incentives and an absence of meaningful data privacy rules, spurred the creation of the prevalent commercial surveillance practices we languish under today—too often so far outside the awareness of consumers that any notion of consent or acquiescence borders on the absurd. To achieve its vision of "[a] vibrant economy fueled by fair competition and an empowered, informed public,"[458] the Commission should pursue Section 18 rulemaking and consider substantive rules regulating commercial surveillance grounded in concepts of loyalty and relational vulnerability. Data privacy rules grounded in such concepts would not be a panacea or s silver bullet, but they are a large step towards what should ultimately be a nuanced, multilayered strategy of consumer protection in digital markets. Substantive limits on commercial surveillance that are nuanced, focused, and elevate consumer wellbeing will not irreparably damage the internet or spell the end of the advertising industry. To the contrary, the Commission has an opportunity to pass substantive rules which benefit consumers and companies alike by fostering trust, enabling human flourishing, and delivering on the lofty ideals of early internet pioneers. A sustainable digital marketplace undergirded by reasonable, substantive consumer protection rules would thus

---

[455] RICHARDS, *supra* note 21,21 at 83; *see also* Lina Khan, Fed. Trade Comm'n, Remarks of Chair Lina M. Khan as Prepared for Delivery IAPP Global Privacy Summit 2022 Washington D.C. (Apr. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf (citing RICHARDS, *supra*).
[456] Hartzog & Richards, *supra* note 37,37 at 1737.
[457] *See* McNamee, *supra* note 29.
[458] FED. TRADE COMM'N, STRATEGIC PLAN FOR FISCAL YEARS 2022 TO 2026 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/fy-2022-2026-ftc-strategic-plan.pdf.

offer significantly greater benefits to consumers, competition, and firms over the long run than the status quo, by encouraging sustainable, trustworthy, loyal information relationships that make all parties better off.

Appendix

1. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).
2. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016).
3. Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019).
4. Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 6 EUR. DATA PROT. L. REV. 492 (2020).
5. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020).
6. Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021).
7. Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985 (2021).
8. Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022).

THE DANGERS OF SURVEILLANCE

Neil M. Richards[*]

From the Fourth Amendment to George Orwell's *Nineteen Eighty-Four*, and from the Electronic Communications Privacy Act to films like *Minority Report* and *The Lives of Others*, our law and culture are full of warnings about state scrutiny of our lives. These warnings are commonplace, but they are rarely very specific. Other than the vague threat of an Orwellian dystopia, as a society we don't really know why surveillance is bad and why we should be wary of it. To the extent that the answer has something to do with "privacy," we lack an understanding of what "privacy" means in this context and why it matters. We've been able to live with this state of affairs largely because the threat of constant surveillance has been relegated to the realms of science fiction and failed totalitarian states.

But these warnings are no longer science fiction. The digital technologies that have revolutionized our daily lives have also created minutely detailed records of those lives. In an age of terror, our government has shown a keen willingness to acquire this data and use it for unknown purposes. We know that governments have been buying and borrowing private-sector databases,[1] and we recently learned that the National Security Agency (NSA) has been building a massive data and supercomputing center in Utah, apparently with the goal of intercepting and storing much of the world's Internet communications for decryption and analysis.[2]

Although we have laws that protect us against government surveillance, secret government programs cannot be challenged until they are discovered. And even when they are, our law of surveillance provides only minimal protections. Courts frequently dismiss challenges to such programs for lack of standing, under the theory that mere surveillance creates no harms. The Supreme Court recently reversed the only major case to hold to the contrary, in *Clapper v. Amnesty International*

---

[*] Professor of Law, Washington University School of Law. For helpful comments on prior drafts, I thank Jim Bohman, John Inazu, Jonathan King, Wendy Niece Richards, and participants in the Washington University Political Theory Workshop. Special thanks are also due to my co-participants at the *Harvard Law Review* Symposium on Privacy and Technology — Professors Julie Cohen, Paul Schwartz, Dan Solove, and Lior Strahilevitz — and my generous commentators, Danielle Citron, David Gray, and Orin Kerr. Thanks also to my research assistants, Matthew Cin and Ananth Iyengar, and my faculty assistant, Rachel Mance.

[1] *See, e.g.*, ROBERT O'HARROW, JR., NO PLACE TO HIDE 1–4 (2005).

[2] James Bamford, *The Black Box*, WIRED, Apr. 2012, at 78, 80.

Electronic copy available at: https://ssrn.com/abstract=2239412

USA,[3] finding that the respondents' claim that their communications were likely being monitored was "too speculative."[4]

But the important point is that our society lacks an understanding of why (and when) government surveillance is harmful. Existing attempts to identify the dangers of surveillance are often unconvincing, and they generally fail to speak in terms that are likely to influence the law. In this Article, I try to explain the harms of government surveillance. Drawing on law, history, literature, and the work of scholars in the emerging interdisciplinary field of "surveillance studies," I offer an account of what those harms are and why they matter. I will move beyond the vagueness of current theories of surveillance to articulate a more coherent understanding and a more workable approach.

At the level of theory, I will explain why and when surveillance is particularly dangerous and when it is not. First, surveillance is harmful because it can chill the exercise of our civil liberties. With respect to civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas. To protect our intellectual freedom to think without state oversight or interference, we need what I have elsewhere called "intellectual privacy."[5] A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance.

At a practical level, I propose a set of four principles that should guide the future development of surveillance law, allowing for a more appropriate balance between the costs and benefits of government surveillance. First, we must recognize that *surveillance transcends the public/private divide*. Public and private surveillance are simply related parts of the same problem, rather than wholly discrete. Even if we are ultimately more concerned with government surveillance, any solution must grapple with the complex relationships between government and corporate watchers. Second, we must recognize that *secret surveillance is illegitimate* and prohibit the creation of any domestic-surveillance programs whose existence is secret. Third, we should recognize that *total surveillance is illegitimate* and reject the

[3] 133 S. Ct. 1138 (2013).

[4] *Id.* at 1147.

[5] *See generally* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008) [hereinafter Richards, *Intellectual Privacy*].

Electronic copy available at: https://ssrn.com/abstract=2239412

idea that it is acceptable for the government to record all Internet activity without authorization. Government surveillance of the Internet is a power with the potential for massive abuse. Like its precursor of telephone wiretapping, it must be subjected to meaningful judicial process be-fore it is authorized. We should carefully scrutinize any surveillance that threatens our intellectual privacy. Fourth, we must recognize that *surveillance is harmful*. Surveillance menaces intellectual privacy and increases the risk of blackmail, coercion, and discrimination; accord-ingly, we must recognize surveillance as a harm in constitutional standing doctrine. Explaining the harms of surveillance in a doctrinally sensitive way is essential if we want to avoid sacrificing our vital civil liberties.

I develop this argument in four steps. In Part I, I show the scope of the problem of modern "surveillance societies," in which individuals are increasingly monitored by an overlapping and entangled assemblage of government and corporate watchers. I then develop an account of why this kind of watching is problematic. Part II shows how surveillance menaces our intellectual privacy and threatens the development of individual beliefs in ways that are inconsistent with the basic commitments of democratic societies. Part III explores how surveillance distorts the power relationships between the watcher and the watched, enhancing the watcher's ability to blackmail, coerce, and discriminate against the people under its scrutiny. Part IV explores the four principles that I argue should guide the development of surveillance law, to protect us from the substantial harms of surveillance.

I. THE AGE OF SURVEILLANCE

We are living in an age of surveillance. The same digital technologies that have revolutionized our daily lives over the past three decades have also created ever more detailed records about those lives. In addition, new technologies, from surveillance cameras and web bugs to thermal scanners and GPS transponders, have increased the ability to track, observe, and monitor. The scope and variety of the types of surveillance that are possible today are unprecedented in human history. This fact alone should give us pause.

But not only have the technologies of surveillance multiplied; so too have the entities that wish to surveil. Autocratic regimes have long been the villains in the stories we tell about surveillance, but they are no longer the only governments that have stepped up their surveillance activities. Democratically elected governments in the West have deepened their commitment to surveillance of the public as well. Since 2001 this monitoring has often been done in the name of counterterrorism, but it has also been justified as protecting cybersecurity, intellectual property, children from predators, and a seemingly ever-growing list of other concerns. Some of the most well-known and

Electronic copy available at: https://ssrn.com/abstract=2239412

valuable publicly traded corporations have also got in on the act, often with the consent (in varying degrees) of their customers. Surveillance, it seems, is not just good politics, but also good business.

What, then, is surveillance? Scholars working throughout the English-speaking academy have produced a thick descriptive literature examining the nature, causes, and implications of the age of surveillance.[6] Working under the umbrella term of "surveillance studies," these scholars represent both the social sciences and humanities, with sociologists making many of the most significant contributions.[7]

Reviewing the vast surveillance studies literature, Professor David Lyon concludes that surveillance is primarily about power, but it is also about personhood.[8] Lyon offers a definition of surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction."[9] Four aspects of this definition are noteworthy, as they expand our understanding of what surveillance is and what its purposes are. First, it is *focused* on learning information about individuals. Second, surveillance is *systematic*; it is intentional rather than random or arbitrary. Third, surveillance is *routine* — a part of the ordinary administrative apparatus that characterizes modern societies.[10] Fourth, surveillance can have a wide variety of *purposes* — rarely totalitarian domination, but more typically subtler forms of influence or control.[11]

A. The Scope of Surveillance

Even a cursory overview of the kinds of surveillance that are being performed today reveals the scope of the surveillance problem. At the level of state surveillance, it should be no surprise that autocratic regimes have been among the worst offenders. For example, China has used Internet activity to detect and censor dissidents,[12] and states resisting the Arab Spring uprisings have also keenly sought social media data in order to stem the tide of the revolts.[13] Some activists also suspect that the Vietnamese government may have used computer viruses

---

[6] For three recent introductions to this vast literature, see, for example, DAVID LYON, SURVEILLANCE STUDIES (2007); SURVEILLANCE AND DEMOCRACY (Kevin D. Haggerty & Minas Samatas eds., 2010); and THE SURVEILLANCE STUDIES READER (Sean P. Hier & Joshua Greenberg eds., 2007).

[7] *See* LYON, *supra* note 6, at 18–22.

[8] *See id.* at 23.

[9] *Id.* at 14.

[10] *Id.*

[11] *See id.* at 15–16.

[12] REBECCA MACKINNON, CONSENT OF THE NETWORKED 36–40 (2012).

[13] *Id.*; Anupam Chander, Essay, *Jasmine Revolutions*, 97 CORNELL L. REV. 1505, 1516–17, 1525–28 (2012).

Electronic copy available at: https://ssrn.com/abstract=2239412

to monitor the Internet activity and private data of dissidents protesting government mining policies.[14]

Surveillance is not just for communists and dictators. Democratic states have also invested heavily in surveillance technologies in the aftermath of the September 11 attacks in America, the London subway bombings of 2005, and other atrocities. Britain is one of the most heavily surveilled countries in the world, with a network of public and private surveillance cameras, traffic enforcement cameras, and broad government powers to examine Internet traffic.[15] In the United States, the NSA has engaged in a program of warrantless wiretapping of telephone conversations. Although many of the details of the wiretapping and other surveillance programs remain shrouded in secrecy, it is clear that the investment in surveillance infrastructure remains significant. And as noted above, a 2012 investigative report by *Wired* magazine revealed that the NSA is building a massive supercomputing facility in the Utah desert, possibly with the goal of capturing and archiving much of the world's Internet traffic, with a view to decrypting and searching it as decryption technologies inevitably advance.[16]

Surveillance is not just for governments either. Private companies big and small generate vast fortunes from the collection, use, and sale of personal data. At the broadest level, we are building an Internet that is on its face free to use, but is in reality funded by billions of transactions where advertisements are individually targeted at Internet users based upon detailed profiles of their reading and consumer habits.[17] Such "behavioral advertising" is a multibillion-dollar business, and is the foundation on which the successes of companies like Google and Facebook have been built.[18] One recent study concludes that this form of surveillance is so ingrained into the fabric of the Internet "that a small number of companies have a window into most of our movements online."[19] Other technologies engage in similar forms of private surveillance. "Social reading" applications embedded into Facebook and other platforms enable the disclosure of one's reading habits,

---

[14] EVGENY MOROZOV, THE NET DELUSION 143–45 (2011).

[15] Brendan M. Palfreyman, Note, *Lessons from the British and American Approaches to Compelled Decryption*, 75 BROOK. L. REV. 345, 362 (2009). *See generally* KIRSTIE BALL ET AL., A REPORT ON THE SURVEILLANCE SOCIETY: FOR THE INFORMATION COMMISSIONER BY THE SURVEILLANCE STUDIES NETWORK (David Murakami Wood ed., 2006), *available at* http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf; *How We Are Being Watched*, BBC NEWS (Nov. 3, 2006, 2:21 AM), http://news.bbc.co.uk/2/hi/uk_news/6110866.stm.

[16] *See generally* Bamford, *supra* note 2.

[17] *See* SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING 26–30 (2011).

[18] *See* DAVID KIRKPATRICK, THE FACEBOOK EFFECT 260–66 (2010); STEVEN LEVY, IN THE PLEX 262–63, 336–37 (2011).

[19] Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 279 (2012).

Electronic copy available at: https://ssrn.com/abstract=2239412

while electronic readers like the Kindle and the Nook track reader behavior down to the specific page of the specific book on which a user's attention is currently lingering.[20]

In recent years, industry, media, and scholars have increasingly focused their attention on the concept of "Big Data," an unwieldy term often used to describe the creation and analysis of massive data sets.[21] Big Data is notable not just because of the amount of personal information that can be processed, but because of the ways data in one area can be linked to other areas and analyzed to produce new inferences and findings. As social scientists danah boyd and Kate Crawford put it, "Big Data is fundamentally networked. Its value comes from the patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself."[22] Big Data holds much potential for good in areas as diverse as medical research, the "smart" electrical grid, and traffic management.[23]

But Big Data also raises many potential problems in areas such as privacy and consumer power. For example, the retail superstore Target uses Big Data analytics to infer which of its customers are pregnant based upon their purchases of other products and upon personally identifying data from other sources.[24] As the *New York Times Magazine* reports, new parents are highly desirable customers not just because they buy many new products, but because their normally stable purchasing habits are "up for grabs" in the chaotic exhaustion that accompanies the birth of a child.[25] Target uses Big Data to snare new parents because, as one of its data analysts concedes, "[w]e knew that if we could identify them in their second trimester, there's a good chance we could capture them for years . . . . As soon as we get them buying diapers from us, they're going to start buying everything else too."[26] Big Data analytics enabled Target to discover that expectant parents display a change in buying habits (for example, buying unscented lotion and magnesium supplements) that mark them as expectant, allowing this kind of (appropriately enough) "targeted" market-

[20] Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 698–99 (2013) [hereinafter Richards, *The Perils of Social Reading*].

[21] danah boyd & Kate Crawford, Six Provocations for Big Data 6 (Sept. 21, 2011) (unpublished manuscript) (on file with the Harvard Law School Library).

[22] *Id.*

[23] *See generally* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. (forthcoming 2013).

[24] Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 16, 2012 (magazine), § 6, at 30, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[25] *Id.*

[26] *Id.*; *see also* Tom Simonite, *What Facebook Knows*, MIT TECH. REV. (June 13, 2012), http://www.technologyreview.com/featured-story/428150/what-facebook-knows/?mod=related.

Electronic copy available at: https://ssrn.com/abstract=2239412

ing. Big Data surveillance and analysis thus affect the commercial power of consumers, identifying their times of relative weakness and allowing more effective marketing to nudge them in the directions that watchful companies desire.

The incentives for the collection and distribution of private data are on the rise. The past fifteen years have seen the rise of an Internet in which personal computers and smartphones have been the dominant personal technologies. But the next fifteen will likely herald the "Internet of Things," in which networked controls, sensors, and data collectors will be increasingly built into our appliances, cars, electric power grid, and homes, enabling new conveniences but subjecting more and more previously unobservable activity to electronic measurement, observation, and control.[27] Many of us already carry GPS tracking devices in our pockets, not by government command, but in the form of powerful multifunction smartphones. Sociologists Zygmunt Bauman and David Lyon have identified the spread of surveillance beyond nonconsensual state watching to a sometimes-private surveillance in which the subjects increasingly consent and participate — a phenomenon that they call "liquid surveillance."[28] Professor Scott Peppet foresees the "unraveling" of privacy,[29] as economic incentives lead consumers to agree to surveillance devices like Progressive Insurance's "MyRate" program, which offers reduced insurance rates in exchange for the installation of a device that monitors driving speed, time, and habits.[30] Peppet argues that this unraveling of privacy creates a novel challenge to privacy law, which has long focused on unconsented surveillance rather than on surveillance as part of an economic transaction.[31]

It might seem curious to think of information gathering by private entities as "surveillance." Notions of surveillance have traditionally been concerned with the watchful gaze of government actors like police and prison officials rather than companies and individuals. But in a postmodern age of "liquid surveillance," the two phenomena are deeply intertwined. Government and nongovernment surveillance support each other in a complex manner that is often impossible to disentangle. At the outset, the technologies of surveillance — software, RFID chips, GPS trackers, cameras, and other cheap sensors —

---

[27] Clive Thompson, *Sensors Everywhere*, WIRED, Dec. 2012, at 72, *available at* http://www.wired.com/opinion/2012/12/20-12-st_thompson/. For a critique of the "Internet of Things," see ROB VAN KRANENBURG, THE INTERNET OF THINGS (2008), *available at* http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf.

[28] ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE 2–3 (2013).

[29] Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1156 (2011).

[30] *Id.* at 1153–56.

[31] *Id.*

Electronic copy available at: https://ssrn.com/abstract=2239412

are being used almost interchangeably by government and nongovernment watchers.[32] Private industry is also marketing new surveillance technologies to the state. Though it sounds perhaps like a plot from a paranoid science fiction novel, the *Guardian* reports that the Disney Corporation has been developing facial recognition technologies for its theme parks and selling the technology to the U.S. military.[33] Nor do the fruits of surveillance respect the public/private divide. Since the September 11 attacks, governments have been eager to acquire the massive consumer and Internet-activity databases that private businesses have compiled for security and other purposes, either by subpoena[34] or outright purchase.[35] Information can also flow in the other direction; the U.S. government recently admitted that it was giving information to insurance companies that it had collected from automated license-plate readers at border crossings.[36]

Similarly, while government regulation might be one way to limit or shape the growth of the data industry in socially beneficial ways, governments also have an interest in making privately collected data amenable to public-sector surveillance. In the United States, for example, the Communications Assistance for Law Enforcement Act of 1994[37] requires telecommunications providers to build their networks in ways that make government surveillance and interception of electronic communications possible.[38] A European analogue, the EC Data Retention Directive Regulations of 2009, requires Internet service providers to retain details of all Internet access, email, and Internet telephony by users for twelve months, so that they can be made available to government investigators for cases of antiterrorism, intellectual property, child protection, or for other purposes.[39] This surveillant symbiosis between companies and governments means that no analysis of surveillance can be strictly limited to just the government or the market in isolation. Surveillance must instead be understood in its aggregated and complex social context.

---

[32] *See* LYON, *supra* note 6, at 111–12.

[33] Naomi Wolf, *The New Totalitarianism of Surveillance Technology*, GUARDIAN (Aug. 15, 2012, 4:12 PM), http://www.guardian.co.uk/commentisfree/2012/aug/15/new-totalitarianism-surveillance-technology.

[34] *See* Gonzales v. Google, Inc., 234 F.R.D. 674, 688 (N.D. Cal. 2006).

[35] *See* O'HARROW, *supra* note 1, at 64, 98–103.

[36] Cyrus Farivar, *License Plates Scanned at Border, Data Shared with Car Insurance Group*, ARS TECHNICA (Aug. 22, 2012, 4:36 PM), http://arstechnica.com/tech-policy/2012/08/license-plates-scanned-at-border-data-shared-with-car-insurance-group/.

[37] 47 U.S.C. §§ 1001–1010 (2006).

[38] *Id.* § 1002.

[39] The United Kingdom version of this regulation is The Data Retention (EC Directive) Regulations, 2009, S.I. 2009/859 (U.K.), *available at* http://www.legislation.gov.uk/ukdsi/2009/9780111473894/contents.

Electronic copy available at: https://ssrn.com/abstract=2239412

B. Surveillance Law's Limited Protections

American law governing surveillance is piecemeal, spanning constitutional protections such as the Fourth Amendment, statutes like the Electronic Communications Privacy Act of 1986[40] (ECPA), and private law rules such as the intrusion-into-seclusion tort.[41] But the general principle under which American law operates is that surveillance is legal unless forbidden. Perhaps out of a fear that surveillance might be used to suppress dissent, American law contains some limited protections against government surveillance of purely political activity. For example, government investigators in antiterrorism cases possess a powerful tool known as the National Security Letter (NSL). NSLs are statutory authorizations by which the FBI can obtain information about people from their telephone companies, Internet service providers, banks, credit agencies, and other institutions with which those people have a relationship. NSLs are covert and come with a gag order that prohibits the recipient of the letter from disclosing its existence, even to the person whose secrets have been told to the government. NSLs can currently be obtained under four federal statutes: the Right to Financial Privacy Act of 1978[42] (RFPA), the ECPA,[43] the Fair Credit Reporting Act[44] (FCRA), and the National Security Act of 1947.[45] Taken together, these provisions allow the FBI to access a wide variety of information about people, including historical and transactional information relating to telephone calls and emails, financial information, and consumer credit information.[46] This information can be obtained by crossing a very low threshold — the FBI must merely certify in writing that the request is "relevant to an authorized investigation to protect against international terrorism or clandestine

---

[40] Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[41] *See generally* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).

[42] 12 U.S.C. §§ 3401–3422 (2006 & Supp. V 2011) (allowing access to personal financial records held by a wide variety of entities, including casinos, insurance companies, automobile dealerships, credit unions, real estate companies, and travel agencies).

[43] 18 U.S.C. § 2709 (allowing access to telephone and email information including billing and call history, email, subscriber information, and screen names).

[44] 15 U.S.C. §§ 1681–1681x (2006 & Supp. V 2011); *see also id.* § 1681u (allowing access to credit history information and the header information on credit reports, including name, address, and employment history); *id.* § 1681v (allowing access to a consumer's full credit report and "all other information in a consumer's file").

[45] 50 U.S.C. §§ 401–442b (2006 & Supp. V 2011); *see also id.* § 436 (allowing the issuance of NSLs in connection with investigations of improper disclosure of classified information by government employees).

[46] *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 10 (2007).

Electronic copy available at: https://ssrn.com/abstract=2239412

intelligence activities."[47] Communications and bank records sought under the ECPA and the RFPA are protected by the additional requirement that the FBI certify that "such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States."[48]

Despite these protections, courts lack the tools to enforce them. This problem predates the current NSL framework. For example, in 1967, the President ordered the U.S. Army to engage in surveillance of domestic dissident groups, fearing civil disorder in the aftermath of the assassination of Martin Luther King, Jr.[49] The program expanded over time to become a large-scale military surveillance program of the domestic political activities of American citizens.[50] In *Laird v. Tatum*,[51] the Supreme Court held that it lacked jurisdiction over the claims that the surveillance violated the First Amendment rights of the subjects of the program, because the subjects claimed only that they felt deterred from exercising their First Amendment rights or that the government could misuse the information it collected in the future.[52] The Court could thus declare that "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[53]

More recent surveillance cases have followed the lead of the *Laird* Court. Challenges to the NSA's wiretapping program have foundered because plaintiffs have failed to convince federal courts that secret surveillance has caused them any legally cognizable injury. In *ACLU v. NSA*,[54] the Sixth Circuit dismissed any suggestion that First Amendment values were threatened when the government listened to private conversations. As that court put it: "The First Amendment protects public speech and the free exchange of ideas, while the Fourth Amendment protects citizens from unwanted intrusion into their personal lives and effects."[55] The court concluded that the plaintiffs had

---

[47] This precise language is quoted from the ECPA, 18 U.S.C. § 2709(b)(1)–(2), but the other NSL provisions are substantially similar. *See* 12 U.S.C. § 3414(a)(5)(A) (RFPA); 15 U.S.C. §§ 1681u(b), 1681v(a) (FCRA); 50 U.S.C. § 436(a)(3) (National Security Act).

[48] 18 U.S.C. § 2709(b)(1)–(2) (ECPA); 12 U.S.C. § 3414(a)(5)(A) (RFPA). The original FCRA NSL provision allowing access to the headers of credit reports only, 15 U.S.C. § 1681u(b), contains such a First Amendment limitation, but since the Patriot Act added § 1681v, which allows for the full credit report to be obtained without meeting the First Amendment requirement, it is unclear what practical effect the limitation in § 1681u(b) will have.

[49] *See* Laird v. Tatum, 408 U.S. 1, 4–5 (1972).

[50] *See id.* at 6–7.

[51] 408 U.S. 1.

[52] *Id.* at 13.

[53] *Id.* at 13–14.

[54] 493 F.3d 644 (6th Cir. 2007).

[55] *Id.* at 657 n.15 (citations omitted).

Electronic copy available at: https://ssrn.com/abstract=2239412

no standing to assert First or Fourth Amendment violations, as they could not prove that the secret government surveillance program had targeted them.[56] Similarly, in *Al-Haramain Islamic Foundation, Inc. v. Bush*,[57] the government successfully invoked the state-secrets doctrine to stop the plaintiffs from finding out whether they were the subjects of secret surveillance under the program.[58] This ruling created a brutal paradox for the plaintiffs: they could not prove whether their telephone calls had been listened to, and thus they could not establish standing to sue for the violation of their civil liberties.[59] Despite the fact that the judges in the case knew whether surveillance had taken place, they believed that the state-secrets doctrine barred them from ruling on that fact.[60] And the Court's most recent decision in *Clapper* affirmed this approach to standing to challenge surveillance. Plaintiffs can only challenge secret government surveillance they can prove, but the government isn't telling. Plaintiffs (and perhaps civil liberties) are out of luck.

So far so bad. Or maybe not. Putting the oppression of totalitarian states to one side, public and private surveillance can have beneficial effects. All other things being equal, greater security from crime and terrorism is a good thing.[61] So too are the conveniences of modern communications, email, and the power of a search engine in our pockets valuable advances that improve our quality of life. And a sensible system of automated traffic regulation can save money and direct scarce police resources to serious criminals rather than ordinary motorists.

As a society, we are thus of two minds about surveillance. On the one hand, it is creepy, Orwellian, and corrosive of civil liberties. On the other hand, it keeps us and our children safe. It makes our lives more convenient and gives us the benefit of a putatively free Internet. Moreover, some influential thinkers argue that data surveillance does not affect privacy at all. As Judge Posner puts it:

> The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their vol-ume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting,

[56] *Id.* at 673–74.
[57] 507 F.3d 1190 (9th Cir. 2007).
[58] *Id.* at 1204.
[59] *See id.* at 1205.
[60] *See id.* at 1204–05.
[61] *See* RICHARD A. POSNER, NOT A SUICIDE PACT 130 (2006) (arguing that adherence to civil liberties like the right to privacy must be flexible where it conflicts with government antiterrorism efforts).

Electronic copy available at: https://ssrn.com/abstract=2239412

> far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.[62]

Surveillance is thus confusing. We like its benefits, though we are fearful (and sometimes dismissive) of its costs. This confusion points to a larger problem: civil liberties advocates lack a compelling account of when and why (if at all) surveillance is harmful. As a society, we have an intuitive understanding that public- and private-sector surveillance is potentially bad, but we do not have an articulate explanation of why it is bad. Some of our intuitions stem from literature, such as George Orwell's chilling portrait of Big Brother in *Nineteen Eighty-Four*.[63] But few critics of government surveillance such as the NSA wiretapping program and the British data-retention regulations would suggest that these programs are directly analogous to the evil regime depicted in Orwell's dystopia. Moreover, the Orwell metaphor seems wholly inapplicable to databases used to personalize targeted advertising on the web, the efforts of insurance companies to promote safe driving, and the practices of online booksellers to sell more books by monitoring consumers' shopping habits in ways that used to be impossible.[64]

We need an account of when and why surveillance is problematic to help us see when we should regulate and when we should not. The following Parts seek to provide an account of some of the dangers of surveillance and the ways in which laws could mitigate them. I want to advance two lines of critique to the notion that surveillance does not create a legally cognizable injury: first, that surveillance by government and private actors threatens intellectual privacy and chills the exercise of vital civil liberties; and second, that surveillance affects the power balance between individuals and those who are watching, increasing the risk of persuasion, blackmail, and other harmful uses of sensitive information by others.

II. SURVEILLANCE AND INTELLECTUAL PRIVACY

The most salient harm of surveillance is that it threatens a value I have elsewhere called "intellectual privacy."[65] Intellectual-privacy

---

[62] Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html.

[63] GEORGE ORWELL, NINETEEN EIGHTY-FOUR (Irving Howe ed., Harcourt Brace Jovanovich, Inc. 1982) (1949).

[64] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON 29–36 (2004) (critiquing the usefulness of Orwell's metaphor as a tool in understanding the private database industry). *But see* Neil M. Richards, Essay, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1133 (2006) (suggesting that the Orwell metaphor retains some validity as a tool to understand electronic surveillance).

[65] Richards, *Intellectual Privacy*, *supra* note 5, at 389; Richards, *The Perils of Social Reading*, *supra* note 20, at 691.

Electronic copy available at: https://ssrn.com/abstract=2239412

theory suggests that new ideas often develop best away from the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing; and that a meaningful guarantee of privacy — protection from surveillance or interference — is necessary to promote this kind of intellectual freedom. It rests on the idea that free minds are the foundation of a free society, and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse.[66] I want to be clear at the outset that intellectual-privacy theory protects "intellectual" activities, broadly defined — the processes of thinking and making sense of the world with our minds. Intellectual privacy has its limits — it is a subset of all things that we might call "privacy," albeit a very important subset. But importantly, intellectual privacy is not just for intellectuals; it is an essential kind of privacy for us all.

At the core of the theory of intellectual privacy are two claims, one normative and one empirical. The normative claim is that the foundation of Anglo-American civil liberties is our commitment to free and unfettered thought and belief — that free citizens should be able to make up their own minds about ideas big and small, political and trivial. This claim requires at a minimum protecting individuals' rights to think and read, as well as the social practice of private consultation with confidantes. It may also require some protection of broader social rights, whether we call them rights of association or assembly.[67] Protection of these individual rights and social practices allows individuals to develop both intellectual diversity and eccentric individuality. They reflect the conviction that big ideas like truth, value, and culture should be generated from the bottom up rather than from the top down.[68]

These commitments to the freedoms of thought, belief, and private speech lie at the foundation of traditional First Amendment theory, though they have been underappreciated elements of that tradition. But as I have argued elsewhere, a careful examination reveals that a commitment to freedom of thought is present in virtually every major text in First Amendment theory.[69] In particular, freedom of thought lies at the core of the modern American tradition of First Amendment libertarianism, which began with the opinions of Justices Holmes and

---

[66] Richards, *Intellectual Privacy*, *supra* note 5, at 403–04.

[67] *See, e.g.*, Ashutosh Bhagwat, *Associational Speech*, 120 YALE L.J. 978, 998 (2011) ("An association is a coming together of individuals for a common cause or based on common values or goals."). *See generally* JOHN D. INAZU, LIBERTY'S REFUGE (2012) (arguing for the protection of political- and religious-group autonomy under the alternative rubric of the right of assembly).

[68] *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF (2012).

[69] *See* Richards, *Intellectual Privacy*, *supra* note 5, at 408–12 (exploring this point in greater detail). For a similar argument, see generally Seana Valentine Shiffrin, *A Thinker-Based Approach to Freedom of Speech*, 27 CONST. COMMENT. 283 (2011).

Electronic copy available at: https://ssrn.com/abstract=2239412

Brandeis in the decade following the end of the First World War. Dissenting from the majority position of the Supreme Court, the two friends developed theories that justified special protection for speech and ideas under the First Amendment. The two men advanced slightly different reasons why speech should be protected — Justice Holmes justified protection in terms of the search for truth, while Justice Brandeis privileged democratic self-government — but each theory enshrined protection for free thought at its core. For example, Justice Holmes's dissent in *Abrams v. United States*[70] is a forceful statement of the idea that democratic institutions depend on minds' being able to freely and fearlessly engage in the search for political truth. As he put it poetically:

> [W]hen men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas — that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.[71]

Justice Brandeis also placed the freedom of thought at the foundation of his justification for special protection for free speech. In *Whitney v. California*,[72] he wrote:

> Those who won our independence believed that *the final end of the State was to make men free to develop their faculties*; and that in its government the deliberative forces should prevail over the arbitrary. They valued liberty both as an end and as a means. They believed liberty to be the secret of happiness and courage to be the secret of liberty. *They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth . . . .*[73]

Thus, in each of the traditional American justifications for freedom of speech,[74] a commitment to freedom of thought — to intellectual freedom — rests at the core of the tradition.

---

[70] 250 U.S. 616 (1919).

[71] *Id.* at 630 (Holmes, J., dissenting).

[72] 274 U.S. 357 (1927).

[73] *Id.* at 375 (Brandeis, J., concurring) (emphasis added).

[74] Although most courts justify free speech in terms of truth-seeking or democratic self-governance, some scholars have argued that free speech is better justified in terms of the autonomy or self-development of the individual. *See, e.g.*, C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 UCLA L. REV. 964, 990–92 (1978); Martin H. Redish, *The Value of Free Speech*, 130 U. PA. L. REV. 591, 593–94 (1982); David A. J. Richards, *Free Speech and Obscenity Law: Toward a Moral Theory of the First Amendment*, 123 U. PA. L. REV. 45, 62 (1974); Thomas Scanlon, *A Theory of Freedom of Expression*, 1 PHIL. & PUB. AFF. 204, 210–19 (1972). Free thought is a logically necessary precondition for autonomous speech, though this point is underdeveloped in the relevant literature. For an analysis of the relationship between free thought and autonomous speech, see Richards, *Intellectual Privacy*, *supra* note 5, at 406 & n.113, and see generally Shiffrin, *supra* note 69.

Electronic copy available at: https://ssrn.com/abstract=2239412

The second claim at the core of the theory of intellectual privacy is an empirical one — that surveillance inclines us to the mainstream and the boring. It is a claim that when we are watched while engaging in intellectual activities, broadly defined — thinking, reading, web-surfing, or private communication — we are deterred from engaging in thoughts or deeds that others might find deviant. Surveillance thus menaces our society's foundational commitments to intellectual diversity and eccentric individuality.

Three different kinds of arguments highlight the ways in which surveillance can restrain intellectual activities. The first set of arguments relies on cultural and literary works exploring the idea that surveillance deters eccentric or deviant behavior. Many such works owe a debt to Jeremy Bentham's idea of the Panopticon, a prison designed around a central surveillance tower from which a warden could see into all of the cells. In the Panopticon, prisoners had to conform their activities to those desired by the prison staff because they had no idea when they were being watched. As Bentham describes this system, "[t]o be incessantly under the eyes of an Inspector is to lose in fact the power of doing ill, and almost the very wish."[75] Of course, the most famous cultural exploration of the conforming effects of surveillance is Orwell's harrowing depiction in *Nineteen Eighty-Four* of the totalitarian state personified by Big Brother.[76] Orwell's fictional state sought to prohibit not just verbal dissent from the state but even the thinking of such ideas, an act punished as "thoughtcrime" and deterred by constant state surveillance.[77] Some scholars have documented how the modern surveillance environment differs from both the classic Panopticon and a fully realized Big Brother in important ways.[78] Nevertheless, Orwell's insight about the effects of surveillance on thought and behavior remains valid — the fear of being watched causes people to act and think differently from the way they might otherwise.

Our cultural intuitions about the effects of surveillance are supported by a second set of arguments that comes from the empirical work of scholars in the interdisciplinary field of surveillance studies. Moving beyond the classic metaphors of the Panopticon and Big Brother, these scholars have tried to understand modern forms of surveillance by governments, companies, and individuals in all of their

---

[75] Jeremy Bentham, *Panopticon*, *in* 3 OPINIONS OF DIFFERENT AUTHORS UPON THE PUNISHMENT OF DEATH 321, 328 (Basil Montagu ed., 1816).

[76] ORWELL, *supra* note 63, at 4.

[77] *Id.* at 14.

[78] *See, e.g.*, Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. SOC. 605, 606–08 (2000); SOLOVE, *supra* note 64, at 33–35.

Electronic copy available at: https://ssrn.com/abstract=2239412

complexities.[79] The scope of this burgeoning literature has been wide-ranging and provides many examples of the normalizing effects of surveillance in a wide variety of contexts. In his pioneering work in the 1980s, for example, Professor Anthony Giddens argues that surveillance continually seeks the supervision of social actors and carries with it a permanent risk that supervision could lead to domination.[80] More recent scholars have explored the risks that surveillance poses to democratic self-governance.[81] One such risk is that of self-censorship, in terms of speech, action, or even belief. Studies of communist states give social-scientific accounts of many of the cultural intuitions about these self-censoring effects of surveillance,[82] but so too do studies of modern forms of surveillance in democratic societies. For example, one study of the EU Data Retention Directive notes that "[u]nder pervasive surveillance, individuals are inclined to make choices that conform to mainstream expectations."[83] As I explore below, the scope of surveillance studies is much broader than merely the study of panoptic state surveillance; scholars working in this field have examined the full scope of modern forms of watching, including data surveillance by private actors. But above all, surveillance scholars continually reaffirm that, while surveillance by government and others can have many purposes, a recurrent purpose of surveillance is to control behavior.[84]

A third and final set of arguments for intellectual privacy comes from First Amendment doctrine. A basic principle of free speech law as it has developed over the past century is that free speech is so important that its protection should err on the side of caution. Given the uncertainty of litigation, the Supreme Court has created a series of procedural devices to attempt to ensure that errors in the adjudication of free speech cases tend to allow unlawful speech rather than engage in mistaken censorship. These doctrines form what Professor Lee Bollinger calls the "First Pillar" of First Amendment law — the "[e]xtraordinary [p]rotection against [c]ensorship."[85] Such doctrines take various forms, such as those of prior restraint, overbreadth, and vagueness, but they are often characterized under the idea of the "chilling effect." This idea maintains that rules that might deter potentially valuable expression should be treated with a high level of suspi-

---

[79] *See generally* LYON, *supra* note 6.

[80] *See generally* ANTHONY GIDDENS, THE NATION-STATE AND VIOLENCE (1985).

[81] *See generally, e.g.*, SURVEILLANCE AND DEMOCRACY, *supra* note 6.

[82] *See, e.g.*, Maria Los, *A Trans-Systemic Surveillance: The Legacy of Communist Surveillance in the Digital Age*, *in* SURVEILLANCE AND DEMOCRACY, *supra* note 6, at 173, 174–75.

[83] Lilian Mitrou, *The Impact of Communications Data Retention on Fundamental Rights and Democracy — The Case of the EU Data Retention Directive*, *in* SURVEILLANCE AND DEMOCRACY, *supra* note 6, at 127, 138.

[84] *See, e.g.*, LYON, *supra* note 6, at 15; BALL ET AL., *supra* note 15, at 4.

[85] LEE C. BOLLINGER, UNINHIBITED, ROBUST, AND WIDE-OPEN 12 (2010).

Electronic copy available at: https://ssrn.com/abstract=2239412

cion by courts. As the Supreme Court put it in perhaps its most important free speech decision of the twentieth century, *New York Times Co. v. Sullivan*,[86] the importance of uninhibited public debate means that, although "erroneous statement is inevitable in free debate, . . . it must be protected if the freedoms of expression are to have the 'breathing space' that they 'need . . . to survive.'"[87] As Professor Frederick Schauer explains, "the chilling effect doctrine recognizes the fact that the legal system is imperfect and mandates the formulation of legal rules that reflect our preference for errors made in favor of free speech."[88] Although the chilling-effect doctrine has been criticized on grounds that it overprotects free speech and makes empirically unsupported judgments,[89] such criticisms miss the point. The doctrines encapsulated by the chilling effect reflect the substantive value judgment that First Amendment values are too important to require scrupulous proof to vindicate them, and that it is (constitutionally speaking) a better bargain to allow more speech, even if society must endure some of that speech's undesirable consequences.

Intellectual-privacy theory explains why we should extend chilling-effect protections to intellectual surveillance, especially traditional-style surveillance by the state. If we care about the development of eccentric individuality and freedom of thought as First Amendment values, then we should be especially wary of surveillance of activities through which those aspects of the self are constructed.[90] Professor Timothy Macklem argues that "[t]he isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and the subversive."[91] A meaningful measure of intellectual privacy should be erected to shield these activities from the normalizing gaze of surveillance. This shield should be justified on the basis of our cultural intuitions and empirical insights about the normalizing effects of surveillance. But it must also be tempered by the chilling-effect doctrine's normative commitment to err on the side of First Amendment values even if proof is imperfect.

---

[86] 376 U.S. 254 (1964).

[87] *Id.* at 271–72 (second omission in original) (quoting NAACP v. Button, 371 U.S. 415, 433 (1963)).

[88] Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 688 (1978).

[89] *See generally, e.g.*, Leslie Kendrick, *Speech, Intent and the Chilling Effect*, 54 WM. & MARY L. REV. (forthcoming 2013).

[90] *See* COHEN, *supra* note 68, at 223–25; Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912, 1918 (2013).

[91] TIMOTHY MACKLEM, INDEPENDENCE OF MIND 36 (2006).

Electronic copy available at: https://ssrn.com/abstract=2239412

Intellectual-privacy theory therefore suggests a solution to the confusion that has plagued courts and others in dealing with whether surveillance programs create legally cognizable injuries. Despite often displaying an intuitive understanding that surveillance might be potentially harmful, courts have struggled to understand why. This absence of clarity has led to courts misunderstanding and diminishing privacy interests that conflict with other values. When faced with balancing a vague and poorly articulated privacy right against state interests such as the prevention of terrorist attacks, surveillance tends to win. Courts also make the mistake that the *ACLU v. NSA* court made and cast surveillance as solely a Fourth Amendment issue of crime prevention, rather than as one that also threatens intellectual freedom and First Amendment values of the highest order.[92] Other decisions mirror the mistake of the *Al-Haramain* court in concluding that preventing secret surveillance is less important than inconveniencing the executive branch.[93] Additionally, some courts can make the mistake that the *Clapper* Court made, refusing to recognize as justiciable harms the costly measures that people must adopt to shield their communications from government surveillance.[94]

Shadowy regimes of surveillance corrode the constitutional commitment to intellectual freedom that lies at the heart of most theories of political freedom in a democracy. Secret programs of wide-ranging intellectual surveillance that are devoid of public process and that cannot be justified in court are inconsistent with this commitment and illegitimate in a free society. My argument is not that intellectual surveillance should never be possible, but that when the state seeks to learn what people are reading, thinking, and saying privately, such scrutiny is a serious threat to civil liberties. Accordingly, meaningful legal process (that is, at least a warrant supported by probable cause) must be followed before the government can perform the digital equivalent of reading our diaries.

But we must also remember that in modern societies, surveillance fails to respect the line between public and private actors. Intellectual privacy should be preserved against private actors as well as against the state. Federal prosecutions based on purely intellectual surveillance are thankfully rare, but the coercive effects of monitoring by our friends and acquaintances are much more common. We are constrained in our actions by peer pressure at least as much as by the state. Moreover, records collected by private parties can be sold to or subpoenaed by the government, which (as noted above) has shown a

[92] *See* ACLU v. NSA, 493 F.3d 644, 657 (6th Cir. 2007).
[93] *See* Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1201–05 (9th Cir. 2007).
[94] *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150–53 (2013).

Electronic copy available at: https://ssrn.com/abstract=2239412

voracious interest in all kinds of personal information, particularly records related to the operation of the mind and political beliefs.[95] Put simply, the problem of intellectual privacy transcends the public/private divide, and justifies additional legal protections on intellectual privacy and the right to read freely.[96] Constitutional law and standing doctrine alone will not solve the threat of surveillance to intellectual freedom and privacy, but they are a good place to start.

III. SURVEILLANCE AND POWER

The mechanics of intellectual privacy discussed so far depend upon knowing, or at least fearing, that someone might be watching us. If we have a sense of privacy, even one that turns out to be an illusion, we are less likely to change our behavior under the panoptic gaze. Truly secret and unexpected surveillance, from this perspective, might appear not to violate our intellectual privacy at all. If we have no inkling that we are being watched, if we really do not care that we are being watched, or if we fear no consequences of being watched, it could be argued that our intellectual freedom is unaffected. It can thus be argued that if the NSA Wiretapping Program had never leaked, it would have posed no threat to intellectual privacy.

There are two problems with this account. First, no program of widespread surveillance is likely to remain secret forever. At some point, such a program will inevitably come to light, either by being leaked (as happened with the NSA program and the Army surveillance in *Laird*), or by actions taken pursuant to the program (such as prosecutions or disclosures). The injury suffered by those thus punished would serve as an example to the rest of us, and the mechanisms of intellectual privacy would come into effect at that point.

Second, surveillance (even secret surveillance) can create additional harms that are separate from the ones suggested by intellectual-privacy theory. Scholars working in surveillance studies have explored the phenomenon of surveillance in all of its contemporary complexity, going beyond the Panopticon to consider private surveillance, the relationships between watchers and watched, and the wide variety of dangers that modern surveillance societies raise.[97] Recall in this regard that Lyon's definition of surveillance notes that surveillance has a purpose,[98] but in the modern era this purpose is rarely totalitarian domination. All the same, most forms of surveillance seek some form

[95] *See* Richards, *Intellectual Privacy*, *supra* note 5, at 427–28 (providing examples).

[96] *See generally* Richards, *The Perils of Social Reading*, *supra* note 20.

[97] *See, e.g.*, Kevin D. Haggerty & Minas Samatas, *Introduction*, *in* SURVEILLANCE AND DEMOCRACY, *supra* note 6, at 1, 3–4.

[98] *See* LYON, *supra* note 6, at 14.

Electronic copy available at: https://ssrn.com/abstract=2239412

of subtler influence or control over others. Even when surveillance is not Orwellian, it is usually about influencing or being able to respond to someone else's behavior. And while surveillance can sometimes have benign goals (like traffic safety, or parents using baby monitors or GPS trackers to keep tabs on their children), it is invariably tied to a particular purpose. Critically, the gathering of information affects the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance.[99] It might sound trite to say that "information is power," but the power of personal information lies at the heart of surveillance. The power effects of surveillance illustrate three additional dangers of surveillance: blackmail, discrimination, and persuasion.

A. Blackmail

Information collected surreptitiously can be used to blackmail or discredit opponents by revealing embarrassing secrets. American political history over the past hundred years furnishes numerous examples of this phenomenon, but perhaps the most compelling is the treatment of Martin Luther King, Jr., by the FBI. Concerned that Dr. King was a threat to public order, the FBI listened to his private telephone conversations in order to seek information with which to blackmail him. As the official government investigation into the Dr. King wiretaps concluded in 1976:

> The FBI collected information about Dr. King's plans and activities through an extensive surveillance program, employing nearly every intelligence-gathering technique at the Bureau's disposal. Wiretaps, which were initially approved by Attorney General Robert F. Kennedy, were maintained on Dr. King's home telephone from October 1963 until mid-1965; the SCLC headquarter's [sic] telephones were covered by wiretaps for an even longer period. Phones in the homes and offices of some of Dr. King's close advisers were also wiretapped. The FBI has acknowledged 16 occasions on which microphones were hidden in Dr. King's hotel and motel rooms in an "attempt" to obtain information about the "private activities of King and his advisers" for use to "completely discredit" them.[100]

Imagine a dissident like Dr. King living in today's information age. A government (or political opponent) that wanted him silenced might be able to obtain not just access to his telephone conversations, but also to his reading habits and emails. This critic could be blackmailed outright, or he could be discredited by disclosure of the information as an example to others. Perhaps he has not been having an affair, but has some other secret. Maybe he is gay, or has a medical condition, or

---

[99] *See id.*

[100] S. REP. NO. 94-755, at 81 (1976) (quoting Memorandum from Frederick Baumgardner to William Sullivan (Jan. 28, 1964)).

Electronic copy available at: https://ssrn.com/abstract=2239412

visits embarrassing web sites, or has cheated on his expenses or his taxes. All of us have secrets we would prefer not be made public. Surveillance allows those secrets greater opportunities to come out, and it gives the watchers power that can be used nefariously.

The risk of the improper use of surveillance records persists over time. Most of the former communist states in Eastern Europe have passed laws strictly regulating access to the surveillance files of the communist secret police. The primary purpose of such laws is to prevent the blackmail of political candidates who may have been surveilled under the former regime.[101] The experience of these laws reveals, moreover, that the risk of such blackmail is one that the law cannot completely prevent after the fact. Professor Maria Los explains that "[s]ecret surveillance files are routinely turned into a weapon in political struggles, seriously undermining democratic processes and freedoms."[102]

More recently, the world observed some of the potential of electronic blackmail during the revolutions in the Arab world. Many observers have argued that the turmoil in Tunisia, Libya, and Syria shows the liberating potential of digital technologies.[103] But the crisis also illustrates the potential of modern surveillance technologies, which have been deployed by authoritarian governments across the Middle East. The Libyan government of Colonel Moammar Gadhafi, for example, attempted to capture Internet and phone communications with the assistance of Western technology companies for later review. As one journalist remarked about the availability of such "'massive intercept' technology" to governments around the world, "[t]oday you can run an approximation of *1984* out of a couple of rooms filled with server racks."[104] Using these technologies, the Libyan government obtained information about dissidents that it was able to use to blackmail them into silence. And while the Gadhafi regime did not hesitate to use violence against its critics, it found blackmail and harassment to be even easier tools to use.[105] The fact that the Gadhafi regime ultimately collapsed does not diminish surveillance's blackmail threat.

Even in democratic societies, the blackmail threat of surveillance is a real one. Surveillance (especially secret surveillance) often detects crimes or embarrassing activity beyond or unrelated to its original purposes. The surveillance of Dr. King, for instance, produced evidence of his marital infidelity. In another infamous case, FISA-authorized surveillance of a terrorist suspect produced chilling evi-

---

[101] Los, *supra* note 82, at 176–77.
[102] *Id.* at 180.
[103] *See, e.g.*, Chander, *supra* note 13, at 1508.
[104] Matthieu Aikins, *Jamming Tripoli*, WIRED, June 2012, at 146, 176.
[105] *Id.*

Electronic copy available at: https://ssrn.com/abstract=2239412

dence of the suspect's murder of his own daughter for dating the wrong boy.[106] Whether these discoveries are important, incidental, or irrelevant, all of them give greater power to the watcher. Unscrupulous government officials could engage in blackmail, whether motivated by political or pecuniary considerations. But even faithful government agents who discover illegal activity would now possess the weapon of selective prosecution, which could be used to influence the subject, and would be able to wield the threat of mere disclosure of legal but embarrassing activity. Putting the seriousness of the crime to one side, it is important to realize that wide-ranging secret surveillance gives coercive power to the watcher.

B. Persuasion

Surveillance also gives the watcher increased power to persuade. Persuasion is a more subtle exercise of the power differential that can be used to blackmail, but it can be even more effective. Consider again Target's use of Big Data to lure pregnant customers into its stores. Even if the customers have told no one that they are expecting, Big Data analytics can look for correlations between pregnancy and other changes in consumer behavior, for instance, purchasing more vitamins or scent-free lotions. Once an inference of pregnancy is established, Target's marketers can offer coupons to the pregnant woman in order to capture her business, knowing that she is at a point in her life when her buying habits are temporarily in flux before they will lock in for a period of some years. It is entirely possible that such actions by a retailer like Target could occur without the knowledge of the pregnant consumer. Indeed, the science of targeted online or "behavioral" advertising seeks to do exactly that: to market products to consumers based upon detailed profiles collected about their behavior. The effective sales technique of behavioral "retargeting" allows marketers to go one step further and literally follow targeted consumers around the web, delivering the same targeted advertisement to them with enough frequency that they are likely eventually to succumb and make a purchase in a moment of weakness.[107]

Governments also use the power of surveillance to control behavior. For example, one of the justifications for massive closed-circuit television (CCTV) networks in modern urban areas is that they allow police greater ability to watch and influence what happens on city streets.[108] Certainly, the presence of cameras or police can persuade citizens to obey the law, but it can have other effects as well. The surveillance-

[106] United States v. Isa, 923 F.2d 1300, 1302 (8th Cir. 1991).
[107] ELI PARISER, THE FILTER BUBBLE 44 (2011).
[108] *See* LYON, *supra* note 6, at 107–08.

Electronic copy available at: https://ssrn.com/abstract=2239412

studies literature has documented the use of government CCTV assemblages to direct public behavior toward commerce and away from other activities ranging from crime to protest.[109] In Britain, where the science of surveillance-based control is at its most advanced, CCTV operates in connection with court-ordered injunctions, known as Anti-Social Behavior Orders, to move groups of teens out of the commercial cores of cities using surveillance and the power of the state to ensure that commerce continues efficiently.[110] Government use of persuasive surveillance is still in its relative infancy, but since the technologies of surveillance and Big Data analytics are available to the state as well as to private companies, we can imagine the government becoming increasingly able to engage in Target-style persuasion in the future.

The bottom line about surveillance and persuasion is that surveillance gives the watcher information about the watched. That information gives the watcher increased power over the watched that can be used to persuade, influence, or otherwise control them, even if they do not know they are being watched or persuaded. Sometimes this power is arguably a good thing, for example when police are engaged in riot control. But we should not forget that surveillance represents a persuasive power shift whether the watcher is a government agent or a corporate marketer, and whether the target is a rioter or law-abiding citizen. The legal system has rules dealing with power imbalances between consumers and businesses, such as the doctrine of unconscionability and much of consumer protection law. There are also rules protecting citizens from state coercion, such as the unconstitutional conditions doctrine and the First Amendment's protections of freedom of thought and conscience. In our age of surveillance, where technological change has given the watcher enhanced powers of persuasion, it may well be time to think about updating those doctrines to restore the balance.

C. Sorting/Discrimination

Many kinds of surveillance are routinely used to sort people into categories. Some of these forms of sorting are insidious. Consider, for example, the use of census records by the American, Canadian, and German governments during the Second World War to identify citizens to relocate to the Japanese internment camps in North America and the concentration camps in Europe.[111] Others seem innocuous or even benign. The vast preference engines that power the "free" Internet are

---

[109] *See, e.g.*, ROY COLEMAN, RECLAIMING THE STREETS 226–28 (2004); LYON, *supra* note 6, at 107–08; Roy Coleman, *Surveillance in the City: Primary Definition and Urban Spatial Order*, *in* THE SURVEILLANCE STUDIES READER, *supra* note 6, at 231, 234–35.

[110] *See* COLEMAN, *supra* note 109, at 111.

[111] LYON, *supra* note 6, at 30, 32.

Electronic copy available at: https://ssrn.com/abstract=2239412

used to profile Internet users for marketing purposes. Companies like Google amass vast detailed profiles of our web-surfing habits, our interests, and our buying habits.[112] Data brokers like Acxiom and LexisNexis create even more detailed consumer profiles by combining various kinds of data and sell the data to a wide variety of sources, including direct marketers, background-check companies, and companies consumers may already have a relationship with, such as car dealers or Target.[113] Commercial data of this kind can be used to offer discounts or selective promotions to more or less desirable customers.

The sorting power of surveillance is a major theme among surveillance scholars. In the 1990s, sociologist Oscar Gandy described the "panoptic sort": the use of consumer databases to profile consumers, sort them into categories, and then discriminate among the categories, allocating opportunities on the basis of the classification.[114] More recently, Lyon and other scholars have built on Gandy's work to show the ways in which software is increasingly used to sort citizens and consumers by governments seeking profiles of criminal risk and by companies seeking profiles of commercial opportunity.[115]

From one perspective, the use of the fruits of data surveillance in this way might look like ordinary marketing. But consider the power that data-driven marketing gives companies in relation to their customers. The power of sorting can bleed imperceptibly into the power of discrimination. A coupon for a frequent shopper might seem innocuous, but consider the power to offer shorter airport security lines (and less onerous procedures) to rich frequent fliers, or to discriminate against customers or citizens on the basis of wealth, geography, gender, race, or ethnicity. The power to treat people differently is a dangerous one, as our many legal rules in the areas of fair credit, civil rights, and constitutional law recognize. Surveillance, especially when fuelled by Big Data, puts pressure on those laws and threatens to upend the basic power balance on which our consumer protection and constitutional laws operate. As Professor Danielle Citron argues, algorithmic decisionmaking based on data raises issues of "technological due process."[116] The sorting power of surveillance only raises the stakes of these issues. After all, what sociologists call "sorting" has many other

---

[112] LEVY, *supra* note 18, at 336–37, 341.

[113] *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 917–18 (2008).

[114] OSCAR H. GANDY, JR., THE PANOPTIC SORT 15 (1993).

[115] *See generally* JOHN GILLIOM, OVERSEERS OF THE POOR (2006); DAVID LYON, SURVEILLANCE AFTER SEPTEMBER 11 (2003); THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY (Kevin D. Haggerty & Richard V. Ericson eds., 2006); SURVEILLANCE AS SOCIAL SORTING (David Lyon ed., 2003).

[116] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1258 (2008).

Electronic copy available at: https://ssrn.com/abstract=2239412

names in the law, with "profiling" and "discrimination" being just two of them.

IV. LIMITING SURVEILLANCE

These insights into the ways in which surveillance is harmful point toward identifying remedies that can be built into law, technologies, and social norms to deter the most dangerous forms of surveillance. In this section, I outline four principles that we should use to guide the treatment of surveillance. My purpose is not to propose neat doctrinal fixes to existing law; as I have shown already, the age of surveillance raises massive challenges that will require us to think creatively about how to capture its benefits without sacrificing important civil liberties. Instead, my purpose is to identify some of the values that the law of surveillance ought to protect and the principles that should guide its evolution.

A. Surveillance Transcends the Public/Private Divide

One of the most significant changes that the age of surveillance has brought about is the increasing difficulty of separating surveillance by governments from that by commercial entities. Public- and private-sector surveillance are intertwined — they use the same technologies and techniques, they operate through a variety of public/private partnerships, and their digital fruits can easily cross the public/private divide. It is probably in this respect that our existing models for understanding surveillance — such as Big Brother and the Panopticon — are the most out of date. Even if we are primarily worried about state surveillance, perhaps because we fear the state's powers of criminal enforcement, our solutions to the problem of surveillance can no longer be confined to regulation of government actors. Any solutions to the problem of surveillance must thus take into account private surveillance as well as public.

In this respect, Professor Orin Kerr is correct when he argues that federal statutory law has advantages over the Fourth Amendment in guarding against surveillance in the digital age.[117] Not only is statutory law easier to change, but it also can be applied to bind both government and nongovernment actors. A good model in this context is the federal ECPA and its state-law equivalents. These laws prohibit wiretapping by private actors and require the government to obtain a warrant under a standard higher than probable cause before it can engage in wiretapping.[118] ECPA has many defects, both in terms of the

[117] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806–08 (2004).

[118] 18 U.S.C. § 2516 (2006).

Electronic copy available at: https://ssrn.com/abstract=2239412

level of protection it offers and in its often-bewildering complexity, but in transcending the public/private divide, it represents a good model for dealing with surveillance.

Additional legal protections will be needed to cope with developments in surveillance practices. Because the government can sidestep many legal restrictions on the collection of data by buying it from private databases, we should place additional restrictions on this growing form of state surveillance. Such regulations could operate in both directions. In relation to government, we could place restrictions both on the government's ability to buy private databases and on its ability to share personal information with the private sector. Privacy law already has numerous models for this latter category, ranging from the Driver's Privacy Protection Act of 1994,[119] which limits the government's ability to sell drivers' license records to industry, to the Privacy Act of 1974,[120] which prevents the government from disclosing many kinds of records about individuals that it has in its possession. In relation to private actors, we can place special obligations of confidentiality upon the holders of personal information related to intellectual privacy, treating them as information fiduciaries. Our law has long had a tradition of confidentiality rules, placing nondisclosure obligations on lawyers, doctors, trustees, librarians, and other information custodians.[121] On the Internet, many companies already promise not to share personal information with governments unless compelled. It would be but a small step to make such promises the default, or even the mandatory practice, for certain kinds of particularly sensitive information.[122]

B. Secret Surveillance Is Illegitimate

Democratic societies should prohibit the creation of any domestic-surveillance programs whose existence is secret. In a democratic society, the people, and not the state apparatus, are sovereign. In American law, this tradition goes back to James Madison, and it lies at the very heart of both First Amendment theory and American constitutionalism itself.[123] These principles are reflected at the core of modern information law. For example, the Supreme Court has made clear that the

---

[119] 18 U.S.C. §§ 2721–2725 (2006).

[120] 5 U.S.C. § 552a (2006).

[121] *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 134–40 (2007).

[122] Richards, *The Perils of Social Reading*, *supra* note 20, at 692.

[123] *Madison's Report on the Virginia Resolutions (1789–1800)*, *in* 4 THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 546, 553–76 (Jonathan Elliot ed., Philadelphia, J.B. Lippincott Co. 2d ed. 1891).

Electronic copy available at: https://ssrn.com/abstract=2239412

federal Freedom of Information Act[124] protects at its core the "citizens' right to be informed about 'what their government is up to.'"[125] As Professor Henry Steele Commager put it aptly, "[t]he generation that made the nation thought secrecy in government [to be] one of the instruments of Old World tyranny and committed itself to the principle that a democracy cannot function unless the people are permitted to know what their government is up to."[126]

The illegitimacy of secret surveillance also lies at the heart of information-privacy law, which remains guided by the "Fair Information Practices" drafted by the U.S. Department of Health, Education, and Welfare in 1973.[127] The Code of Fair Information Practices recommended by the Department has continued to influence information-privacy law throughout the world,[128] and the first of its five principles is the commitment that "there must be no personal-data record-keeping systems whose very existence is secret."[129]

Requiring the existence of domestic-surveillance programs to be disclosed solves a practical problem that has bedeviled courts trying to assess legal challenges to secret surveillance programs. How can plaintiffs prove injury if the government is not required to admit whether surveillance exists in the first place? A prohibition on secret surveillance programs solves this problem. When government programs are public — when we have no secret surveillance — courts will be able to assess their legality in the open. The NSA wiretapping program was hard to challenge because its details were shrouded in secrecy, denials, and unassessable invocations of national security interests.[130] At the same time, its shadowy nature created an even greater threat to intellectual privacy in particular because no one knew if her telephone calls were being listened to or not. Requiring disclosure of the existence and capabilities of domestic-surveillance programs to the general public makes them amenable to judicial and public scrutiny to ensure their compatibility with the rule of law. At the same time, the prohibition on secret surveillance *systems* does not require the government to notify *individual targets* of surveillance that they are being

---

[124] 5 U.S.C. § 552 (2006 & Supp. V 2011).

[125] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 773 (1989) (quoting EPA v. Mink, 410 U.S. 73, 105 (1973)).

[126] Henry Steele Commager, *The Defeat of America*, N.Y. REV. BOOKS, Oct. 5, 1972, at 7, 7 (reviewing RICHARD J. BARNET, ROOTS OF WAR (1972)).

[127] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973).

[128] LAWRENCE LESSIG, CODE: VERSION 2.0, at 227 (2006); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 130 (2008).

[129] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 127, at 41; *see also id.* 29–30, 41–42.

[130] *See In re* NSA Telecomm. Record Litig., 671 F.3d 881, 893 (9th Cir. 2011).

Electronic copy available at: https://ssrn.com/abstract=2239412

watched. But fundamentally, surveillance requires legal process and the involvement of the judiciary to ensure that surveillance is targeted, justified, and no more extensive than is necessary.

Thus, while covert domestic surveillance can be justified in discrete (and temporary) instances when there is advance judicial process, blanket surveillance of all Internet activity menaces our intellectual privacy and gives the government too much power to blackmail or discriminate against the subjects of surveillance. In a free society, all forms of surveillance must be ultimately accountable to a self-governing public, and for this reason, secret domestic-surveillance programs of any kind are illegitimate.

C. Total Surveillance Is Illegitimate

Democratic societies should also reject the idea that it is reasonable for the government to record all Internet and telephone activity with or without authorization. Government surveillance of the Internet is a power with the potential for massive abuse, as the (thankfully) failed attempts by the Gadhafi regime illustrated.[131] Like its precursor, telephone wiretapping, Internet surveillance must be subjected to meaningful judicial process before it is authorized. And such authorization must allow only discrete and limited forms of surveillance. Otherwise, there would be no constraint on the government's ability to record and archive all electronic communications and read them at its leisure. The magnitude of technological change should not blind us to the important values that our law has protected for decades: the importance of private communications, intellectual privacy, and unfettered intellectual exploration. Moreover, a world of total surveillance would be one in which the power dangers of surveillance are even more menacing. In such a world, watchers would have increased power to blackmail, selectively prosecute, coerce, persuade, and sort individuals. A world of total surveillance is not just science fiction. It is the world toward which we are slowly creeping, as software is coded, databases are combined, and each CCTV camera is successively added to the network.

Rather than jettisoning longstanding civil liberties in our brave new digital world, we should instead follow the example of federal wiretapping law, which for decades has rested on the premise that private communications should be exactly that, shielded from the government (and other private actors) except in cases of proven law-enforcement need for limited access to those communications. Such a regime is a far cry from the security-driven argument for total surveillance, even in an age of terror.

---

[131] *See generally* Aikins, *supra* note 104.

Electronic copy available at: https://ssrn.com/abstract=2239412

D. Surveillance Is Harmful

As Parts II and III of this Article demonstrate, many forms of surveillance — covert and overt, public and private — menace our intellectual privacy and the processes of belief formation on which a free society depends. They also create a power imbalance between the watcher and the watched that creates risks of blackmail, undue persuasion, and discrimination. Courts and legislatures should therefore scrutinize any surveillance that threatens these values. But because of its relationship to First Amendment values and political freedom, surveillance of intellectual records — Internet search histories, email, web traffic, and telephone communications — is particularly harmful. In practice, this means that surveillance by government that seeks access to intellectual records should be subjected to a high threshold before a warrant can issue. A good model for this rule is Title I of the ECPA, which provides for a more stringent procedure under federal wiretapping law before a warrant may issue to intercept the contents of a telephone or electronic communication.[132] The ECPA requires more than just the standard probable cause requirement that is the constitutional floor under Fourth Amendment law. In addition to probable cause, government agents seeking to tap a phone or electronic communication must also show three other elements: (1) that the warrant is sought for a limited time, (2) that the interception of the communication is necessary to obtain the information sought, and (3) that the wiretapping will be conducted in such a way as to minimize the interception of information not relevant to the warrant.[133] These "super-warrant" protections for communications should be expanded to cover the full range of intellectual records.

For private-sector surveillance, additional statutory procedures are necessary to ensure that intellectual records are handled with greater care by the entities that hold them. We already have piecemeal protections for intellectual privacy against private-sector surveillance, which could serve as useful models for the extension of intellectual-privacy protection more broadly.[134] For example, the ECPA prohibition against warrantless wiretapping applies to private actors as well.[135] The Act makes private acts of wiretapping illegal, providing severe criminal and civil liability — up to five years in prison[136] and fines or

---

[132] 18 U.S.C. § 2518 (2006).

[133] *See id.*; *see also* Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1554 (2010).

[134] For an expanded treatment of this argument in the context of reading records, see generally Richards, *The Perils of Social Reading*, *supra* note 20.

[135] 18 U.S.C. § 2511 ("any person").

[136] *Id.* § 2511(4)(a).

Electronic copy available at: https://ssrn.com/abstract=2239412

tort liability of $10,000 for each violation of the Act.[137] Other good models for intellectual-privacy protection in the private sector include the confidentiality obligations placed on video-rental companies by the Video Privacy Protection Act of 1988,[138] on librarians by the vast number of library-records confidentiality laws, and on print and electronic booksellers in California under its Reader Privacy Act.[139]

Because surveillance of intellectual activities menaces self-government, our law must also recognize it as a harm in standing doctrine. One of the difficulties that courts have faced in dealing with surveillance in the past is an inability to articulate exactly why surveillance is harmful. This inability was the problem in *Laird* and also in the NSA wiretapping cases. Contrary to the trend of the law, *Amnesty International USA v. Clapper*[140] held that amendments to the Foreign Intelligence Surveillance Act that authorized the NSA wiretapping program actually *could* cause a legally cognizable injury to journalists, lawyers, and aid workers whose communications with overseas clients might be subjected to surveillance by the United States government.[141] But even that outlier case, which the Supreme Court reversed on appeal, failed to recognize that a reasonable fear of government surveillance threatens the privacy of the surveilled, causing them to act differently. The Second Circuit found standing but rested its conclusions instead upon injury to the professional duties of the doctors and lawyers who feared that the government was listening. The professional duties of the plaintiffs in *Clapper* are important, and the Second Circuit was correct to recognize injuries to those duties as harms under standing doctrine. But on its own terms, even the Second Circuit seemed to suggest that only professional elites have standing to challenge surveillance. Such a conclusion is underprotective of the rights of all people to be free from unlawful surveillance and to be able to challenge unlawful surveillance in court. As I have argued, intellectual privacy is not just for intellectuals. If the government is engaged in unwarranted surveillance of a person's intellectual activities, that person should have standing to challenge the legality of the surveillance. The surveillance may or may not turn out to be warranted in each particular case, but our society's fundamental commitments to due process, freedom of the mind, and the rule of law suggest that such dangerous surveillance should be subject to legal challenge.

Intellectual-privacy theory thus corrects the errors of *Clapper*, *Laird*, and the NSA cases. It would extend protection from surveil-

---

137 *Id.* § 2520(2)(B).
138 18 U.S.C. § 2710 (2006).
139 CAL. CIV. CODE § 1798.90.05 (West 2012).
140 638 F.3d 118 (2d Cir. 2011), *rev'd*, 133 S. Ct. 1138 (2013).
141 *Id.* at 121–22.

Electronic copy available at: https://ssrn.com/abstract=2239412

lance to all people, and not just to professional elites. It explains why surveillance of reading, thinking, and private communication harms the development of ideas and beliefs unfettered by the skewing effects of observation. Accordingly, a reasonable fear of government surveillance that affects the subject's intellectual activities (reading, thinking, and communicating) should be recognized as a harm sufficient to prove an injury in fact under standing doctrine. Such a change to our law would not be a radical one; in fact, it is precisely the way courts currently assess challenges to individual free speech rights under the First Amendment's chilling-effects doctrine. Since intellectual privacy protects, at heart, First Amendment values, it is appropriate to extend these existing and workable doctrinal tools to this related area of the law.

This is not to say that individual determinations of the chilling of intellectual activities will always be easy. Determining whether a chill to intellectual privacy is substantial would certainly present difficult cases at the margins. In our law, the devil is frequently in the details. But as the chilling-effects doctrine has demonstrated, courts have managed to balance threats to free speech against competing government interests. Moreover, because the general details of government surveillance programs should be public, courts and litigants will have more information with which to assess the effects of surveillance. And even when publication of the details of surveillance might threaten ongoing investigations, such details could be released either under seal to the litigants or shared with the court. Courts have a wide variety of tools to manage the flow of confidential information that litigation inevitably produces, and they would be well suited to such a task. Such tasks may be difficult and require judgment, but that is the job of courts. The alternative to grappling with the civil-liberties threats that surveillance poses is to ignore those threats altogether, to face the prospect of rendering widespread government surveillance unreviewable and uncheckable. Democratic societies can do better than that.

V. CONCLUSION

The challenge to our law posed by the Age of Surveillance is immense. The justifications for surveillance by public and private actors are significant, but so too are the costs that the rising tide of unfettered surveillance is creating. Surveillance can sometimes be necessary, even helpful. But unconstrained surveillance, especially of our intellectual activities, threatens a cognitive revolution that cuts at the core of the freedom of the mind that our political institutions presuppose. Therefore, surveillance must be constrained by legal and social rules. The technological, economic, and geopolitical changes of the past twenty years have whittled away at those rules, both formally on their substance (for example, the Patriot Act and the expansion of National Se-

Electronic copy available at: https://ssrn.com/abstract=2239412

curity Letter jurisdiction) and in practice (for example, the pressure that the technological social practices of the Internet have exerted on privacy). By thus recognizing the harms of surveillance and crafting our laws accordingly, we can obtain many of its benefits without sacrificing our vital civil liberties or upending the power balance between individuals on the one hand and companies and governments on the other.

Electronic copy available at: https://ssrn.com/abstract=2239412

TAKING TRUST SERIOUSLY IN PRIVACY LAW

Neil Richards* & Woodrow Hartzog**

CITE AS: 19 STAN. TECH. L. REV. 431 (2016)

ABSTRACT

Trust—the willingness to accept vulnerability to the actions of others—is the essential ingredient for friendship, commerce, transportation, and virtually every other activity that involves other people. It allows us to build things, and it allows us to grow. Trust is everywhere, but particularly at the core of the information relationships that have come to characterize our modern, digital lives. Relationships between people and their ISPs, social networks, and hired professionals are typically understood in terms of privacy. But the way we have talked about privacy has a pessimism problem—privacy is conceptualized in negative terms, which leads us to mistakenly look for "creepy" new practices, focus excessively on harms from invasions of privacy, and place too much weight on the ability of individuals to opt out of harmful or offensive data practices.

But there is another way to think about privacy and shape our laws. Instead of trying to protect us against bad things, privacy rules can be used to create good things, like trust. In this paper, we argue that privacy can and should be thought of as enabling trust in our essential information relationships. This vision of privacy creates value for all parties to an information transaction and enables the kind of sustainable information relationships on which our digital economy must depend.

Privacy laws and practices centered on trust would enrich our understanding of the existing FIP principles of confidentiality, transparency, and data protection, moving them from procedural means of compliance for data extraction towards substantive principles

---

* Thomas and Karole Green Professor of Law, Washington University School of Law, Affiliate Scholar, The Center for Internet and Society at Stanford Law School.

** Starnes Professor of Law, Samford University's Cumberland School of Law, Affiliate Scholar, The Center for Internet and Society at Stanford Law School. We thank Lisa Austin, Ryan Calo, Julie Cohen, Nico van Eijk, Sue Glueck, Mike Hintze, Margot Kaminski, Bill McGeveran, Caroline Nguyen, Jules Polonetsky, Jason Schultz, Jeffrey Vagle, Christopher Yoo, and the participants at workshops at the Center for Technology, Innovation & Competition at Penn Law, the Privacy Law Scholars Conferences at Berkeley Law and the IViR at the University of Amsterdam, the Privacy and Security Forum at George Washington University, Saint Louis University, Dartmouth College, Berkeley Law, Notre Dame Law School, the Future of Privacy Forum, and Microsoft, Inc. for their helpful comments and suggestions. We also thank Ujjayini Bose, Kevin Jacobsen, Lydia Wimberly, and Megan Fitzpatrick for their excellent research assistance.

to build trusted, sustainable information relationships. Thinking about privacy in terms of trust also reveals a principle that should become a new bedrock tenet of privacy law: Loyalty. Rejuvenating privacy law by getting past Privacy Pessimism is essential if we are to build the kind of digital society that is sustainable and ultimately beneficial to all—users, governments, and companies. There is a better way forward for privacy. Trust us.

TABLE OF CONTENTS

I. INTRODUCTION 433
II. PRIVACY'S PESSIMISM PROBLEM 436
A. *The Creepy Trap* 437
B. *The Harm Fixation* 441
C. *The Control Illusion* 444
III. A THEORY OF PRIVACY AND TRUST 447
D. *Conceptualizing Trust* 448
E. *Why Trust Matters in Information Relationships* 451
IV. REJUVENATING PRIVACY LAW THROUGH TRUST 457
A. *Relying on Fiduciaries* 457
B. *Improving the Existing FIPs* 458
1. *Confidentiality as Discretion* 459
2. *Transparency as Honesty* 462
3. *Security as Protection* 465
C. *Introducing Loyalty as a Foundational Privacy Value* 468
V. CONCLUSION 471

I. INTRODUCTION

Trust is beautiful. The willingness to accept vulnerability to the actions of others is the essential ingredient for friendships, commerce, transportation, and virtually every other activity that involves other people. It allows us to build things, and it allows us to grow.

Trust is everywhere, even if it is not obvious. We trust that architects and builders have created bridges that will support us when we cross them. We trust that merchants will accept the small, green pieces of paper (or digital code) we've earned in exchange for goods and services. We trust that airplanes will arrive safely and to the correct airport. We trust that professionals in our service will act in our best interest, and we trust that our friends will support us and look out for us. Without trust, our modern systems of government, commerce, and society itself would crumble.

Trust is also the essential ingredient for our digital lives. So much of modern networked life is mediated by information relationships, in which professionals, private institutions, or the government hold information about us as part of providing a service. Such relationships are everywhere we look. We see them when we share sensitive personal information with Internet service providers (ISPs), doctors, banks, search engines, credit card companies, and countless other information recipients and intermediaries. We also see them as we get information via large and small computers to access apps, social media, and the Internet at large.

Even relationships that used to have no significant informational component—grocery stores, airlines, political party affiliations, and the like—are now part of the data game. Merchants use data to predict what shoppers will do. Companies give away products and services "for free" just to get the information that

comes with it. Data brokers amass vast troves of data to enable their clients to profile, segment, and influence people as consumers or as voters. The stampede for big data and the development of the "Internet of Things" are only accelerating these developments. If we want a sustainable digital society, we need strong, trusted information relationships.

When we talk about personal information changing hands, policymakers, lawyers, and citizens throughout the world use the word "privacy." In this context, privacy means the rules governing the collection, use, and disclosure of information. Ostensibly, privacy rules should encourage and fortify information relationships. They should build trust in these relationships. But they don't. Rather than encouraging trust, modern American privacy law encourages companies to profit in short-sighted ways by extracting as much value as possible from personal data in the short term. As long as companies don't cause a narrow set of legally recognized, largely financial harms, they are essentially free to set up the terms of information relationships any way they wish. Companies have this power because of a second hallmark of modern American privacy law, its reliance on a control-based regime of "notice and choice." Under this arrangement, terms are hidden in the fine print of legal notices virtually no one reads, and there is as little meaningful choice as in old-fashioned consumer adhesion contracts. Consumers are left exposed and bewildered, lamenting what they see as the "death of privacy."[1]

Privacy—the legal regime governing the use of personal information—is not dead, nor is it going away. In a society in which the exploitation of personal data is an enormous source of value, national and international rules governing that data are inevitable. But how we talk about privacy matters, as it structures the terms of a debate in which little is inevitable and so much is up for grabs.

Critically, the way we talk about privacy as lawyers is increasingly inadequate because it is too often framed in negative terms. Privacy is seen a tax on profits, a drain on innovation, a dangerous and naive assumption, and a burden on the individual to fend for herself in the digital thicket. Hot information age topics like "permissionless innovation," "creepiness," "privacy harm," and "the privacy paradox" highlight what is to be lost rather than gained in the privacy debate. In short, privacy has a pessimism problem.

Such negative ways of thinking about privacy are incomplete and often inaccurate. What's missing is a positive understanding of privacy in terms of the good it can potentially do. And what's missing is the essential relationship between privacy and trust. Privacy Pessimists often ignore trust, even though trust is essential. Yet thinking about information relationships and privacy rules in terms of trust reveals how privacy protections can be a positive force, generating deeper and more sustainable information relationships and corporate profits.

We need information relationships to function in our modern networked society. But as users we're bewildered. Our information is collected, used, and ana-

1. Neil M. Richards, *Four Privacy Myths*, *in* A WORLD WITHOUT PRIVACY? 33 (Austin Sarat ed., 2015) (critiquing the rhetoric of the "death of privacy").

lyzed in ways we cannot understand and can rarely control. Given this fact, it should be no surprise that people feel confused and disempowered when it comes to their data. Instead of feeling confident that we'll be protected when we share information with others, we increasingly feel helpless and resigned to our fate, whatever that might be.

This is a problem not just for consumers but also for the companies and governments on the other side of these relationships. Without trust, people share less information, bad information, or no information at all. They become anxious, bewildered, and suspicious. They lie or self-censor otherwise beneficial information. If people don't trust a company, they are more likely to switch to a competitor or resist or fail to become fully invested in the commercial relationship. Our piecemeal laws of personal data create incentives for a quick buck through a kind of data strip mining. We have a legal regime that encourages a short-term and short-sighted "monetization" of data that leaves consumers confused and frustrated. This is an inefficient and unsustainable state of affairs, yet both our laws and the ways we talk about privacy enable it.

Our basic claim in this paper is quite simple: modern privacy law is incomplete because from its inception it has failed to account for the importance of trust. This gap has biased privacy law and norms toward a pessimistic proceduralism in which harm avoidance is the only substantive value. Trust in information relationships is necessary for the digital economy not just to function, but to flourish. Acting together, privacy and trust can do more than avoid harm, but can create value. We can do better, and should use privacy law promote trust across the board.

Our argument proceeds in three steps. First, we highlight the problem of Privacy Pessimism. We survey the world of privacy law and describe how and why it has led us to be pessimistic. Framing the privacy debate over what is being lost has frustrated the true potential of information rules to benefit everyone. This frame, which affects both our policies and the ways we talk about them, results in casting privacy in opposition to other interests like innovation and security. It leads us to obsess over locating "privacy harms" and scratch our heads over mysteries like "creepiness," "the privacy paradox" and "notice and choice." This pessimism is then enshrined in law, which perpetuates the fatalistic cycle.

Second, we propose an alternate vision for privacy by conceptualizing it in terms of trust. Privacy rules—regulation of information in relationships—have enormous potential to build the trust necessary for our digital society to flourish. Our theory of privacy and trust seeks to encourage the creation of long-term, sustainable information relationships to unlock the full potential of data and modern technology. Thinking about privacy in terms of its potential to build trust focuses on creating strong social bonds and sustainable, profitable relationships. It serves the interests of commerce, social relationships, and promotion of free expression and political engagement. It also shows thinking of privacy exclusively in negative terms is just plain wrong.

Finally, we suggest how our law and social practices can better promote trust in government and corporate information relationships. We propose two paths

forward. First, the Fair Information Practices (FIPs) and their progeny should be rejuvenated by incorporating trust as a guiding principle. Doing so will add nuance, rigor, and direction to many of the exiting obligations under the many legal regimes that incorporate the FIPs. Confidentiality becomes more useful and contextual as a duty of *Discretion*. Transparency becomes more effective and inclusive if re-conceptualized as an obligation of *Honesty*. And, security becomes more complete when framed as a duty of *Protection*.

We also introduce the new concept of *Loyalty* as a foundational value for privacy law. Borrowing from the law of fiduciaries, we argue that there should be limits on the amount of self-dealing one can engage in after being entrusted with personal information. Consent via the fine print of a legal agreement no one reads is disloyal and illegitimate. One of the biggest fears in the modern information economy is that personal information obtained from users will be used against their interests. The obligation of Loyalty aims to prevent that from happening, and should be enshrined in statutes as well as the common law torts and consumer protection law.

There is a better way forward for privacy. Trust us.

II. PRIVACY'S PESSIMISM PROBLEM

Modern privacy law has painted us into a corner. We have designed elaborate, nuanced, and even powerful frameworks to respond to the wrongful collection, use, and dissemination of personal information. For a while, it worked reasonably well. But new problems have come to thwart the best intentions of privacy law.

Modern privacy law is the offspring of two separate bodies of law. The privacy torts were developed in response to new surveillance technologies and a perceived media aggressiveness,[2] while the Fair Information Practices or "FIPs" were developed in response to electronic databases.[3] Tort privacy offers a substantive principle: Do No Harm when processing personal data. By contrast, the FIPs offer a procedural framework for managing the collection and flow of personal data rooted in some opportunity for individuals to have *notice* of when their data is being collected or used and some *choice* to control objectionable practices.[4] Together, the *Harm Principle* that comes from tort law and the *Control Principle* that comes from the FIPs are the bedrock of modern privacy law, animating everything from statutes like the federal Privacy Act and HIPAA to the substance of FTC enforcement actions and foreign privacy regimes.

As we discuss below, while the FIPs haven proven to be quite useful as an or-

---

2. Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 361-62 (2011).

3. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY (2015).

4. *See* Robert Gellman, Fair Information Practices: A Basic History, Version 2.16, Feb. 11, 2015, http://bobgellman.com/rg-docs/rg-FIPShistory.pdf [http://perma.cc/54DD-WPAT]; HELEN NISSENBAUM, PRIVACY IN CONTEXT 129 (2010).

ganizing principle, they are weakening. Not only are the FIPs non-responsive to some new privacy problems, but they are also centered on the autonomous ideal of control. As long as users have control to decide when they relinquish certain privacy rights, then companies are abiding by the FIPs. In the current system of FIPs-based regulation of personal data, the user is seen as a completely rational, autonomous actor capable of controlling her down privacy destiny. If she loses any privacy, it is because she chooses to do so.

This model of choice and control is well established in the privacy literature at all levels. Some of the most popular theories of privacy cast the concept in terms of control.[5] So too does the dominant system of informal regulation in the corporate world.[6] But both the *Harm Principle* and the *Control Principle* are oriented in negative terms—Do No Harm in using data, or at least get some kind of consent before you do. From this perspective, privacy is almost always a negative and costly concept, a harm to be avoided, or a consent to be obtained before something positive can happen. This is the pathology of Privacy Pessimism, and in this Part, we describe how Privacy Pessimism has caused us to think about privacy in a way that is unnecessary, incomplete, and focused on fixing harm rather than creating value. Three dimensions of this pessimism problem are most important. We call them *the Creepy Trap, the Harm Fixation*, and *the Control Illusion.*

A. *The Creepy Trap*

Most discussions of privacy and new technologies run into accusations of creepiness at some point. Surveillance-based advertising? Creepy.[7] Facebook tweaking your news feed to make you sad? Creepy.[8] The NSA, black box data recorders in cars, eavesdropping Barbie dolls, the Internet of Things, drones, or Google scanning your Gmail? Each of these practices have been labeled as "creepy" at one time or another.[9]

---

5. Alan Westin defined privacy as an individual's right "to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others." ALAN WESTIN, PRIVACY AND FREEDOM (1967).

6. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 260 (2011); Michael Zimmer, *Mark Zuckerberg's Theory of Privacy*, WASH. POST, Feb. 3, 2014, http://www.washingtonpost.com/lifestyle/style/mark-zuckerbergs-theory-of-privacy/2014/02/03/2c1d780a-8cea-11e3-95dd-36ff657a4dae_story.html [http://perma.cc/26KZ-9MLR].

7. *See generally* JULIA ANGWIN, DRAGNET NATION (2014).

8. Caitlin Dewey, *9 Answers About Facebook's Creepy Emotional-Manipulation Experiment*, WASH. POST (July 1, 2014), http://www.washingtonpost.com/news/the-intersect/wp/2014/07/01/9-answers-about-facebooks-creepy-emotional-manipulation-experiment [http://perma.cc/FZT9-BJ45].

9. Douglas Rushkoff, *NSA's Phone Snooping a Different Kind of Creepy*, CNN (June 6, 2013, 2:34 PM), http://www.cnn.com/2013/06/06/opinion/rushkoff-nsa-verizon [http://perma.cc/9VY3-YVAQ]; Chris Ward, *In Car Black Box Data Recorder Sounds Creepy*, DAILYCARBLOG (Jan. 15, 2015), http://www.dailycarblog.com/2015/01/car-black-box-data-recorder-sounds-creepy [http://perma.cc/Z86A-DUGR]; Tony Bradley, *The Creepy Factor of the 'Internet of Things'*, RSA BLOG (June 17, 2014), http://blogs.rsa.com/creepy-factor-internet-

This should be no surprise. Creepiness is our first impulse when we encounter changing norms or technologies that leave us exposed or vulnerable. It's a visceral sensation of discomfort and revulsion, a trigger that tells us when privacy might be threatened. If we feel that a practice is creepy, goes the intuition, maybe we should think about regulating it. But the flip side also seems to be true: if something isn't creepy, then it probably isn't a problem.

Creepiness has been explored as a privacy concept. In advice to technology companies about how to avoid the creepiness reaction from their users, Omer Tene and Jules Polonetsky suggest that there are "several categories of corporate behavior that customers and commentators have begun to label 'creepy' for lack of a better word," activities that don't violate any established law, but which give their customers the creeps.[10] Tene and Polonetsky advise companies to avoid deploying new technologies (or old technologies in new ways) in ways that seem creepy. Such limits are necessary, they assert, because "social values are far more nuanced and fickle that any existing (and most likely future) laws and regulations. In order to avoid creep, companies should resist the temptation to act with chutzpah, even though brazen and audacious behavior constitutes a hallmark of Silicon Valley entrepreneurship culture. The challenge is for companies to set the right tone when seeking intimate relationships with consumers."[11]

Creepiness is also embedded in more formal kinds of privacy law. The old privacy tort of "intrusion into seclusion" protects private places and relationships from menacing (or creepy) intrusions.[12] The Fourth Amendment's venerable *Katz* test requires not only a famous "reasonable expectation of privacy," but a subjective expectation of privacy as well.[13] This subjective element means that for the Fourth Amendment to apply, a citizen has to feel violated by a government intrusion or monitoring. Though rarely phrased in terms of creepiness, Fourth Amendment law is based upon a similar idea that privacy is only invaded when there is a felt sense of intrusion of violation.

Helen Nissenbaum's much-praised theory of privacy as "contextual integrity"

---

things [http://perma.cc/EQJ2-CB3M]; Cyrus Farivar, *Vancouver Man Creeped Out by Drone Buzzing Near His 36th-Story Condo*, ARS TECHNICA (Aug. 20, 2014, 12:27 PM), http://arstechnica.com/tech-policy/2014/08/vancouver-man-creeped-out-by-drone-buzzing-near-his-36th-story-condo [http://perma.cc/5LS3-AXYS]; Benjamin Herold, *Lawsuit Alleges That Google Has Crossed a 'Creepy Line' With Student Data*, HUFFINGTON POST (Mar. 17, 2014, 2:49 PM), http://www.huffingtonpost.com/2014/03/17/google-data-mining-students_n_4980422.html [http://perma.cc/89LP-8QJX]; Sarah Halzack, *Privacy Advocates Try to Keep 'Creepy' 'Eavesdropping' Hello Barbie from Hitting Shelves*, WASH. POST (Mar. 11 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hello-barbie-from-hitting-shelves [http://perma.cc/VB9R-NJBX].

10. Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J. L. & TECH. 59, 61 (2013-14).

11. *Id.* at 101.

12. RICHARDS, *supra* note 3, at 64-72.

13. *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1521-22 (2010).

also contains overtones of creepiness. Nissenbaum suggests that privacy violations occur when "context-relative informational norms" are not respected when sharing information.[14] Her framework of contextual integrity suggests that "finely calibrated systems of social norms, or rules, govern the flow of personal information in distinct social contexts (e.g., education, health care, and politics)."[15] Individuals experience privacy violations when those social norms about information are violated in inappropriate ways.[16] Nissenbaum's theory has been highly influential among academics, and is starting to influence policy, with her work built into the Federal Trade Commission's updated approach to regulating privacy.[17] At the core of Nissenbaum's theory is her claim that we should consider privacy issues in the first instance when people react to new information practices by expressing "alarm."[18] In other words, although she does not use the term, something like creepiness in a particular context is the trigger for a potential privacy violation.

But there is a problem with creepiness, regardless of how carefully it is defined. It might be a very human and natural way to respond to new social or technological circumstances, but it ultimately tells us little about whether a legally cognizable privacy issue exists. At the outset, creepiness is over-inclusive as a proxy for information privacy threats. Lots of new technologies that might at first appear viscerally creepy will turn out to be either unproblematic or beneficial. Evan Selinger reminds us that early train passengers were not merely creeped out but terrified, fainting, and complaining of serious maladies from traveling at speeds that by today's standard would not constitute speeding in a school zone.[19] In the early days of the Internet, many users refused to buy products online, fearing security lapses from digital technologies they didn't understand.[20] Facebook's

---

14. NISSENBAUM, *supra* note 4, at 129; Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 155 (2004).

15. NISSENBAUM, *supra* note 4, at 3.

16. Nissenbaum, *supra* note 14, at 155.

17. Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All Over the FTCs New Approach to Privacy*, THE ATLANTIC (Mar. 29, 2012), http://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/ [http://perma.cc/FMH6-SKLK].

18. NISSENBAUM, *supra* note 4, at 3, 11. Nissenbaum's theory offers more than creepiness, but we note it here because it is (a) prominent and influential, and (b) its violation of "context-relative information norms" bears a close similarity to the what is colloquially deemed as "creepiness." As Nissenbaum's work on context becomes adopted by third-parties into regulation, and thus loses academic nuance, we predict that her nuanced philosophical treatment is likely to be folded in with colloquial "creepiness."

19. Evan Selinger, *Why Do We Love to Call New Technologies "Creepy"?*, SLATE (Aug. 22, 2012, 3:30 AM), http://www.slate.com/articles/technology/future_tense/2012/08/facial_recognition_software_targeted_advertising_we_love_to_call_new_technologies_creepy_.html [http://perma.cc/UZ9W-DZCH].

20. Ye Diana Wang & Henry H. Emurian, *An Overview of Online Trust: Concept, Elements, and Implications*, 21 COMPUTERS IN HUMAN BEHAVIOR 105 (2005), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.2184&rep=rep1&type=pdf [http://perma.cc/8TW9-AY5Y].

News Feed feature "creeped out" many users when it was first introduced because users were not accustomed to having all their information aggregated in one place for easy consumption.[21] Now the feature is considered to be fundamental both to the company's success and to the social awareness of many users of its network.[22]

But creepiness is also under-inclusive. New information practices that we don't understand fully, or highly invasive practices of which we are unaware, may never seem creepy, yet still present serious threats to values we care about. Take, for example, surveillance of which we are unaware,[23] or the use of secret algorithms to score our lives.[24] Such practices may unconstitutionally subject us to criminal or civil punishment (from jail time to designation on "no-fly" or "watch" lists), or they may deny us access to health, insurance, or economic opportunities (in the case of scoring by credit or university admissions algorithms). Such practices may be illegal, inaccurate, or both, but if they operate behind layers of secrecy, we may never learn about them. And things we are unaware of are unlikely to trigger the creepiness reaction.

Finally, because it rests on psychological reactions to perceived practices, creepiness is not only socially contingent, but malleable. A pervasive threat to privacy or our civil liberties can be made less creepy as we become conditioned to it. Such a threat may remain equally serious, but become normalized as we fit it into our understanding of the world in which we have to operate, like police corruption, sexism, or drunk drivers. Arguably, the Internet advertising industry, which relies on detailed surveillance of individual web-surfing to target ads, has fallen into this category.[25] Becoming "normal" in this way hardly removes the problem, even if we become accustomed or resigned to it. In the context of privacy, consider the ever-expanding reach of data collection, always pushing up against (and seeking to roll back or desensitize) the creepiness reaction. As Google's Eric Schmidt put it honestly in 2010, "Google policy is to get right up to the creepy line and not cross it."[26]

While it may be a natural psychological response to novelty, in the context of privacy law, creepiness is ultimately a trap. It locks us into a false binary of things that are *creepy* and thus potentially problematic, and things that are *not creepy* and thus presumably okay. Under the standard story, a finding of creepiness is only

---

21. danah boyd, *Facebook's Privacy Train Wreck*, 14 CONVERGENCE 13 http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf; Tiffany A. Pempek, Yevdokiya A. Yermolayeva, & Sandra L. Calvert. *College students' social networking experiences on Facebook,* 30 J. APPLIED DEV. PSYCH. 227 (2009).

22. Sam Biddle, *Facebook's New News Feed: The Biggest Change in Years*, GIZMODO (Mar. 7, 2013, 1:12 PM) http://gizmodo.com/5989228/facebooks-new-news-feed-the-biggest-change-in-years-updating-live [http://perma.cc/CAC8-2G95].

23. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

24. *See generally* FRANK PASQUALE, BLACK BOX SOCIETY (2015).

25. ANGWIN, *supra* note 7, at 4-5.

26. Shane Richmond, *Eric Schmidt: Google Gets Close to the "Creepy Line,"* TELEGRAPH (October 5, 2010), http://blogs.telegraph.co.uk/technology/shanerichmond/100005766/eric-schmidt-getting-close-to-the-creepy-line [http://perma.cc/5VZ4-BULW].

the start of the inquiry. Since some things that are creepy actually turn out to be desirable (recall the screaming Victorian train passengers and Facebook's News Feed), a creepy new technology begs a second question of whether something experienced as creepy is actually harmful. This fixation on harm is another major symptom of Privacy Pessimism, which we'll turn to now.

B. *The Harm Fixation*

A second pathology of Privacy Pessimism is that it is too focused on privacy's costs, often to the exclusion of any benefits. From this perspective, privacy is an injury to be remedied, a cost to be balanced in the ledger book, a harm rather than an opportunity. After all, goes the logic, we have to find out whether our sense of creepiness is actually a harmful one or just a false positive.

The Harm Fixation began with Warren and Brandeis, who were concerned about coverage of elite social functions by newspapers and by the new technology of "instantaneous photography." Worried that press coverage of intimate affairs and the circulation of unauthorized photos were causing psychological harm, they argued that the common law should recognize a tort to remedy these emotional injuries.[27]

Today's privacy law has expanded far beyond Warren and Brandeis's tort claims against the press. Modern privacy law is regulatory in scope, structuring data relationships in personal data and covering types of information and advanced technologies that nineteenth century lawyers might find indistinguishable from magic.[28] "Instantaneous photography" has nothing on Snapchat or GPS, and the Fair Credit Reporting Act and FTC investigations are much more complex and nuanced than a common law tort claim. But even though privacy law has evolved far from its origins in tort law, tort law's fixation on compensable individual harm has stubbornly remained with it, even when other elements of the law of torts have fallen by the wayside.

The Harm Fixation also manifests in the form of balancing tests used to decide whether certain information practices should be permissible or not. For example, Section 5 of the FTC Act, which outlaws unfair and deceptive trade practices, has become the most important piece of legislation for protecting consumer privacy in the United States.[29] But in order for a practice to be deemed unfair, it must be "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."[30]

---

27. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); RICHARDS, *supra* note 3, at 17.

28. This is of course Arthur C. Clarke's Third Law of Technology, first posited in Leigh Brackett, *The Sorcerer of Rhiannon*, ASTOUNDING, Feb. 1942, at 39.

29. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588 (2014).

30. 15 U.S.C. § 45(n) (2013).

In privacy-related disputes, companies, agencies, and courts are asked to articulate whether the cost of acting fairly, in this instance to preserve privacy, is outweighed by the potential benefit to the consumer, which is often articulated as "cost savings passed on to the consumer."[31] The Obama White House's proposed "Consumer Privacy Bill of Rights" wholly embraces balancing privacy risks with other considerations.[32] It provides for a rulemaking procedure that considers "among other factors, the privacy risks posed by personal data processing by categories of persons of various sizes, experiences, resources, and types of commercial activity, including nonprofit activity; the importance of mitigating privacy risks; and the costs and benefits of including those categories of persons as covered entities."[33] This balancing requirement pits privacy and affordability against each other as values in conflict.

Companies, agencies, and courts are not the only privacy pessimists fixated on the cost of privacy. Critics of privacy regulation bemoan its toll on "innovation" and "progress."[34] Very few companies want to cause problems to people or hurt them, but focusing on the expense of privacy inevitably frames privacy as "the cost of doing business" instead of an opportunity to help form long-term, sustainable relationships.[35] Even advocates for privacy frequently consider privacy as a negative value that must be balanced against innovation, efficiency, or security. Responding to the framing of Privacy Pessimism, there is a large academic literature on "privacy harm" seeking to articulate exactly what the nature of the injury caused by threats to privacy.[36]

The Harm Fixation is thus problematic because it frames the privacy inquiry in negative, costly terms. But there is a second problem. The Harm Fixation also demands proof that is increasingly elusive.[37] In order to be actionable, all of the privacy torts demand a demonstration of harm that is "highly offensive to a reasonable person."[38] Those arguing against regulation of behavioral advertising assert that regulation is unnecessary because no harm from the practice can be

---

31. *See* Solove & Hartzog, *supra* note 29.

32. White House, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015 (Feb. 27, 2015), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [http://perma.cc/8SJ6-ND47] ("If a covered entity processes personal data in a manner that is not reasonable in light of context, the covered entity shall conduct a privacy risk analysis . . . to examine the potential for privacy risk. Covered entities shall take reasonable steps to mitigate any identified privacy risks, which shall include, but are not limited to, providing heightened transparency and individual control.").

33. *Id.*

34. *See, e.g.,* ADAM THIERER, PERMISSIONLESS INNOVATION (2014).

35. See Richards, *supra* note 1 (collecting examples).

36. *See, e.g.,* Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); *see also,* Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 849 (2014).

37. Calo, *supra* note 36.

38. RESTATEMENT (SECOND) OF TORTS §§ 652B-D (1977).

demonstrated.[39] Claims against companies for providing poor data security usually fail unless the plaintiff can demonstrate actual individualized harm, such as financial loss, instead of harms like uncertainty or increased risk shared across large numbers of people that are large in the aggregate but small for each affected individual.[40] The Supreme Court has taken a number of cases in recent years assessing whether allegations of harm are sufficient under the Federal Privacy Act,[41] and a pending case asks whether a private cause of action under the Fair Credit Reporting Act can ever satisfy Article III standing.[42] In these and other cases, the Supreme Court is increasingly interpreting privacy harm very narrowly.[43] State courts also routinely reject notions of privacy that are not immediately ascertainable or are speculative in nature.[44] Given the arc of decisions limiting notions of what constitutes privacy harm, an alternative focus would be useful.

Harm is, of course, an important concept in our law. It will remain a critical component in regulatory regimes that punish companies and provide redress through private causes of action for individuals, whether for identity theft, data breach, or revenge porn. It is an effective way of determining compensation amounts and separating important claims from trivial or meritless ones. But the goal of privacy law shouldn't *solely* be to avoid harm. Such a fixation is too rigid and focuses our attention away from important areas where privacy regulation can create value, rather than merely remedying injury.

While many laws are designed to deter harm, that is not the only function of law. Other laws, like tax regulations that provide incentives for charitable giving and consumer spending, are designed to encourage behavior that is seen as desirable within society.

The Harm Fixation forces us to come up with ill-fitting theories of harm

---

39. *See, e.g.*, Joel Rosenblatt, *Facebook Seeks Dismissal of $15 Billion Privacy Suit*, BLOOMBERG BUSINESS (Oct. 5, 2012, 11:06 AM), http://www.bloomberg.com/news/articles/2012-10-05/facebook-seeks-dismissal-of-15-billion-privacy-suit [http://perma.cc/67KN-GASC].

40. *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012) (finding no harm from increased risk of identity theft); Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011); Holmes v. Countrywide Fin. Corp., No. 5:08–CV–00205–R, 2012 WL 2873892 (W.D. Ky. July 12, 2012) (rejecting theory of harm for time and efforts expended to deal with breach); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. Nov. 23, 2009) (rejecting standing for increased risk of identity theft); Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006) (rejecting standing for increased risk of identity theft); Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (rejecting theory of harm for increased risk of junk mail).

41. E.g., Doe v. Chao, 540 U.S. 614 (2004); Fed. Aviation Admin. v. Cooper, 132 S.Ct. 1441 (2012).

42. *See Spokeo v. Robins, Inc.*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/spokeo-inc-v-robins/ [http://perma.cc/9YKM-HEJ3].

43. *See, e.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2013) ("[R]respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.").

44. *See, e.g.*, *Holmes*, 2012 WL 2873892; *Amburgy*, 671 F. Supp. 2d 1046; Key, 454 F. Supp. 2d 684; *McLoughlin*, 2009 WL 2843269; *Bell*, 2006 WL 2850042.

when we inevitably sense that there is a problem but cannot easily articulate a clear, cognizable, and individualized injury. Like an itch that can't be scratched or a problem that we just can't seem to put our finger on, this dimension of Privacy Pessimism paints us into a corner of narratives like "creepy" that sound compelling at first, but crumble in practice or under scrutiny.[45]

C. *The Control Illusion*

A third problem of Privacy Pessimism is its assumption that people can adequately make choices to protect their information. In the United States, privacy policy is largely centered on the idea that the best way to protect your privacy is to be careful about what and how much information you disclose and to whom. We have called this the *Control Principle,* though it is also called a "notice and choice regime" or "privacy self-management."[46]

When the FTC first started to regulate privacy in the late 1990s, it adopted a basic notice and choice regime for businesses that was congruous with many of the FIPs. As long as companies notified people about their information collection, use, and disclosure practices and gave them a choice to opt out (usually by not using the service), then companies were free to act in any way consistent with the notice given to consumers. The most salient example of this notice and choice regime is the ubiquitous privacy policy, that dense, unreadable, boilerplate text tucked away in some corner of virtually every website and application on the Internet.

In most cases that matter, the assumption that users have actual notice or meaningful choice is an illusion. Privacy self-management is increasingly recognized to be unworkable and possibly even a farce. There are many jokes about whether anyone reads privacy policies or Apple's infamously turgid Terms of Service agreement, but these jokes rest on the undeniable truth that privacy self-management is impossible. For example, one study by computer scientists found that if an ordinary Internet user were to quickly read every privacy policy they encountered over the course of a year, it would take them seventy-six working days to do so.[47] Another study by leading privacy journalist Julia Angwin revealed that it was practically impossible to opt-out of pervasive surveillance by governments and companies without practically opting out of society and human contact

---

45. *See, e.g.,* Tene & Polonetsky, *supra* note 10.

46. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879 (2013); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

47. Alex C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012, 2:25 PM), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851 [http://perma.cc/2ZJN-BYLA]; Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. POL'Y INFO. SOC'Y 543 (2009).

itself.[48] The Control Principle is the key element of American data regulation, but it is false.

When pressed on this point, federal regulators concede the futility of notice and the absence of real choice about the pervasive collection of personal data. The White House Privacy and Civil Liberties Oversight Board recognized as much in its long-awaited report on privacy and surveillance.[49] In its report on Big Data, the White House also repudiated the Control Principle, stating, "[t]he framework of notice and consent is also becoming unworkable as a useful foundation for policy."[50] Even the FTC has realized the limits of notice and choice.[51] The agency's report on protecting consumer privacy in the digital age acknowledged that "the emphasis on notice and choice alone has not sufficiently accounted for other widely recognized fair information practices, such as access, collection limitation, purpose specification, and assuring data quality and integrity."[52] Yet despite the acknowledgment that choice cannot do the work we ask of it, new proposals remain rooted in the Control Illusion. For example, the White House "Privacy Bill of Rights" released in February 2015 surprisingly remains rooted in a notice and choice view of the world.[53]

Such fixation on choice is especially problematic because the illusion of the Control Principle benefits the rich at the expense of the poor. AT&T's Internet service, for example, will let users opt out of a "supercookie" that monitors its users' habits for $29 a month.[54] Privacy then becomes merely a luxury good that

---

48. ANGWIN, *supra* note 7.

49. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014).

50. EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 46 (May 2014).

51. Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at Proskauer on Privacy 2 (Oct. 19, 2010), http://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-julie-brill/101019proskauerspeech.pdf [http://perma.cc/CQH4-TA8R] ("[T]he Notice and Choice model, as it is often deployed today, places too great a burden on consumers."); Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable 3 (Dec. 7, 2009), http://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf [http://perma.cc/XCQ5-PXLW] ("We do feel that the approaches we've tried so far—both the notice and choice regime, and later the harm-based approach—haven't worked quite as well as we would like.").

52. Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 2 (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (also acknowledging the limits of privacy harm, stating "[t]he FTC's harm-based approach also has limitations. In general, it focuses on a narrow set of privacy-related harms—those that cause physical or economic injury or unwarranted intrusion into consumers' daily lives. But, for some consumers, the actual range of privacy related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there.'").

53. White House, *supra* note 32.

54. Sophia Cope & Jeremy Gillula, *AT&T is putting a price on privacy. That is outrageous,*

most people cannot afford. Thus, under the Control Illusion, users simply "choose" surveillance and the loss of privacy either because they cannot afford anything else, or because (as noted earlier) privacy harm is notoriously hard to calculate. Other times surveillance of everyday life just gets built into modern technologies, whether it is Samsung's "smart" TVs that record conversations in your living room, or Lenovo's laptops that shipped with insecure software that surveilled user web surfing in order to serve ads.[55]

The reality that the Control Principle is an illusion also provides an answer to one of the by-products of Privacy Pessimism, the so-called "privacy paradox." This is the idea that surveys consistently measure both consumer anxiety about privacy and behavior that is seemingly at odds with such concerns. Some commentators use the paradox to suggest that individuals are either hypocritical or ignorant.[56] But the privacy paradox is fallacious because it only considers one party in an information relationship: the user. Users given a blunt choice between protecting their data and participating in modern society really have no choice at all, especially when the terms of any such choice are clouded by confusing technology and legal mumbo-jumbo, where long-term interests in privacy are hard to value, or where meaningful choice is an illusion. In fact, given the limited notice and choice that most of us encounter, the privacy paradox suggests that users care about their personal data *in spite* of the limited legal and technological choices they face in protecting it.[57] If our revealed preferences show that we don't care about privacy, why do so many of us remain anxious about our personal data?

Ultimately, the Control Illusion reveals the limits of the procedural approach taken by the FIPs. For years, there was no privacy problem the FIPs purportedly could not fix. But doing so has worn out the concept amid the explosion of new data applications. Big Data has challenged the wisdom and practicality of data retention.[58] Profiling, discrimination, and other inferential harms happen so re-

---

GUARDIAN (Feb. 20, 2015, 12:09 PM), http://www.theguardian.com/commentisfree/2015/feb/20/att-price-on-privacy?CMP=fb_us [http://perma.cc/ZB2X-MZN6].

55. Parker Higgins, *Big Brother Is Listening: Users Need the Ability to Teach Smart TVs New Lessons*, ELEC. FRONTIER FOUND. (Feb. 11, 2015), http://www.eff.org/deeplinks/2015/02/big-brother-listening-users-need-ability-teach-smart-tvs-new-lessons [http://perma.cc/9YA9-EZPN]; Seth Rosenblatt, *Lenovo's Superfish Security Snafu Blows Up in its Face*, CNET (Feb. 20, 2015, 5:00 AM), http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware [http://perma.cc/WW29-PBVC].

56. Stuart N. Brotman, *Grappling with the Privacy Paradox*, BROOKINGS INST. (July 8, 2014, 7:30 AM), http://www.brookings.edu/blogs/techtank/posts/2014/07/8-brotman-privacy-paradox#.U7xJMEM6Z4M.twitter [http://perma.cc/A6ZC-MDKS]; Steve Lohr, *The Privacy Paradox, a Challenge for Business*, N.Y. TIMES (June 12, 2014, 2:12 PM), http://bits.blogs.nytimes.com/2014/06/12/the-privacy-paradox-a-challenge-for-business/?_php=true&_type=blogs&_r=0 [http://perma.cc/VGC2-LU4P]; Diane Brady, *Privacy Paradox: Americans Happy to Share Personal Data With Big Business*, BLOOMBERG BUSINESSWEEK (June 25, 2013), http://www.bloomberg.com/bw/articles/2013-06-25/privacy-paradox-americans-happy-to-share-personal-data-with-big-business [http://perma.cc/Z3LH-892E].

57. Richards, *supra* note 1 (suggesting the existence of such a "reverse privacy paradox.").

58. Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of*

motely from the source as to remove any doubt that the "choice" offered to users who disclose personal in the modern world is usually an illusion. After all, what choice can users have to opt out of profiling by ad networks and data brokers of whose existence they are unaware?

The FIPs have been whittled away to an empty shell in many areas of privacy law, especially the law protecting consumers in their Internet usage in the United States. In many areas, the FIPs have become little more than a set of procedural protections lacking a substantive theory of what privacy is and why it matters. From this perspective, it should be no wonder why so many people are pessimistic about privacy.[59]

***

Behold, then, the traditional story we tell ourselves about privacy, a story we have called "Privacy Pessimism." Privacy is under threat from new technologies and business practices that we perceive as "creepy." When we encounter a creepy privacy practice, tort law has trained us to see if there is any harm. Yet in many instances, regardless of the harm, we feel like our consent is being wrongly manufactured using fine print and malicious design. The Harm Fixation limits our ability to think about what privacy can do for us, while the fiction of the Control Illusion manufactures consent through the operation of the FIPs.

Privacy Pessimism is reactive, negative, and largely ineffective at protecting individuals in information relationships. It is worn out. If privacy law is to survive, if ordinary people are to have any meaningful participation in when, whether, and how their data is being used, some positive articulation of what good privacy can do is necessary. We offer such a theory in the next Part.

III. A THEORY OF PRIVACY AND TRUST

Getting past privacy's pessimism problem requires companies and confidants to recognize that protecting the privacy of others is mutually beneficial. Businesses, intermediaries, carriers, and intimates must *want* privacy for articulable reasons beyond moral or ethical concerns. Without articulable benefits to recipients of personal information, we will never escape Privacy Pessimism.

Our current set of ground rules about what kinds of data uses are permissible will not create a sustainable digital society. To remedy this problem, we offer a new theory of privacy and trust. Put simply, privacy matters because it enables trust. Privacy rules can govern the uses of information in relationships, and these rules can build trust. Trust-promoting privacy rules allow people to safely disclose personal information in ways that benefit not just individuals, but the entities they share their data with as well. Understanding how privacy rules can promote trust goes beyond the Harm Principle. Instead of remedying speculative harm,

---

Analytics, 11 NW. J. TECH. & INTELL. PROP. 239 (2013).

59. *See* Richards, *supra* note 1, at 59 ("[T]he available evidence suggests that people do in fact care about privacy, but they are bewildered by the difficulty of protecting their personal information in a time of rapid technological change and limited options.").

privacy can promote trust and promise a way forward for the safe and equitable collection, use, and disclosure of information in long-term, sustainable relationships. Similarly, trust mitigates the problems and distrust that stem from the Control Illusion. From this perspective, privacy isn't a paradox, it is essential to our digital future. It's not a drain on progress, but rather a signpost to the way forward.

D. *Conceptualizing Trust*

Trust is an essential component of healthy relationships and healthy societies.[60] Although various disciplines define trust in various ways, at bottom, "trust is a state of mind that enables its possessor to be willing to make herself vulnerable to another—that is, to rely on another despite a positive risk that the other will act in a way that can harm the truster."[61] Trust allows cooperation with other people in spite of the fact that exposing ourselves enables them to harm us.

There is a vast literature on trust across a variety of academic disciplines, from social sciences like political science and psychology to fields as wide-ranging as medicine, management, and neuroscience.[62] There is also substantial legal

---

60. *See, e.g.*, FRANCIS FUKUYAMA, TRUST: THE SOCIAL VIRTUES AND THE CREATION OF PROSPERITY 26 (1995); Diego Gambetta, *Can We Trust Trust?*, *in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 217 (Diego Gambetta ed., 1988); PIOTR SZTOMPKA, TRUST: A SOCIOLOGICAL THEORY 25 (1999); THE WESTMINSTER DICTIONARY OF CHRISTIAN ETHICS 632 (James F. Childress & John Macquarrie eds., 1986); Margaret M. Blair & Lynn A. Stout, *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law*, 149 U. PA. L. REV. 1735, 1745-46 (2001); Eli Bukspan, *Trust and the Triangle Expectation Model in Twenty-First Century Contract Law*, 11 DEPAUL BUS. & COM. L.J. 379, 415 (2013).

61. Claire A. Hill & Erin Ann O'Hara, *A Cognitive Theory of Trust*, 84 WASH. U. L. REV. 1717, 1723-24 (2006) (citing Denise M. Rousseau et al., *Not So Different After All: A Cross-Discipline View of Trust*, 23(3) ACAD. MGMT. REV. 393, 394-395 (1998)). *See also* FUKUYAMA, *supra* note 60; Gambetta, *supra* note 60; Frank B. Cross, *Law and Trust*, 93 GEO. L.J. 1457, 1461 (2005); Sirkka L. Jarvenpaa & Emerson H. Tiller, *Customer Trust in Virtual Environments: A Managerial Perspective*, 81 B.U. L. REV. 665, 677-78 (2001).

62. KENNETH J. ARROW, THE LIMITS OF ORGANIZATION (1974); BERNARD BARBER, THE LOGIC AND LIMITS OF TRUST (1983); Morton Deutsch, *Cooperation and Trust: Some Theoretical Notes*, *in* 10 NEBRASKA SYMPOSIUM ON MOTIVATION 275 (1962); Gambetta, *supra* note 60; RUSSELL HARDIN, TRUST AND TRUSTWORTHINESS (2002); Jack Knight, *Social Norms and the Rule of Law: Fostering Trust in a Socially Diverse Society*, *in* TRUST IN SOCIETY 354 (Karen S. Cook ed., 2001); PAUL SEABRIGHT, THE COMPANY OF STRANGERS: A NATURAL HISTORY OF ECONOMIC LIFE (2004); TRUST IN ORGANIZATIONS: FRONTIERS OF THEORY AND RESEARCH (Roderick M. Kramer & Tom R. Tyler, eds., 1996); Philip Worchel, *Trust and Distrust*, *in* THE SOCIAL PSYCHOLOGY OF INTERGROUP RELATIONS 174 (William G. Austin & Stephen Worchel eds., 1979); Mark A. Hall et al., *Measuring Patients' Trust in Their Primary Care Providers*, 59 MED. CARE RES. & REV. 293 (2002); Hill & O'Hara, *supra* note 61, at 1796; Brooks King-Casas et al., *Getting to Know You: Reputation and Trust in a Two-Person Economic Exchange*, 308 SCI. 78 (2005); Michael Kosfeld et al., *Oxytocin Increases Trust in Humans*, 435 NATURE 673 (June 2, 2005); Kevin A. McCabe & Vernon L. Smith, *A Comparison of Naïve and Sophisticated Subject with Game Theoretic Predictions*, 97(7) PROC. NAT'L ACAD. SCI. 3777 (2000); *Special Topic Forum on Trust In and Between Organizations*, 23 ACAD. MGMT. REV. 393 (Denise M. Rousseau et al. eds., 1998); *See also* Julian B. Rotter, *Interpersonal Trust, Trustworthiness, and Gullibility*, 35 AM. PSYCHOL. 1, 1 (1980) ("Common sense tells us that interpersonal trust is an important variable affecting human relationships at all lev-

scholarship on the role of the law in general in generating or discouraging trust,[63] as well as in such sub-disciplines as contracts, corporations, and the law of fiduciary duties.[64] Our purpose in this paper is not to advance a theory of trust for all purposes or even all purposes in the law. Our goal is more modest. While we recognize and draw from the vast scholarly literature on trust, we have no wish to enter academic debates other than how we should think about privacy rules in a digital society, for that problem is large enough.

We offer instead a theory of trust in the context of information relationships that allows us to better understand why legal, technological, and social rules regulating the collection, uses, and flows of information in those relationships can make us all better off.[65] Put simply, privacy rules are necessary to build the trust our digital society needs not merely to function sustainably over the long term, but also to flourish. There have been occasional references to trust in the scholarship on law, technology, and privacy, but trust has failed to develop as a core justification for why privacy matters.[66] In this paper, we make exactly that case: that thinking of privacy in terms of trust is essential, and that trust must become an essential part of the legal conversations about data, innovation, technology, and privacy.

In the context of information relationships, trust means the willingness to become vulnerable to a person or organization by disclosing personal infor-

---

els . . . ."); Tom R. Tyler, *Trust and Law Abidingness: A Proactive Model of Social Regulation*, 81 B.U. L. REV. 361, 362 (2001); Russell Hardin, *Distrust*, 81 B.U. L. REV. 495, 496 (2001); Justin (Gus) Hurwitz, *Trust and Online Interaction*, 161 U. PA. L. REV. 1579 (2013).

63. Hill & O'Hara, *supra* note 61, at 1720; Tamar Frankel and Wendy J. Gordon, *Symposium: Trust Relationships*, 81 B.U. L. REV. 321 (2001); Tyler, *supra* note 62.

64. *See, e.g.* CHARLES FRIED, CONTRACT AS PROMISE: A THEORY OF CONTRACTUAL OBLIGATION (1981); Blair & Stout, *supra* note 60 at 1738 ("We contend that people often trust, and often behave trustworthily, to a far greater degree than can possibly be explained by legal or market incentives."); John J. Chung, *Promissory Estoppel and the Protection of Interpersonal Trust*, 56 CLEV. ST. L. REV. 37, 38-39 (2008).

65. A very small number of legal scholars have suggested that trust might be important in privacy disputes. Indeed, this is a claim that each of us has made in prior work. *See* Richards, *supra* note 1; RICHARDS, *supra* note 3. In a forthcoming article, Ari Waldman draws on the work of sociologists to argue that sociological notions of trust are broader than the "everyday trust" we have in our friends and family members. Waldman concludes from this analysis that privacy and trust are the same thing. Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in the Twenty-First Century*, 69 U. MIAMI L. REV. 559, 629. While we agree with Waldman that modern understandings of privacy fail to account for trust, we disagree with him to the extent that he thinks trust and privacy are just synonyms for each other. In our view, privacy and trust are distinct concepts, and trust is an important end that privacy law can serve. Privacy rules—rules governing the treatment of personal information—can serve many purposes, not just remedying the harms of Privacy Pessimism, but protecting our civil liberties, *see* RICHARDS, *supra* note 1, and a whole host of other goals. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2009). Rather than bind all of privacy law to the mast of trust, for the reasons we give in this article, we think it is sufficient (and more nuanced) to argue that rules governing personal data in information relationships are trust-promoting, and that this function is essential for the kind of sustainable digital society we should want to build.

66. *See, e.g.* Hurwitz, *Trust and Online Interaction*, *supra* note 62; Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron*, 81 B.U. L. REV. 635 (2001); Waldman, *supra* note 65.

mation. Some terminology is necessary to aid in precision. We will refer to disclosers of this personal information as *trusters*, the act of sharing sensitive personal information as *entrusting*, and the recipient of such information as *entrustees*. While the natural term for one entrusted with personal information is a "trustee," we are mindful of the specific meaning of this term within, for example, fiduciary and estate law. We will use the term "entrustee" for greater precision, but we are also mindful that the power of an information recipient to harm another is part of the historical basis for the imposition of a trustee relationship in the law of fiduciaries.[67] The difference between an "entrustee" and a "trustee" may be negligible in practice. We nevertheless want to separate them because an "entrustee" is a factual description ("someone has entrusted their data with me . . ."), while becoming a "trustee" means the imposition of legal obligations (". . . and the law requires me as her Trustee to treat it a certain way").

Let us illustrate how these terms work in practice. We are all trusters at various times. As trusters, we share data by entrusting it with entrustees. A truster can be a bank customer, the user of a search engine, or a customer at Target. In these cases, the entrustee is the bank, the search engine, or the big box retailer, and the information being entrusted can be financial data, search queries, or information about the consumer's purchases.

When trusters entrust information about themselves, they make themselves vulnerable. Their vulnerability might include increased risk of information misuse, unauthorized disclosure, manipulation, or loss of autonomy. A bank could leave their account numbers on a laptop in an airport.[68] A search engine could turn their queries over to the government[69] or the general public.[70] Target could guess that they are pregnant and market to them at their time of vulnerability,[71] or Target could itself be the victim of a data breach.[72] The possibilities for disclosure, injury, or manipulation in such cases are limited only by the human potential for innovation. Once a truster's information is disclosed, she no longer has sole control over its use and dissemination.[73] She is exposed and at the mercy of

---

67. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 135 (2007).

68. *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012); *see also* Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006).

69. *See, e.g.*, Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D. Cal. 2006).

70. *See, e.g.*, Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all [http://perma.cc/Y2YL-DJQQ].

71. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all [http://perma.cc/TPV6-WNGY].

72. *A Message from CEO Gregg Steinhafel about Target's Payment Card Issues*, TARGET (Dec. 20, 2013), http://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca [http://perma.cc/9S7W-J8ZG].

73. Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 658 (2012) ("[I]ndividuals lose control of their personal information once they disclose it on the Internet.").

the entrustee.

When people disclose personal details within information relationships, two distinct kinds of vulnerabilities occur. The first is vulnerability to actions by the trustee. One of us has written regarding surveillance that "information gives the watcher increased power over the watched that can be used to persuade, influence, or otherwise control them."[74] The same is true within information relationships. Employees can be immediately fired, insurance can be denied, friends can be embarrassed, lovers can be devastated by the disclosure of secrets or sexy photos. Increasingly, Internet users can be manipulated by technological design guided by companies with an intimate knowledge of their background and preferences. If you know your customers well, it is much easier to nudge them into doing what you want them to do, even when it is a choice they might not otherwise have made freely.[75]

A second kind of vulnerability faced by trusters is to third parties who receive the personal information from the entrustee. This can happen when the entrustee sells or rents the data "downstream," or it can happen when the entruster's security is breached by a true third party. An ISP might sell web-surfing habits to an advertising company or data broker.[76] Any retailer, data broker, or other entity might get hacked by online criminals.[77] When trusters intentionally or unintentionally disclose entrusted information to others, entrustees can be manipulated, user profiles can be impersonated, reputations can be destroyed, and bank accounts can be cleaned out.

Virtually every disclosure of personal information in the modern age leaves the discloser vulnerable in some way, if even only incrementally. As a result, every information relationship involves some degree of trust, or willingness to become vulnerable. This is true even if that trust is not a conscious one on the part of the truster.[78] The phenomenon of trust exists in all information relationships, though of course to different degrees. The key, then, is determining which information relationships require extra scrutiny from the law.

E. *Why Trust Matters in Information Relationships*

Because disclosure of personal data leaves people vulnerable, trust is the glue that holds together virtually every information relationship. An information relationship is any relationship that requires personal information to develop or

---

74. Richards, *supra* note 23, at 1956.

75. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Duhigg, *supra* note 71.

76. Natasha Singer, *Your Online Attention, Bought in an Instant*, N.Y. TIMES (Nov. 17, 2012), http://www.nytimes.com/2012/11/18/technology/your-online-attention-bought-in-an-instant-by-advertisers.html?pagewanted [http://perma.cc/D6DA-C3C6].

77. Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUS. (Mar. 13, 2014), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data [http://perma.cc/6C67-758Y].

78. Cross, *supra* note 61, at 1459; Hill & O'Hara, *supra* note 61, at 1721-22.

achieve a particular goal. This includes a person's relationship with merchants, doctors, employers, common carriers, intermediaries, friends, and intimate partners.[79] And in practice, privacy rules—rules governing the uses of personal information—are essential requirements for the existence of these trust-dependent relationships in the first place.

Trust in these relationships produces numerous benefits, but three are particularly worth highlighting. These three values—commerce, social interaction, and free expression—cannot exist without a willingness to become vulnerable to the actions of others.

Commerce. Commercial relationships, the engine of any economy, are entirely a product of trust. Without this trust, our modern way of life simply would not exist. When privacy is conceptualized as trust, it becomes clear how privacy can be essential for business.[80] If consumers cannot trust businesses with information, they will be hesitant to buy goods and services that require information relationships. Online commerce is particularly reliant upon trust.

Trust is essential to nearly every component of commerce, not just aspects involving privacy and personal information. Trust in commerce begins with the most common initiator of a commercial exchange—a promise which leads to a contract.[81] As first-year law students learn, the most important tool in commerce, the contract, is essentially a mechanism for encouraging and protecting trust.[82]

---

79. *See, e.g.*, Avner Ben-Ner & Louis Putterman, *Trusting and Trustworthiness*, 81 B.U. L. REV. 523, 523 (2001); Cross, *supra* note 61, at 1459; *see also* G. Richard Shell, *Opportunism and Trust in the Negotiation of Commercial Contracts: Toward a New Cause of Action*, 44 VAND. L. REV. 221, 265 (1991); *cf.* Hurwitz, *supra* note 62 (discussing the vital role of trust between Internet users, Internet intermediaries, and the architecture of the Internet itself); Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 913 (2006); Joel Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105 (1995); Larry E. Ribstein, *Law v. Trust*, 81 B.U. L. REV. 553, 554-55 (2001); Ethan J. Leib, *Friends As Fiduciaries*, 86 WASH. U. L. REV. 665, 673 (2009).

80. Nicole Ozer, *Privacy and Free Speech: It's Good for Business*, ACLU CAL. (2d ed. 2012), http://www.americanbar.org/content/dam/aba/events/labor_law/2013/04/aba_national_symposiumontechnologyinlaboremployementlaw/2_conley.authcheckdam.pdf [http://perma.cc/L45X-5DQK].

81. Bukspan, *supra* note 60, at 382-83. Bukspan notes how "[t]he idea of interpersonal trust has personal, social, moral, psychological, and utilitarian advantages that are consistent with common sense and easily relatable. Thus, it comes as no surprise that interpersonal trust has been adopted into many fields, particularly social and economic fields. From a social perspective, trust is understood as a vital element in the relationship between people." *Id.* Buskpan argued that trust is an essential ingredient for commerce, stating: "Mutual trust is a tool that is used to avoid economic pitfalls . . . . [I]nterpersonal trust promotes cooperation and contributes to economic performance in large organizations." *Id.*; *see also* Cross, *supra* note 61, at 1460 ("There is evidence that legal regulation strengthens securities markets around the world. Because investment in corporate equity requires at least a modicum (and sometimes a great deal) of trust, this evidence suggests the positive effect of the law. Other international evidence shows the benefit of the law and contracts on overall economic growth, providing more evidence that law is associated with greater trust.").

82. Anthony J. Bellia Jr., *Promises, Trust, and Contract Law*, 47 AM. J. JURIS. 25, 25-26 (2002) ("By making a promise, a person invites another to trust, and to break a promise is to

While trust has not been fully embraced in regulatory conversations about privacy, it has played a critical role in commerce and consumer protection. Kenneth A. Bamberger and Deirdre K. Mulligan's research into the practices of corporate privacy officers revealed that "promoting consumer trust, rather than protecting individual privacy, motivates many recent privacy interventions."[83]

Intimacy. People simply cannot be close to each other without trusting others with personal information, which is often deeply sensitive. We trust those we love by revealing ourselves (sometimes quite literally). We expose our hopes and fears, our wishes and secrets, our body parts, and our desires to intimates, trusting that they will not reveal what we have shown and told them to others. Most especially, we trust that they will be loyal with our confidences and will not use what they have learned against us.

Trust is an essential component for friendship as well. Friends share basic kinds of information such as hobbies, opinions, and jokes. But true friendship is based upon much more personal disclosures and experiences. Psychologists Irwin Altman and Dalmas Taylor have shown that the strength of relationships is based upon the frequency of reciprocal personal disclosure and degree of vulnerability that reciprocal disclosure creates.[84] In other words, the quality of friendships is defined by the extent to which we trust each other with personal disclosures.[85] Altman's theory of privacy as a boundary regulation process works with his social penetration theory to establish that privacy is "selective control of access to the

---

abuse that trust."). Bellia noted that many theorists have argued that "in order to maximize aggregate preferences, one must have some incentive to rely on certain promises. The incentive to rely on a promise exists only to the degree that a promise is trustworthy." *Id.* Bellia summarizes the theorists who claim that the role of contract is essentially "to protect the ability of individuals to trust promises in circumstances in which that trust is socially beneficial." *Id.* at 28 ("In many contexts, it is the enforceability of promises that creates possibilities for relationships of lesser trust to ripen into relationships of greater trust."); *see also* Bukspan, *supra* note 60, at 379 ("The concept of trust best explains the true nature of contract law and is found in key contract-law doctrines, such as good faith and public policy.").

83. Bamberger & Mulligan, *supra* note 6, at 260. According to Bamberger and Mulligan, "[t]he language of 'trust,' and the connection between privacy and consumer protection, first arose on the global stage during the early days of the commercial Internet." *Id.* at 279. Bamberger and Mulligan found that trust was truly the impetus for companies who sought to protect privacy. The privacy leaders they interviewed as part of their research equated privacy to trust and respect for people, even if they had difficulty articulating what trust rules should look like. *Id.* at 283 ("The link between privacy, trust, and commerce was underscored by repeated consumer pushback after corporate privacy blunders. Companies announced information-sharing deals only to cancel them once masses of consumers made their objections known.")

84. IRWIN ALTMAN & DALMAS A. TAYLOR, SOCIAL PENETRATION: THE DEVELOPMENT OF INTERPERSONAL RELATIONSHIPS (1973); Irwin Altman, *Reciprocity of Interpersonal Exchange*, 3 J. THEORY SOC. BEHAVIOUR 249 (1973); Dalmas A. Taylor, *The Development of Interpersonal Relationships: Social Penetration Processes*, 75 J. SOC. PSYCH. 79 (1968); *see also* STEPHEN LITTLEJOHN, THEORIES OF HUMAN COMMUNICATION 250 (2002) (describing social penetration theory as "[t]he idea that relationships become more intimate over time when partners disclose more and more information about themselves").

85. Altman, *Reciprocity of Interpersonal Exchange*, *supra* note 84; Taylor, *The Development of Interpersonal Relationships: Social Penetration Processes*, *supra* note 84.

self."[86] This insight might seem intuitive, but it has yet to be fully incorporated into a policy that promotes trust in the interests of establishing and maintaining friendship and intimacy.[87]

This theory helps us understand why we disclose even more information on social media when we have privacy settings.[88] At first, the research around privacy settings confused us. Why would those that are contentious enough about privacy to employ privacy settings actually share more information? The reason is that people disclose more when they trust. When they believe that the other party is trustworthy, they are more likely to share, just as they do with their doctors, lawyers, and spiritual advisors. When control is not an illusion, trusted sharing can occur. Privacy is thus not merely an interest for selfish users. Contrary to the mantra of Dave Eggers' fictitious social network "The Circle" in his novel of the same name, privacy is not theft.[89] Instead, it is good for businesses like social media that need users to share with friends in order to be considered successful. Trust enables the strong relationships that make sustainable digital business possible.

Expression. Finally, trust within information relationships is critical for free expression and a precursor to many kinds of political engagement. We have become used to talking about the Internet purely in the economic language of the

---

86. IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING (1975); Stephen T. Margulis, *On the Status and Contribution of Westin's and Altman's Theories of Privacy*, 59 J. SOC. ISSUES 411, 412 (2003). Other scholars have built upon Altman's concept to theorize that disclosure happens only when we trust that the information is safe within an outer boundary. SANDRA PETRONIO, BOUNDARIES OF PRIVACY (2002); Valerian J. Derlega & Alan L. Chaikin, *Privacy and Self-Disclosure in Social Relationships*, 33 J. SOC. ISSUES 102 (1977); Leysia Palen & Paul Dourish, *Unpacking "Privacy" for a Networked World*, CHI '03 PROC. ACM SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS., Apr. 5-10, 2013, at 129, 130; Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 919-20 (2005).

87. *See generally* ETHAN LEIB, FRIEND V. FRIEND: THE TRANSFORMATION OF FRIENDSHIP AND WHAT THE LAW HAS TO DO WITH IT (2011); Leib, *supra* note 79, at 670 ("We should accept close friendship as triggering certain fiduciary duties. Courts have already started to treat friends as fiduciaries—and there is much that can be appreciated about friendship itself when friends begin to see their relationships through the lens of the fiduciary concept."); *see also* Ethan J. Leib, *Contracts and Friendships*, 59 EMORY L.J. 649, 652 (2010).

88. Laura Brandimarte, Alessandro Acquisti & George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf [http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf]; *see also* Fred Stutzman, Ralph Gross & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY 7 (2012); Maritza Johnson, Serge Egelman & Steve Bellovin, *Facebook and Privacy: It's Complicated*, SYMP. ON USABLE PRIVACY AND SECURITY, July 11-13, 2012, http://www.guanotronic.com/~serge/papers/soups12-facebook.pdf [http://perma.cc/37EQ-MC2T]; Somini Sengupta, *Study: Facebook Users More Protective Even as They Reveal More About Themselves*, N.Y. TIMES (Mar. 5, 2013), http://bits.blogs.nytimes.com/2013/03/05/study-facebook-users-more-protective-even-as-they-reveal-more-about-themselves [http://perma.cc/98QB-ZKRU].

89. DAVE EGGERS, THE CIRCLE (2013).

market. From this perspective, Internet users are consumers rationally maximizing their preferences. But the Internet has long been a forum for political engagement and free speech, and it was such well before the "dot-com" era and the rise of the surveillance economy turned the Internet into a shopping mall as well. It remains a source of political fundraising,[90] political information,[91] and political activism.[92] The Internet's consumers are also citizens, and the way their access to information is structured has enormous effect on political debate and the political process more generally.

The architecture of the Internet relies upon our ability to trust each other in routing communications.[93] People must also be able to trust recipients with possibly controversial ideas that are not yet fully formed. Thus, as a practical matter, people need to be able to rely upon intermediaries and recipients to engage politically and further the free speech ideals of self-development, self-governance, government accountability, and the search for truth. Trust is not only necessary to protect our economic interests; it is an essential component of our political rights and civil liberties. Without privacy rules promoting trust in digital systems, even freedom of speech is imperiled.

In our lifetimes, communication technologies based upon paper have increasingly been supplemented or even replaced by digital forms; emails have replaced letters, websites have replaced newspapers, and electronic books (and books ordered over the Internet) have begun to rival those sold in bookstores for market share. These digital technologies have been a force for good, expanding both our access to knowledge and our practical ability to engage in free expression. But while our digital technologies expand our reach, they are capable of monitoring our reading, thinking, and private communications in ways that would be impossible for paper-based technologies. Whenever we shop, read, speak, and think, we now do so using computers that create records of these activities.[94]

Our ISPs, for example, have records of every web site we visit—a virtual transcript of our intellectual explorations, of our reading and thinking. Consider further all the searches you may have entered into Google's search box, or everything

---

90. Aaron Smith, *The Internet's Role in Campaign 2008*, Pew Research Center, Apr. 15, 2009, http://www.pewinternet.org/2009/04/15/the-internets-role-in-campaign-2008 [http://perma.cc/MZT5-FPPE].

91. Amy Mitchell et al., *Political Polarization and Media Habits*, Pew Research Center, Oct. 21, 2014, http://www.journalism.org/2014/10/21/political-polarization-media-habits [http://perma.cc/H78D-MDH8]; Amy Mitchell, *State of the News Media 2014*, , Pew Research Center, March 26, 2014, http://www.journalism.org/2014/03/26/state-of-the-news-media-2014-overview [http://perma.cc/37ZU-XGAS].

92. Yochai Benkler et al., *Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate*, Berkman Center Research Paper No. 2013-16 (July 19, 2013).

93. Hurwitz, *supra* note 62, at 1580 ("From its inception in the 1960s through commercialization in 1993, the Internet was a relatively simple network that was designed, constructed, and used by a relatively small community of research and governmental institutions with broadly aligned incentives . . . [E]ven as these institutions gave way to diverse commercial interests, trust remained an organizing principle").

94. RICHARDS, *supra* note 3, at 1.

you have said on the phone. Many powerful but shadowy entities, from data brokers to the National Security Agency, have shown an interest in our intellectual records—our reading habits, surfing habits, and private communications. Such activities threaten our intellectual privacy, the protection from surveillance or interference when we are engaged in the processes of generating ideas—thinking, reading, and speaking with confidantes before our ideas are ready for public consumption.

Surveillance or interference of our reading and thinking can drive our beliefs to the average, the mainstream, and the boring. Many studies document the often substantial deterrent effects of surveillance on criminal activity, from employee theft[95] to misbehavior by police.[96] But in a free society surveillance can have a substantial chilling effect on thought, reading habits, and private speech. Recent studies, for example, demonstrate that the Snowden revelations produced a chilling effect on Google searches, in areas not merely related to national security, but also things that were unrelated to the NSA's dragnet, like divorce lawyers, mental illness, and weight loss.[97] Another study suggested that surveillance makes writers and journalists more likely to self-censor.[98]

As a society, we say frequently that we care about individuality, diversity, eccentricity, and the vibrant weirdness that freedom makes possible. If we don't have intellectual privacy, all of these important values that make life worth living are threatened. But rules protecting intellectual privacy can safeguard the trust in our digital tools to enable fearless and unfettered intellectual exploration and private communication. This is a reality that librarians recognized decades ago, when they established both professional duties and legal requirements protecting the privacy and confidentiality of patron records.[99] Today librarians remain among the most trusted information professionals.[100]

Intellectual privacy rules produce the trust in digital systems that enables engagement with ideas, political association, and truly free speech to flourish. From this perspective, trust-promoting privacy rules serve not merely economic values, but those of a constitutional magnitude as well. Trust is essential for the kind of society we want to live in. To review, trust drives commerce and it creates the conditions for intimacy and free expression. If we want to flourish as humans, we must be able to trust each other.

---

95. Lamar Pierce et al., *Cleaning House: The Impact of Information Technology Monitoring on Employee Theft and Productivity,* MIT Sloan Research Paper No. 5029-13 (Oct. 15, 2014).

96. *See generally*, Richards, *supra* note 23 (collecting examples).

97. Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior*, SSRN (Apr. 29, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564.

98. *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, PEN America (Nov. 12, 2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf [http://perma.cc/S27M-7R3U].

99. Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L. J. 689 (2013).

100. Maureen Sullivan et al., *Librarians Working Together*, American Libraries Magazine, (June 25, 2013), http://americanlibrariesmagazine.org/2013/06/25/librarians-working-together [http://perma.cc/PE6E-3435].

IV. REJUVENATING PRIVACY LAW THROUGH TRUST

Privacy law's legacy of harm and control has left our privacy torts useless and the FIPs threadbare. Privacy law is not just pessimistic. It is worn out. In this Part, we show how trust can rejuvenate privacy law and policy.

First, trust can add nuance and force to foundational privacy concepts such as confidentiality, transparency and security by reimagining them as discretion, honesty, and protection. In addition to rejuvenating old privacy concepts, we introduce loyalty as a foundational concept in privacy law. We argue that entrustees have a duty to avoid unreasonable and dangerous self-dealing. These concepts are not new. They are foundations of one of the most established legal concepts involving trust in relationships: the law of fiduciaries.

A. *Relying on Fiduciaries*

The best place to look for wisdom on how to secure trust is from relationships that are defined by trust—fiduciaries. Fiduciaries are an ancient concept in the common law, and the central goal of fiduciary law is to protect against the exploitation of a vulnerability created by trust in another.[101] From this perspective, fiduciary relationships are the paradigm case for law enabling trust by imposing duties such as care, loyalty, and confidentiality. It should thus be no surprise that most if not all fiduciary relationships also fit within the larger category we have been calling "information relationships."

A few prominent privacy and cyberlaw scholars have also suggested that privacy law might take cues from the law of fiduciaries. Jack Balkin has proposed looking to the law of fiduciaries in the privacy context, explaining that "[t]he concept of an information fiduciary helps us understand how we might protect digital privacy while not running afoul of the First Amendment. . . . Traditionally, a fiduciary is a person who has a relationship of trust with a party (the beneficiary), and who is authorized to hold something valuable—for example—the beneficiary's

101. Leib, *supra* note 79, at 732; J.C. SHEPHERD, THE LAW OF FIDUCIARIES (1981); Robert C. Clark, *Agency Costs Versus Fiduciary Duties*, in PRINCIPALS AND AGENTS 55 (John W. Pratt & Richard J. Zeckhauser eds., 1985); Robert Cooter & Bradley J. Freedman, *The Fiduciary Relationship: Its Economic Character and Legal Consequences*, 66 N.Y.U. L. REV. 1045 (1991); Kenneth B. Davis, Jr., *Judicial Review of Fiduciary Decisionmaking—Some Theoretical Perspectives*, 80 NW. U. L. REV. 1 (1985); Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 37 DUKE L.J. 879 (1988); Scott FitzGibbon, *Fiduciary Relationships Are Not Contracts*, 82 MARQ. L. REV. 303 (1999); Robert Flannigan, *The Economics of Fiduciary Accountability*, 32 DEL. J. CORP. L. 393 (2007); Robert Flannigan, *The Fiduciary Obligation*, 9 OX. J. LEGAL STUD. 285 (1989) [hereinafter Flannigan, *The Fiduciary Obligation*]; Tamar Frankel, *Fiduciary Law*, 71 CAL. L. REV. 795 (1983); Lawrence E. Mitchell, *The Death of Fiduciary Duty in Close Corporations*, 138 U. PA. L. REV. 1675 (1990); Eileen A. Scallen, *Promises Broken vs. Promised Betrayed: Metaphor, Analogy, and the New Fiduciary Principle*, 1993 U. ILL. L. REV. 897; L.S. Sealy, *Fiduciary Relationships*, 1962 CAMBRIDGE L.J. 69; J.C. Shepherd, *Towards a Unified Concept of Fiduciary Relationships*, 97 L. Q. REV. 51 (1981); D. Gordon Smith, *The Critical Resource Theory of Fiduciary Duty*, 55 VAND. L. REV. 1399 (2002); Ernest J. Weinrib, *The Fiduciary Obligation*, 25 U. TORONTO L.J. 1 (1975).

assets or other property—and manage them on the beneficiary's behalf."[102] Daniel Solove has also suggested looking to the law of fiduciaries as a way to guide sound policy in the age of data brokers who collect an overwhelming amount of personal information.[103]

We agree with Balkin and Solove that the concept of fiduciaries helpfully reorients privacy and crystalizes the concept of trust in information relationships. To be clear, though, we are not recommending that all relationships of trust should automatically be considered as fiduciary in nature. Imposition of the full panoply of fiduciary duties is a serious and burdensome decision. But the law need not face the binary choice of treating information relationships as either "fiduciary" or "unprotected." Surely some middle ground exists between these two extremes. Accordingly, we recommend that duties inspired by fiduciary law can apply in a flexible and variable way across the full spectrum of information relationships.

In relationships where vulnerabilities are minimized because there is only a small amount of trust, these remedies should be applied sparingly or lightly. Where there is greater trust (or greater potential for exposure), entrustees should be held to higher duties of care and loyalty. Rather than relying on a rigid fiduciary/nonfiduciary distinction, we propose a more flexible approach that recognizes the role of trust is *all* information relationships. Yet our fundamental point is that the law of fiduciary relationship can helpfully shed light on the specific duties and actions that promote and erode trust.

B. *Improving the Existing FIPs*

Although the FIPs are worn out, they remain the foundational structure for the regulation of personal data, not only in the United States, but throughout the world.[104] Replacing the FIPs entirely would be a daunting task. But fortunately, what is needed is not the replacement of the FIPs, but rather their rejuvenation from a procedural means of manufacturing consent into a substantive system of regulating the processing of personal data in the interests of all. Trust can provide the source of that rejuvenation, allowing us to rethink the FIPs in ways that are positive, substantive, and inspiring, rather than pessimistic, procedural, and depressing. When viewed through the lens of trust-building the existing FIPs of Confidentiality, Transparency, and Security become the substantive obligations of Discretion, Honesty, and Protection. Even more importantly, when we thinking about privacy in terms of trust suggests the adoption of a new Fair Information Practice: Loyalty.

---

102. Jack Balkin, *Information Fiduciaries in the Digital Age,* BALKINIZATION, http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [http://perma.cc/T65R-MNZB]. Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. DAVIS. L. REV. 1183 (2016).

103. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2006).

104. *See* Gellman, *supra* note 4.

Our proposed modifications are not merely word games. Discretion, Honesty, Protection, and Loyalty offer an alternative vision of privacy protection that escapes the Harm Principle and the Control Illusion. They identify the substantive values that privacy law should embrace if it is to promote the trust that is essential for sustainable information relationships. But critically, when we argue that privacy law should promote trust, this requires a meaningful, substantive level of trust rather than trickery. By contrast, our vision for a rejuvenated, positive theory of privacy protection requires real trust; trust that is accountable. It is for this reason that the substantive principle of loyalty must be understood as essential to the information privacy law project.

1. *Confidentiality as Discretion*

The concept of confidentiality is perhaps the earliest and most foundational in all of privacy law.[105] Despite its entrenched and robust presence in the doctrine, confidentiality is a surprisingly under-developed concept. In most forms of existing regulation, confidentiality is conceptualized merely as nondisclosure. For example, the limited tort of breach of confidentiality prohibited those within confidential relationships from divulging confidential information to any unauthorized parties.[106] As a FIP, confidentiality is articulated as a mere limit on disclosure. This can either take a vague form like "there shall be limits on the external disclosures of information about an individual a record-keeping organization may make,"[107] or be tethered to the purpose of collection and contingent upon the consent of the data subject.[108]

Conceptualizing confidentiality solely in terms of nondisclosure obligations has limited this otherwise dependable, bedrock concept. In many ways, characterizing confidentiality solely in terms of nondisclosure is like characterizing safe sexual practices solely in terms of abstinence—it's effective, but risks overkill and is often too costly. Because confidentiality is so restricting, most people in information relationships are not confidants. They are free to share the information with whomever they wish. The law is rightfully reluctant to make most recipients of information bound by a legal obligation of confidentiality. People need to be able to share most of the information they receive, whether they are businesses and intermediaries or friends and acquaintances.

---

105. Richards & Solove, *supra* note 67, at 135.

106. *Id.*

107. Privacy Protection Study Commission (PPSC) report, Personal Privacy in an Information Society at 501-502 (1977), http://epic.org/privacy/ppsc1977report [http://perma.cc/L4MG-VMUK].

108. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [http://perma.cc/98M6-3BBX] ("Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.").

Yet people still trust recipients of personal information who are not confidants not to hurt them with that personal information. Is there a middle ground between confidentiality and "every man for himself"? We argue that there is. There are ways other than rigid nondisclosure that entrustees can protect trustors. They can limit to whom they disclose information, they can limit what they share with others, and they can control how they share information to make sure they preserve the trust placed in them. We argue that entrustees can combine all of these strategies: nondisclosure, limited disclosure, trustworthy recipients, and obfuscation to be discreet.

Perhaps the most basic assumption people make when disclosing personal information is that the recipient will be discreet. Discretion, defined as "the quality of behaving or speaking in such a way as to avoid causing offense or revealing private information,"[109] is an implicit part of most information relationships.[110] We trust doctors not to reveal information about our health and mental state; we trust lovers not to kiss and tell; and we trust ISPs and search engines not to reveal our search history. In information relationships, the quickest way to betray a trust is indiscretion: revealing personal information to the wrong person or in the wrong way.

The most robust form of discretion is confidentiality, which we have elsewhere characterized as an obligation of nondisclosure in relationships.[111] Discretion is a broader concept than confidentiality, as it recognizes that trust can be preserved even when the trustee shares information in limited ways. Our disclosures on social media demonstrate this notion of discretion as "appropriate disclosure."

Most disclosures on social network sites like Facebook, Twitter, and Instagram are not confidential. Yet there is an expectation that they are less than "public"—that they will not be read by most people, just by our friends or perhaps our "friends" in the Facebook sense. Professor Lior Strahilevitz has observed this phenomenon and argued that privacy law should take a lesson from the way we expect our disclosures to travel through our offline social networks.[112] Strahilevitz explains that "given the . . . ease with which juicy secrets can spread among people, one might expect that we would play our cards close to our vests, refusing to reveal these embarrassing details to anyone. Yet it is likely that most of us have

---

109. *Discretion*, OXFORD ENGLISH DICTIONARIES, http://www.oxforddictionaries.com/us/definition/american_english/discretion [http://perma.cc/U5EP-T6DZ].

110. Lee Rainie et al., *Anonymity, Privacy, and Security Online*, PEW RESEARCH CENTER (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online [http://perma.cc/MSP9-27Q3], (detailing the importance of control over information and importance of authorization of recipients); Susannah Fox, *Trust and Privacy Online*, PEW RESEARCH CENTER (Aug. 20, 2000), http://www.pewinternet.org/2000/08/20/trust-and-privacy-online [http://perma.cc/2EDC-THU2].

111. Richards & Solove, *supra* note 67.

112. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

shared our most embarrassing details with other people: spouses, siblings, parents, best friends, clergy, psychiatrists, coworkers, or perhaps even strangers on transatlantic flights . . . . By common parlance, we still consider these facts to be "secrets" even after we have revealed them to a handful of people."[113] Strahilevitz draws from sociology, network theory, and related disciplines to argue that people make risk calculations when sharing information. They often assume that their disclosures will stay within certain social networks even if it doesn't remain completely confidential.[114] Such calculations rely not merely on notions of practical obscurity, but on discretion as well.[115]

So trust is preserved when entrustees exercise sound discretion in choosing what and to whom personal information is revealed. It can also be preserved when individuals refrain from becoming entrustees. But at its core, discretion protects against wrongful disclosure, and nondisclosure enables our ability to make friendships, communicate with other people, and participate in society.[116] As Daniel Solove explains, "social judgment and social norms can impede these practices . . . . Protection against disclosure shields us from the harshness of social judgment, which, if left unregulated, could become too powerful and oppressive."[117]

When people are confident that their entrustees will be discreet with their personal information, they become free to engage in commercial and social activities that form the basis of modern society.[118] We gossip, we love, we shop, and we seek help. This has benefits not just for the individual, but also for society as a whole. Commercial activity keeps the lights on. Seeking help from medical professionals benefits public health. The exploration of political beliefs leads to a better-informed electorate, better political decisions, and potentially better leaders. All because entrustees remain discreet.

Privacy law should embrace discretion, which reflects the blurry and contextual lines between "public" and "private." Regulators, legislators, and judges should create some kind of obligation on entrustees to obfuscate disclosures such that the general public or specifically unauthorized parties are unlikely to find or understand entrusted information, even when the information relationship is not

---

113. *Id.*

114. *Id.*

115. *See generally* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013); Lauren Gellman, *Privacy, Free Speech, and 'Blurry-Edged' Social Networks*, 50 B.C. L. REV. 1315 (2009).

116. Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1064 (2003).

117. *Id.* ("People's lives in the public sphere are precarious, for they are constantly subject to the judgment of others and to the sting of social sanctions. It is because people care so much about their public lives, about how others in society regard and treat them, that protection against disclosure is important.").

118. Obligations of nondisclosure also allow people to disclose information that might be used against them, such as credit card numbers, health conditions, and any number of other kinds of personal information that can lead to lost employment, identity theft, and reputational harm.

strictly confidential. The tort of breach of confidentiality could be enhanced by taking discretion into account. The Federal Trade Commission could find a lack of discretion in some instances to be an unfair or deceptive trade practice. Such laws could look to whether entrustees made sure that recipients of data were trustworthy or whether they ensured that certain kinds of information were not publicly available through search engines like Google.

2. *Transparency as Honesty*

One of the bedrock notions of privacy law is that companies should be transparent about their data collection, use, and disclosure practices so that individuals will be on notice of any potentially worrisome practices and can tailor their disclosures accordingly.[119] The FIPs refer to this as the "Openness," that "[t]here should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."[120] The law and regulations built upon the FIPs often refer to this as "notice and choice," which we discussed above.

In a notice and choice regime, mere disclosure and transparency is usually sufficient to relieve a company of its legal obligations. As long as the data collector is putting its practices out there, it often does not matter whether the data subject reads or even knows about an entrustee's data practices. This is the Choice Illusion in practice. But if trust is to be kept, it is not sufficient to be merely "open" or "transparent." Trust in information relationships requires an affirmative obligation of honesty to correct misinterpretations and to actively dispel notions of mistaken trust.

At a minimum, entrustees must be honest and open with those who disclose personal information to them. The duty of candor and disclosure is a significant one for fiduciaries.[121] Generally speaking, fiduciary trustees should keep those to

---

119. *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1049 (2012) (citing Paula J. Dalley, *The Use and Misuse of Disclosure as a Regulatory System*, 34 FLA. ST. U. L. REV. 1089, 1093 (2007) ("[D]isclosure schemes comport with the prevailing political philosophy in that disclosure preserves individual choice while avoiding direct governmental interference.")); Joel Reidenberg, et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: A J. OF L. & POL'Y FOR THE INFO. SOC'Y 485 (2015).

120. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [http://perma.cc/GWP4-8YNY].

121. Ethan J. Leib, *Friends As Fiduciaries*, 86 WASH. U. L. REV. 665, 675 (2009) ("This may take the form of requiring doctors to reveal their personal financial interests to their patients (even when those interests are "unrelated to the patient's health") or it may take the form of a general "accounting" requirement, necessitating accurate bookkeeping subject to inspection by the beneficiary as well as the disclosure of all relevant information pertaining to the relationship."); Balkin, *supra* note 102 ("The fiduciary's duty of loyalty may also create a duty of honesty to disclose to the beneficiary how the fiduciary is handling the assets or property.").

whom they are accountable informed. This means accommodating requests for inspection and either affirmatively disclosing or making information available upon request.[122] One rationale for this obligation is that trustees must have the information necessary in order for them to be able to enforce the obligations of the trustee.[123] Obligations of transparency and honestly also help ensure that the trustees are complying with their duty of care and duty of loyalty.

Beyond the narrow category of legal fiduciaries such as trustees, principles of honesty are essential to information relationships more generally. Earlier in our argument, we explained that while the Control Illusion is part of Privacy Pessimism, the problem is one of excessive weight placed on individuals to manage their own privacy from complex, generalized, and often hidden notices. Honesty, by contrast, requires more affirmative steps than passive notice, and includes an obligation to make sure that trusters are actually aware of things that matter to them.[124] It takes the fiction out of constructive notice to require actual notice. Honesty also serves the additional function of forcing companies to take stock of their information practices in order to be accurate when keeping individuals informed.[125]

A focus on honesty can also drive particularized remedies designed to build and maintain trust. California has already mandated privacy policies for mobile apps. GLB and COPPA also require notice. FTC Commissioner Julie Brill's "Reclaim Your Name" campaign, which is designed to increase data broker transparency, is a promising approach for building consumer trust in disclosing personal information.[126]

To be sure, there are many obstacles to ever fully "informing" individuals about a certain practice or risk.[127] Information can be too vast or complex to convey, and the audiences can be too diverse. The goal should not be more notice, but *better* notice. But the goal of honesty-based disclosure in these sorts of cases is broader than just informing. While notice rules are horrible at informing people,

---

122. *Id.*

123. This guiding principle can be seen in the law of irrevocable trusts. *See, e.g.*, Lauren Z. Curry, *Agents in Secrecy: The Use of Information Surrogates in Trust Administration*, 64 VAND. L. REV. 925, 929 (2011) ("Under the most basic principle, a beneficiary of an irrevocable trust is always entitled to information about the trust that is reasonably necessary to allow the beneficiary to enforce the trust, even if the terms of the trust restrict disclosure.").

124. Calo, *supra* note 119.

125. Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1264-65 (2002) ("[C]ritics have largely overlooked . . . important benefits from these notices. Perhaps most significantly, publication of the notices and the new legal obligation to comply with them have forced financial institutions to engage in considerable self-scrutiny as to their data handling practices.").

126. Julie Brill, *Demanding Transparency From Data Brokers*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680-0382-11e3-9259-e2aafe5a5f84_story.html [http://perma.cc/2LMD-ZLPV].

127. *See generally* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, THE FAILURE OF MANDATED DISCLOSURE (2014).

they can be very good at generating the skepticism necessary to avoid a misplaced trust. 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.

"*If I had only known*" is a common response by victims of alleged wrongdoing by others. This refrain is based upon the theory that if certain information had been presented, the would-be victim could have acted differently, or at least knowingly accepted her fate. The idea of notice as savior is the foundation for many disclosure-based regulatory regimes such as privacy policies, Miranda warnings, informed consent, and health warnings on unhealthy products.[128] However, the discussion surrounding notice too often misses the fact that individuals need not fully appreciate risk in order to avoid it. They only need to become skeptical enough to avoid a misplaced trust. If companies or government entities want to avoid creating skeptics, they must embrace and protect the trust users place in them and be honest and transparent.

There are several ways the law might implement honesty requirements. Mandated disclosure regimes might be leveraged to help build trust or, in the least, encourage the kind of skepticism we have mentioned above. Mandated disclosure regimes such as privacy policies, nutrition labels, or informed consent are popular because they are relatively cheap and use a soft regulatory touch. But they are also seen as ineffective, particularly with respect to privacy policies.[129] No one reads the fine print on websites and mobile apps, nor should they be expected to.

A focus on trust might remedy the problems with privacy policies as a tool for consumers. While it is one thing for a company to be forced to list in the fine print the ways in which it collects and shares people's information, it is something else entirely for a company to be forced to admit, "You cannot trust us to be discreet, honest, loyal, or protective." Indications of trust are more intuitive and useful to consumers than dry recitations of what types of information are collected and vague assurances that personal information will only be disclosed to "third party affiliates."

Another way privacy law could better encourage and protect trust is to better situate the concept within the existing law of deception and fraud. Courts and policymakers could find that when people and companies invite or encourage trust, they are making a representation that they must keep. Under this notion, to breach a trust is to deceive. Equating a breached trust with deception will empower the Federal Trade Commission to declare certain breached trusts a deceptive trade practice under Section 5.[130]

Betrayed trusters could also look to the tort of fraud or the law of contracts. This approach would be similar to the finding of an implied confidence, where

---

128. *Id.*

129. *Id.*

130. 15 U.S.C § 45; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

even though no explicit promise of privacy was made, the surrounding norms and context make it clear a trust was invited and a reasonable person would expect it to be maintained.[131]

Trust need not be exclusively a matter of government policy. Companies can also voluntarily adopt trust-enhancing internal policies, safeguards, and organizational schemes. As with data security, companies can segment entrusted information from less critical data and limit the accessibility of the information. Company executives can make trust a priority by requiring employee training, enshrining trustworthy practices in employee manuals and regularly enforcing these obligations. Companies can delete data when it is no longer needed and collect no more information than is necessary for the information relationship. Even if a company accidentally fails to be discreet or protective, it can help maintain trust by creating and implementing a response plan for when a trust is breached.

Because trust is good for business, companies should be competing to be the most trustworthy. Companies that earn the trust of their users will get more information and sales. Consumers that trust companies will have less reason to flee to competitors who might be less trustworthy. The end result is that the information economy can flourish while still protecting consumers. Everyone wins, except the untrustworthy.

3. *Security as Protection*

Attackers have always sought unauthorized access to personal information. This is why file cabinets have long contained locks and even the earliest databases were protected by passwords. Such stores of information were maintained by "secretaries," a profession dating to medieval times as "one who is entrusted with private or secret matters; a confidant; one privy to a secret."[132]

Tort law has been slow to recognize data security obligations because harms from data breaches can be very difficult to prove.[133] (This is of course but another manifestation of the harm fixation). By contrast, the FIPs have always required data security, with language usually along the lines of "personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data."[134] Policymakers have tended to interpret security requirements in terms of the process data holders must take to protect against attackers.[135] This mainly consists of regularly auditing data assets and risk, minimizing data, implementing technical, physical, and

---

131. Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 764 (2014).

132. *Secretary*, OXFORD ENGLISH DICTIONARY (2015).

133. *See infra* Part II.

134. OECD PRIVACY GUIDELINES, *supra* note 120, at § 5.

135. *See* FEDERAL TRADE COMMISSION, *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [http://perma.cc/WH5U-66AF]; 45 C.F.R. § 164.306(a) (2015); 15 U.S.C.A. §§ 6801-6809.

administrative safeguards, and creating and following a data breach response plan.[136]

New threats to data require a more holistic approach to data security than just protecting held data. Entrustees must adopt a mentality of data stewardship, which includes protecting information passed on to others. Put simply, in order to preserve a trust, entrustees must protect data, not just secure databases. This requires going beyond firewalls and passwords and affirmatively acting in the interest of data holders. This is the obligation of Protection.

While there are antecedents to Protection from common law duties owed by bodyguards (for physical protection) and banks and lawyers (for protection of secrets and money), Protection has taken on particular importance in the digital age.

In the early 2000s it became clear that personal data was a critical component of our national infrastructure and that external threats to personal data were mounting. The Privacy Rights Clearinghouse has reported that since 2005 there have been over 4,400 data breaches made public with a total of over 932 million records breached.[137] Such estimates are even more startling given that they fail to include the vast number of data breaches that companies have not reported and the unknown number of breaches occurred without companies realizing that they have happened. Data protection is largely hidden from consumers, who typically have no way of knowing how securely their data is being held, or even if databases containing their personal information have been compromised. People in this situation (which is to say, all of us) can only hope that companies will reasonably protect the data that has been entrusted to them.[138]

That data is constantly under attack is no secret. Almost every week a national story breaks detailing the latest data breach, leading 2014 to be dubbed by some as "the year of the breach."[139] Most individuals likely anticipate that trustees will keep information reasonably safe.[140] This was highlighted by the recent massive Office of Personnel Management data breach, where a number of commenters

---

136. *Id.*

137. *Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach [http://perma.cc/T2F9-BFF8].

138. BRUCE SCHNEIER, LIARS AND OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE (2012).

139. *See, e.g.*, P.J. Smith, *Lessons Learned from 2014: The Year of the Breach*, WIRED INNOVATION INSIGHTS (Dec. 26, 2014, 10:41 AM), http://insights.wired.com/profiles/blogs/lessons-learned-from-2014-the-year-of-the-breach [http://perma.cc/U8U3-FZB9]; Tara Seals, *2014 So Far: The Year of the Data Breach*, INFORMATION SECURITY (Aug. 12, 2014), http://www.infosecurity-magazine.com/news/2014-the-year-of-the-data-breach [http://perma.cc/NLR7-2RSA]; Daniel Fisher, *If 2014 Was the Year of the Data Breach, Brace for More*, FORBES (Jan. 2, 2015), http://www.forbes.com/sites/danielfisher/2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more [http://perma.cc/Q9X3-B7GF].

140. HELEN NISSENBAUM, *Will Security Enhance Trust, or Supplant It?*, *in* TRUST AND DISTRUST WITHIN ORGANIZATIONS: EMERGING PERSPECTIVES, ENDURING QUESTIONS 155 (Roderick Kramer & Karen Cook eds., 2004).

stated a betrayal of their trust in the government to protect their highly sensitive personal information.[141]

People need to be able to trust that entities will protect their data against attackers. Computer company Lenovo breached its users' trust when it surreptitiously installed malware on its new laptops. This code altered users' search results to show them different ads than they would otherwise have seen.[142] The secret deployment of the malware also weakened the laptops' security settings, exposing the computer's browsing history to hackers with the ability to use a particular exploit against the software. In addition to being dishonest and disloyal, this weakening of the computers' security settings violated the duty of Protection.[143]

Protection means more than just setting up a few technical safeguards like firewalls, user authentication requirements, and encryption. It requires a more complete commitment to data protection that includes having procedures to regularly audit the stores of personal information and continuously assess risk using updated threat models, minimizing data collection and storage, instituting procedural and physical safeguards, and preparing a response plan in case of a breach.

Data protection also involves more than just data security. It involves protecting the identity and sensitive attributes of those in stored and released data sets. This means as a practical matter that Discretion will often be essential to protect security as well. The government of New York City betrayed the trust of its tourists and citizens when it released data on 173 million individual taxi trips that were improperly deidentified, inadvertently making it trivial to identify people in the data set.[144] Data sets (big or small) that are shared with others must also be properly scrubbed and protected to minimize the risk that any particular individual will be re-identified. Requirements of this sort are particularly important now that data science is getting better at reidentifying allegedly "anonymized" data sets.[145] More robust techniques of deidentification are being developed, such as k-anonymity and differential privacy, and Protection requires that entrustees (es-

---

141. Jamie Winterton, How OPM Betrayed Me, SLATE (July 16, 2015), http://www.slate.com/articles/technology/future_tense/2015/07/opm_security_clearance_hack_i_trusted_the_government_it_betrayed_me.html?wpsrc=sh_all_dt_tw_top [http://perma.cc/79FT-VEW2].

142. Rosenblat, *Lenovo's Superfish Security Snafu Blows Up in Its Face*, *supra* note 55.

143. *Id.*

144. Alex Hern, *New York Taxi Details Can Be Extracted from Anonymized Data, Researchers* Say, THE GUARDIAN (June 27, 2014, 10:57 AM), http://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn [http://perma.cc/PKV3-A4F4].

145. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 2 (2011); Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117 (2013); Daniel Barth-Jones, *The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now* (June 18, 2012), http://fpf.org/wp-content/uploads/The-Re-identification-of-Governor-Welds-Medical-Information-Daniel-Barth-Jones.pdf [http://perma.cc/4BLU-FF6T].

pecially sophisticated commercial ones) stay abreast of such Protection innovations.[146]

Just as our physical security is a combination of technologies like door locks and legal prohibitions on burglary and assault, so too must data Protection rely on law as well as technologies and marked protections. Such legal protections can include contracts prohibiting recipients from reidentification attempts and obligating them to mandate their duties as entrustees to all downstream holders of the data.[147] For example, the Department of Health and Human Services (HHS) and the FTC recently suggested that those who receive anonymized data, whether it be researchers or companies, must promise in advance (preferably via contract) not to attempt to reidentify it.[148] The data security threats our digital society faces are complex, and we should not shirk from sophisticated, multilayered solutions along these lines. Protection of personal data demands no less.

C. *Introducing Loyalty as a Foundational Privacy Value*

One of the foundational obligations of a fiduciary is loyalty, which is an obligation to avoid in self-dealing at the expense of the entrustee.[149] Yet the concept of loyalty is completely missing from privacy law that regulates those who accept information in a fiduciary-like context. We propose that trust in information relationships can be promoted by establishing loyalty as a foundational concept in privacy law.

Personal information is valuable. In the technology industry, it is commonplace to state that "data is the new oil," meaning a fundamental source of value in the information economy.[150] People are becoming wise to the fact that "free" services are only free in the sense that companies do not charge money for them. Their cost is frequently an implicit or unwitting transaction of the customer's personal information and mental attention to advertisements targeted on the basis of

---

146. *See generally* Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117 (2013).

147. *See generally* Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33 (2010); Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657 (2012).

148. *Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators*, 76 FED. REG. 44,512, 44,519-20 (July 26, 2011); FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf , William McGeveran et al., *Deidentification and Reidentification in Returning Individual Findings from Biobank and Secondary Research: Regulatory Challenges and Models for Management*, 13 MINN. J. L. SCI. & TECH 485 (2012); Robert Gellman, *supra* note 147.

149. *See* RESTATEMENT (SECOND) OF TRUSTS § 170 cmt. a ("A trustee . . . is under a duty not to profit at the expense of the beneficiary . . . unless authorized to do so by the terms of the trust."); Ethan J. Leib, *supra* note 79.

150. ANGWIN, supra note 7, at 32.

that data.[151] Given the commercial value of personal data, it is not surprising that entrustees in information relationships are tempted to use personal information they receive for their own benefit.

The duty of loyalty is a bedrock principle of the law of fiduciaries. A trustee, for example, cannot lend entrusted funds to herself; nor can trust property be bought by a trustee unless explicitly authorized by the trust instrument.[152] The rationale behind the obligation to avoid self-dealing is to cut off avenues for fraud. As one court put it, "The rule is founded in the highest wisdom. It recognizes the infirmity of human nature, and interposes a barrier against the operation of selfishness and greed. It discourages fraud by taking away motive for its perpetration."[153] Formal trustees are bound to act in the interest of the principal.

Outside the formal context of fiduciary law, not all self-dealing will betray trust. Companies can legitimately use entrusted personal information to their benefit in many different ways. Data can be mined to offer and improve services, effectively anonymized for public research, and even shared with others also willing to preserve a trust. Facebook leverages the personal information of its users to create a precise advertising service. One of Amazon's most valuable features is its recommendation system, which relies upon user data.[154] Websites routinely share deidentified data with others for profit and to simply fine-tune their services.[155]

Such activities are loyal only up to a point, as personal information can quite easily be used to the detriment of trusters. Recall that when we trust others by disclosing our personal information, we expose our vulnerabilities. We regularly expose our preferences, our weaknesses, our desires, and our tendencies to act in a certain way. Disclosure creates power in trustees who can exploit our personal information for their own gain.

The law of consumer protection, for example, is littered with examples of disloyal companies that have misused personal information entrusted to them, for example by using credit card information or other financial data to engage in un-

---

151. Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606 (2014); Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327 (2012).

152. *See In re* Noonan's Estate, 63 A.2d 80, 83 (Pa. 1949) (holding the executor liable for self-dealing in selling the trust property where he had a personal interest in the transaction that might affect his judgment); RESTATEMENT (SECOND) OF TRUSTS § 170(1) cmt. b (1959) ("A trustee with power to sell trust property is under a duty not to sell to himself . . . [even if he] acts in good faith . . . [and] pays a fair consideration.").

153. *In re* Ryan's Will, 52 N.E.2d 909, 923-24 (N.Y. 1943) (quoting Justice Kent in Bergen v. Bennett, 1 Caines, Cas., 19); *see also* Charles Bryan Baron, *Self-Dealing Trustees and the Exoneration Clause: Can Trustees Ever Profit from Transactions Involving Trust Property?*, 72 ST. JOHN'S L. REV. 43 (2012).

154. Richards, *Social Reading*, *supra* note 99.

155. *See, e.g.*, Ricardo Alonso-Zaldivar & Jack Gillum, *HealthCare.gov Quietly Sharing Personal Data*, WASH. TIMES (Jan. 20, 2015), http://www.washingtontimes.com/news/2015/jan/20/healthcaregov-quietly-sharing-personal-data/?page=all [perma.cc/PLG4-ADUA].

authorized transactions. In *FTC v. Hill*, the FTC alleged that defendant used consumers' financial and credit card data to "pay for goods or services without the consumers' consent."[156] Less nefarious, but equally disloyal, was Orbitz's tactic of showing pricier hotel rooms to users it knew were using Apple computers, based upon the assumption that these users were used to paying more for goods and services.[157]

Disloyalty can take a variety of forms, many of which are not merely financial. Consider the Facebook emotional contagion experiment, in which researchers manipulated Facebook's news feed by, among other things, showing fewer positive posts to some users to see if they would lead to greater user expressions of sadness.[158] Exploiting the power to make trusters unwittingly sad (or angry, or hungry, or aroused) is the definition of disloyalty.

Consider also Uber, the app-based transportation network and taxi company. Uber is entrusted with incredibly sensitive data beyond financial information, including where its users currently are, where they have been, and where they are going. The company created an interface it ominously called "God View," which let administrators see all of the cars in a city as well as the users who are waiting for cars.[159] When "God Mode" was used to entertain corporate party-goers by pointing out one-night stands, this was not loyal. (It had many other issues, of course, including not being discreet). More infamously, Uber was disloyal when it contemplated mining its database to find information to smear journalists who were critical of its business.[160] In such cases, the threat of exposure has ramifications not just for the journalists who used Uber, but political and free expression ones from its chilling of public debate.

Ryan Calo has helpfully coined the term "digital market manipulation" to describe this practice of leveraging personal information against consumers in mediated environments.[161] Calo argues that some manipulations of users which exploit vulnerabilities should be legally actionable.[162] Our theory of privacy as trust

---

156. Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Sitesearch (D.Ariz., Dec. 22, 2014), http://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf [http://perma.cc/4U7C-DQ6K].

157. Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J. (Aug. 23, 2012, 6:07 PM), http://www.wsj.com/articles/SB10001424052702304458604577488822667325882 [perma.cc/X23K-TJDJ].

158. Dewey, *9 Answers About Facebook's Creepy Emotional-Manipulation Experiment*, *supra* note 8.

159. Kashmir Hill, *'God View': Uber Allegedly Stalked Users For Party-Goers Viewing Pleasure*, FORBES (Oct. 3, 2014, 11:32 AM), http://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure [perma.cc/MXV5-68P7].

160. Ben Smith, *Uber Executive Suggests Digging Up Dirt on Journalists*, BUZZFEED (Nov. 17, 2014, 6:57 PM), http://www.buzzfeed.com/bensmith/uber-executive-suggests-digging-up-dirt-on-journalists#.guwMYyV65 [perma.cc/RH8R-XFJE].

161. Calo, *Digital Market Manipulation*, *supra* note 75.

162. *Id.*

helps to explain why this should be the case, by better capturing the essence of the wrongdoing (here, as trust-destroying disloyalty).

More broadly, many of our deep-seeded fears about "big data," genetic information, and discrimination are at base fears about disloyalty.[163] After a recent public investigation of big data's discriminatory potential,[164] the FTC expressed its serious concerns about the use of big data analytics to unfairly exclude lower-income consumers.[165] Similar fears of digital "redlining" undergird the White House's study of big data.[166] Companies could use big data to exclude disadvantaged populations from the marketplace. Much of this exclusion could be justified as fair competition. However, the law should prohibit unreasonable self-dealing and regulate disloyal entrustees of information. This could be done through presumptions of trust created via tort law by expanding the breach of confidentiality tort or through regulatory mechanisms like a consumer privacy bill of rights or Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices. But regardless of how it is implemented, loyalty is essential to any theory of privacy that meaningfully safeguards trust.

V. CONCLUSION

We have thought about privacy in pessimistic and outdated terms for too long. Uses of personal information can certainly cause anxiety and stimulate feelings of creepiness, they can absolutely cause harm, and individual choice certainly will have an appropriate role to play in our digital future. But Privacy Pessimism is a limited and incomplete way of conceptualizing questions of personal information and new technologies. It looks only to the costs of privacy rules rather than their benefits, and in so doing blinkers our vision, preventing us from imagining ways in which privacy rules can create value rather than impose costs and inefficiencies.

Understanding privacy in terms of its ability to promote trust solves the problem of Privacy Pessimism. Information relationships have long been essential to our lives, and the growth of digital networked technologies has only deepened their importance. Our venerable information relationships with doctors, lawyers, and merchants recognized the importance of information rules, and how those rules could produce the trust necessary for the kinds of long-term relationships that served the interests of trusters, entrustees, and society as a whole. Yet these understandings were perhaps so obviously correct as to be implicit and rarely re-

---

163. Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

164. *See* FTC, *Big Data: A Tool for Inclusion or Exclusion?: Event Webpage*, FTC (Sept. 15, 2014), http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion [perma.cc/74CF-6DRF].

165. *Id.* ("For example, high-income consumers may receive offers for 'gold level' credit cards and low-income consumers may receive offers for subprime credit cards.").

166. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 46 (May 2014).

marked upon.

As we embark on the creation of new information relationships involving new entrustees and new kinds of personal information, we must ensure that the essential elements of social trust are built into them so that our new relationships can be as sustainable as our older ones. This observation is, we believe, the most important contribution this Article makes. Trust is necessary for a sustainable digital future, and trust-promoting privacy rules can create individual and social value. If trust becomes a major part of the privacy conversation; if we look beyond Privacy Pessimism towards a kind of Privacy Optimism that can guide social norms and legal rules, we believe that our intervention will have been a success.

THE PATHOLOGIES OF DIGITAL CONSENT

NEIL RICHARDS[*] AND WOODROW HARTZOG[**]

ABSTRACT

Consent permeates both our law and our lives—particularly in the digital context. Consent is the foundation of the relationships we have with search engines, social networks, commercial web sites, and any one of the dozens of other digitally mediated businesses we interact with regularly. We are frequently asked to consent to terms of service, privacy notices, the use of cookies, and so many other commercial practices. Consent is important, but it's possible to have too much of a good thing. As scholars have documented, while consent models permeate the digital consumer landscape, the practical conditions of these agreements fall far short of the gold standard of knowing and voluntary consent. Yet as scholars, advocates, and consumers, we lack a common vocabulary for talking about the different ways in which digital consents can be flawed.

This article offers four contributions to improve our understanding of consent in the digital world. First, we offer a conceptual vocabulary of "the pathologies of consent"—a framework for talking about different kinds of defects that consent models can suffer, including unwitting consent, coerced consent, and incapacitated consent. Second, we offer three conditions for when consent will be most valid in the digital context: when choice is infrequent, when the potential harms resulting from that choice are vivid and easy to imagine, and where we have the correct incentives choose consciously and seriously. The further we fall from these conditions, we argue, the more a particular consent will be pathological and thus suspect. Third, we argue that our theory of consent pathologies sheds light on the so-called "privacy paradox"—the notion that there is a gap between what consumers say about wanting privacy and what they actually do in practice. Understanding the "privacy paradox" in terms of consent pathologies shows how consumers are not hypocrites who say one thing but do another. On the contrary, the pathologies of consent reveal how consumers can be nudged and manipulated by powerful companies against their actual interests, and that this process is easier when consumer protection law falls

---

* Koch Distinguished Professor of Law & Director, Cordell Institute, Washington University.

** Professor of Law and Computer Science, Northeastern University. For helpful comments on prior drafts and discussions on this topic, we would both like to thank Scott Baker, Danielle Citron, Jon Heusel, Jonathan King, and Katie Shilton. We would particularly like to thank Ari Waldman for his partnership in the conference that led to this paper, to Rachel Mance for her outstanding work in planning and running the conference, and to Luis Fernandez and Siri Nelson for their excellent research assistance.

far from the gold standard. In light of these findings, we offer a fourth contribution—the theory of consumer trust we have suggested in prior work and which we further elaborate here as an alternative to an over-reliance on increasingly pathological models of consent.

INTRODUCTION

Consent permeates our law. It is one of its most powerful and most important building blocks. This should be no wonder. We live in a society that lionizes individual choice in the many social roles we play every day, whether as consumers, citizens, family members, voters, lovers, or employees. Consent reinforces fundamental cultural notions of autonomy and choice. It transforms the moral landscape between people and makes the otherwise impossible possible.[1] It is essential to the exercise (and waiver) of fundamental constitutional rights, and it is at the essence of political freedom, whether we are talking broadly about a "social contract" or making political choices for individual candidates and referenda in the voting booth.

Consider the substantial amount of legal work that consent performs. It is the basis of contracts, whether for goods, services, real estate, or marriage. The consent of the governed is the basis for the rule of law in democratic societies and was an important basis for the American Revolution. Consent can also work magic. When consent is present, trespassers can become dinner guests, a battery can become a welcome pat on the back, and even what would otherwise be a sexual assault can become an act of intimacy.[2]

Consent's power, its usefulness, and its resonance with norms of autonomy and choice make it an easy legal tool to reach for when we want to regulate behavior. Just as activities that have no harm might warrant lesser (or no) regulation, what consenting adults choose to do together takes that activity presumptively beyond the law's regulatory power. This is true whether the activity happens in the open or behind the proverbial closed doors. Consent's power is particularly justified in cases of what we might

---

1. For a more developed history of consent for data practices and contemplation of its role, see NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019); Elizabeth Edenberg & Meg Leta Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, 21 NEW MEDIA & SOC'Y 1804 (2019); Meg Leta Jones, *The Development of Consent to Computing*, 2019 IEEE ANNALS OF THE HISTORY OF COMPUTING (forthcoming).

2. Edenberg & Jones, *supra* note 1, at 1804–05 ("Valid consent can render permissible an otherwise impermissible action. It transforms the specific relations between the consenter and consentee about a clearly defined action. We can consent to sexual relations, borrowing a car, surgery, and the use of personal information. Without consent, the same actions can become sexual assault, theft, battery, and an invasion of privacy.").

call "gold standard" consent—agreements between parties who have equal bargaining power, significant resources, and who *knowingly* and *voluntarily* agree to assume contractual or other legal obligations.

Perhaps nowhere has consent been deployed more frequently as a legal concept than in the context of digital goods and services. Consent is the foundation of the relationships we have with search engines, social networks, commercial web sites, and any one of the dozens of other digitally mediated businesses we interact with regularly. We are frequently asked to consent to terms of service, privacy notices, the use of tracking cookies, and so many other commercial practices. But it's possible to have too much of a good thing. As we and other privacy law scholars have documented elsewhere, while consent models permeate the digital consumer landscape, the practical conditions of these agreements fall far short of the gold standard.[3] Think about your own agreements with the social networks you use, the apps you install on your phone, or the Amazon Alexa that might sit, listening, in your kitchen or bedroom. Do you know what you agreed to? Have you read the agreements? Did you have a meaningful choice? While the answer to these questions is usually "no," the dominant legal regime that applies in the United States is that the terms and conditions of these services are valid as long as there is some kind of "notice and choice" to consumers.[4] In practice, and as enforced with occasional exception by the Federal Trade Commission (FTC), notice-and-choice models can be legally sufficient even if the notice is buried somewhere in a dense privacy policy, and the choice is take-it-or-leave-it—accept what a company wants to do with your data or not use the service at all.[5]

---

3. *See, e.g.*, NANCY KIM, WRAP CONTRACTS (2013) [hereinafter KIM, WRAP CONTRACTS]; MARGARET RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L.J. 1180 (2017) [hereinafter Richards & Hartzog, *Privacy's Trust Gap*]; Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*]; Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1880 (2013); Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529 (2007); Scott Peppet, *Unraveling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future*, 105 NW. L. REV. 1153 (2011); Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85 (2014).

4. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS iii (2010); Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405 (2010) [hereinafter Hartzog, *The New Price to Play*].

5. *See, e.g.*, Richards & Hartzog, *Privacy's Trust Gap*, *supra* note 3, at 1198; Richards & Hartzog, *Taking Trust Seriously*, *supra* note 3, at 444.

While criticism of the over-use of consent in the consumer privacy context is rising, critics lack a shared vocabulary with which to discuss when consent is legitimate, when it is flawed, and how to talk about and distinguish those flaws.[6] Our lack of the right words and concepts with which to talk about defects in consent models runs into the rhetorical, cultural, and legal power of consent. As a consequence, consent criticism can fail to gain traction in the minds of those who are undecided or who have taken consent's powerful "consenting adults" rhetoric at face value. This results in a projection of gold standard norms onto the deficient digital landscape in ways that we want to suggest are *pathological*. In this article, we offer a conceptual framework for *thinking* about when consent is valid and when it has pathologies, and a conceptual vocabulary for *talking* about different kinds of pathologies that consent models can suffer. Our analysis is focused on the consumer privacy context, but we believe that our model and the vocabulary of the pathologies of consent can be useful in many of the other areas of the law in which consent is frequently applied.

Let us be clear about our claim: We are not arguing for a wholesale rejection of consent. A legal system without consent would be so radically different from what we have that it would be almost unimaginable. More fundamentally, we believe that consent should retain its prominent place in our law generally. Our argument is more nuanced. Consent is undeniably powerful, and often very attractive. But we have relied upon it too much, and deployed it in ways and in contexts to do more harm than good, and in ways that have masked the effects of largely unchecked (and sometimes unconscionable) power.[7] The gold standard of consent to data practices has been articulated throughout our law as being "knowing and voluntary."[8] European law uses an analogous method to require consent that is "freely given, specific, informed," and voluntary.[9] But this ideal can only exist

6. *See* Solove, *supra* note 3, at 1880–81; *see also* Edenberg & Jones, *supra* note 1, at 1810–14 (arguing in favor of locating the normative core of consent for data practices).

7. *See* Solove, *supra* note 3, at 1894.

8. *See infra* Part I.

9. For example, the EU's new General Data Protection Regulation (GDPR) embodies this concept by defining "consent" to require "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." Regulation 2016/679, art. 4(32), 2016 O.J. (L 119) 1, 34. Recital 32 of the GDPR explains further that "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement." Regulation 2016/679, pmbl. ¶ 32, 2016 O.J. (L 119) 1, 6.

under certain circumstances,[10] which is what we hope to illuminate in this essay. We argue that consent is most valid when we are asked to choose *infrequently*, when the potential harms that result from the consent are *easy to imagine*, and when we have the correct *incentives to consent* consciously and seriously. The further we fall from this gold standard, the more a particular consent is pathological and thus suspect.

Beyond the conceptual framework and vocabulary, we offer a third contribution to our understanding in this area. We believe that the theory of consent pathologies offered here complicates a seductive but simplistic story that has been offered in tech policy circles for over a decade. This is the notion of the "privacy paradox"—the idea that consumer anxiety about privacy is undermined by the fact that consumers act in privacy-diminishing ways in practice. Understanding this phenomenon in terms of consent pathologies reveals that consumers are not hypocrites who say one thing but do another that reveals their true preferences. On the contrary, the pathologies of consent show how consumers can be nudged and manipulated by powerful companies against their actual interests, and this phenomenon is easier when the legal regime that purports to protect consumers falls far from the gold standard. As a fourth contribution, we suggest that the solution is not to double down on our increasingly pathological models of consent, but to look to other mechanisms that are more sensitive to relationships and power differentials, such as those designed to inspire the social trust that makes consent less necessary.

Our argument has four parts. In Part I, "the Empire of Consent," we survey the many instances of consent in our law, illustrating both the varied work that consent performs and the varied tests for consent that courts and legislatures have produced. We show how different legal regimes produce different formulations on a continuum of how consent should be measured by the law, and how much consent is necessary in particular contexts. Toward the more restrictive end of the continuum, models of consent coalesce around the standard of "knowing and voluntary," for example in the relinquishment of a fundamental right such as the right to a jury trial. Yet in the digital context, the rhetorical practice of many technology companies is to talk like they are offering informed consent while offering something far inferior legal or practical matter.

---

10. *See* Edenberg & Jones, *supra* note 1, at 1805 ("Consent can be legally binding, as long as the transaction has met certain legal requirements or institutional standards defining the scope of consent. The legal notion of consent is built on the moral notion; however, problems arise when legally binding consent fails to capture the relevant morally legitimate transference of rights and obligations.").

The heart of our article is Part II, "the Pathologies of Consent," in which we offer a conceptual framework of the ways in which consent to data practices might fall short of the gold standard. We begin with a note on our methodology, adapted from the method by which the economist Richard Thaler developed a series of critiques of the dominant rational actor model in economics, thereby significantly contributing to the development of the field of behavioral economics.[11] We then offer three different sets of circumstances in which we suspect that consent may be less accurate, useful or legitimate. First, there is *unwitting consent*, which takes the "knowing" out of "knowing and voluntary." This can take at least three forms, including not understanding the legal agreement, not understanding the technology being agreed to, or not understanding the practical consequences or risks of agreement. Second, there is *coerced consent*, a consent that takes the "voluntary" out of "knowing and voluntary," for example in cases where a person is confronted with a choice between consent and the loss of an important asset such as their life or their job. Third, there is *incapacitated* consent, in which voluntariness is not available as a matter of law, such as with children and others who are categorically incapable of legally consenting.

In Part III, "Ideal Consent," we suggest a set of preconditions necessary for consent to achieve the ideal of being knowing and voluntary. Without these preconditions, we argue that consent models will not be particularly useful or legitimate. In fact, without these preconditions, consent models for data practices risk being harmful and corrosive to the very autonomy they seek to protect. First, the choice to be made must be *infrequent* (so as not to overload the capacity of our minds to make rational choices). Second, the *harms* which we might incur by granting consent must be *vivid* (i.e., they must be easy to imagine).[12] Third, the stakes of a decision to consent must be *significant* (i.e., there is ample incentive to take each decision seriously). Consent works well where these three criteria are satisfied. But where some or all of these criteria are not present, consent starts to lose both its usefulness and its very legitimacy. We call the presence of these three factors *gold standard consent*, and argue that it should be the benchmark against which the legal and ethical validity of consent are measured.

---

11. For Thaler's own description of his process, see RICHARD H. THALER, MISBEHAVING: THE MAKING OF BEHAVIORAL ECONOMICS (2016). For an application of this process in privacy law scholarship, see ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2010).

12. *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1027 (2013).

In Part IV, "Beyond Consent," we offer a roadmap for a world in which consent is cabined to the contexts in which it is most effective and most legitimate. As elsewhere in the paper, we use the example of the laws regulating consumer technologies powered by human information as our example. We argue that while consent will and should remain an important option in the legal toolbox, we should resist the easy but troublesome tendency of always going to consent in the first instance. In other words, we argue that consent should not be a common tool in modern data protection regimes. To use the parlance of Silicon Valley, consent does not scale. It is almost entirely incompatible with the modern realities of data and technology in all but the most limited of circumstances.

Instead, building on other work, we propose a privacy framework with a major focus on the concept of trust.[13] Trust-based protections would require parties in information relationships to protect the data placed in their care and to treat each other fairly and with deference. They would prohibit entrusted entities from asking for consent to practices that would make people unreasonably vulnerable. Lawmakers looking to embrace trust and minimize the pathologies of consent could leverage rules concerning the design of technologies and legal prohibitions on consent such as unconscionability to shift the policy conversation in a way that values both consent and privacy, and protects the millions and millions of human beings to whom these rules apply.

I. THE EMPIRE OF CONSENT

Consent flows through our legal system to such an extent that it would be almost impossible to imagine our law without it. Consent's importance in our law has been recognized for generations. Henry Sumner Maine famously observed in 1861 that "the movement of the progressive societies has hitherto been a movement *from Status to Contract*."[14] Maine's argument was that unlike the premodern societies characterized by social interactions structured by kinship and other forms of hierarchical ordering, modern societies were increasingly characterized by social interactions structured

13. *See generally* Richards & Hartzog, *Privacy's Trust Gap*, *supra* note 3; Richards & Hartzog, *Taking Trust Seriously*, *supra* note 3; ARI WALDMAN, PRIVACY AS TRUST (2018); Jack Balkin, *Information Fiduciaries and the First Amendment*, 46 U.C. DAVIS L. REV. 1183 (2016).

14. 1 HENRY MAINE, ANCIENT LAW 101 (J.H. Morgan ed., J.M. Dent & Sons 1917) (1861).

by contracts—private agreements whose chief hallmark was consent.[15] Consent thus became one of our basic social structures, and if we look for it, we can see it everywhere.

Let us take a moment to be precise about what we mean here. When we talk about "consent" in this article, we mean a legal relationship characterized in form or substance by agreement or a concurrence of wills.[16] In a moral sense, we mean to rely on Edenberg and Jones's definition of consent as "effective communication of an intentional transfer of rights and obligations between parties. Valid consent transforms the specific relation between the consenter and consentee about a clearly defined action."[17] In its strongest form, as Justice Story memorably put it in 1835, "[c]onsent is an act of reason, accompanied with deliberation, the mind weighing, as in a balance the good or evil on each side."[18] Yet as we will see below, the prevalence of consent in our law includes weaker forms, including presumed consent and even fictive consent. In this Part, we survey at a high level some of the ways in which Maine's observation about contractual ordering has proven correct by showing how our law can be viewed in a very real sense as an empire of consent.

Perhaps the easiest place to begin an appreciation of the role of consent in our law is the common law. As all lawyers are familiar, contract law's basic elements of offer and acceptance are predicated on the notion of consent. Contractual consent is objective, meaning it does not matter what you actually thought you were consenting to, only what you objectively manifested consent to.[19] Contract law also allows consent to alternative dispute resolution, via arbitration or mediation clauses, at least when such contracts are not adhesionary, and there is bargaining power between the contracting parties.[20]

Property law's hallmark is the right of alienation—the voluntary right to agree to transfer one's property, real or personal—to another.[21] This

---

15. Katharina Isabel Schmidt, *Henry Maine's "Modern Law": From Status to Contract and Back Again?*, 65 AM. J. COMP. L. 145, 154 (2017).

16. *Cf. Consent*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("A voluntary yielding to what another proposes or desires; agreement, approval, or permission regarding some act or purpose, esp. given voluntarily by a competent person; legally effective assent.").

17. Edenberg & Jones, *supra* note 1, at 1811.

18. 1 JOSEPH STORY, COMMENTARIES ON EQUITY JURISPRUDENCE § 222 (1835).

19. Hartzog, *The New Price to Play*, *supra* note 4.

20. *E.g.*, Sutton's Steel & Supply, Inc. v. Bellsouth Mobility, Inc., 776 So. 2d 589, 597 (La. Ct. App. 2000).

21. Thomas W. Merrill, *The Property Strategy*, 160 U. PA. L. REV. 2061, 2079 (2012).

principle runs throughout the law of property, but it is easiest to appreciate in the rules governing gifts, which require donative intent (a donor voluntarily intending (i.e., consenting) to give a gift to the donee), delivery (physical transfer of the gift to the donee), and acceptance (consent to the gift by the donee).[22] Similarly, consent allows exceptions to the right to exclude, whether by turning a trespasser into a dinner guest, or by allowing the creation of licenses, easements, and bailments.

Consent is less central in tort law, which imposes duties that flow to the general population or some subset thereof, like in the case of the duty to exercise reasonable care. But consent remains important, for it can work to assume the risks of someone else's actions. Thus, if you are my karate instructor, and you negligently (or even recklessly) injure me, I might be unable to recover if I sue you because I assumed the risk of engaging in the dangerous sport and consented to spar with you in the first place.[23] Or if you go to watch the Boston Red Sox and are injured by a foul ball, the Red Sox will probably be immune from suit because you are presumed to have accepted the risk of injury by consenting to watch them play at Fenway Park (or wherever).[24]

With respect to intentional torts like assault, battery, conversion, and trespass, consent is typically treated as an affirmative defense.[25] Consider a surgical procedure, which would be a legal battery without consent, and even where some consent is supplied can become a battery again when consent is exceeded.[26] Consider further the important role consent plays in the complex of "privacy torts," the subset of intentional torts dealing with the collection, dissemination, and use of sensitive personal information. The four torts recognized by William Prosser[27]—intrusion into seclusion, disclosure of private facts, false light publicity, and appropriation of likeness—are all negated by consent to the invasion of privacy.[28] Thus, for example, it violates the intrusion tort when a surgeon photographs a patient during cosmetic breast surgery, and the patient's consent form does not

22. Guardian State Bank & Tr. Co. v. Jacobson, 369 N.W.2d 80, 83–84 (Neb. 1985).
23. *E.g.*, Levine v. Gross, 704 N.E.2d 262, 263 (Ohio Ct. App. 1997).
24. Costa v. Boston Red Sox Baseball Club, 809 N.E.2d 1090 (Mass. App. Ct. 2004).
25. *Consent*, BLACK'S LAW DICTIONARY, *supra* note 16.
26. *E.g.*, Kaplan v. Mamelak, 75 Cal. Rptr. 3d 861 (Cal. Ct. App. 2008).
27. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960). For additional background about the privacy torts and Prosser's role in their creation, see G. EDWARD WHITE, TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY 176–179 (expanded ed. 2003); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).
28. RESTATEMENT (SECOND) OF TORTS § 652A(2) (1977).

cover such uses of the photographs.[29] Consent to have your image used for commercial purposes is also a defense to an action for appropriation of likeness for commercial gain.[30] Of course, there are more intentional torts governing the collection, use, and disclosure of information than the four recognized by Prosser. A full "expanded set" of privacy torts includes trespass, breach of confidence, defamation, and intentional infliction of emotional distress.[31] Yet even this broader group of torts can be negated by defense—a trespasser with permission becomes a licensee or even a guest,[32] permission to disclose eliminates a duty of confidentiality,[33] and you can permit (or pay) someone to say mean or false things about you. In all of these cases, if you consent, you cannot sue.

Beyond contracts, property, and tort, consent also plays an important role in the law regulating family and sexual relations. For over a century, courts have recognized that "[t]he fundamental principle of all marriage is mutual consent."[34] This principle was echoed in *Obergefell v. Hodges*, when the Supreme Court held that the Fourteenth Amendment protects the right of marital choice, a concept that runs throughout its analysis.[35] The foundation of the Court's analysis is thus its statement that the Fourteenth Amendment's liberty guarantee "extend[s] to certain personal choices central to individual dignity and autonomy, including intimate choices that define personal identity and beliefs."[36] The Court concluded that "[u]nder the Constitution, same-sex couples seek in marriage the same legal treatment as opposite-sex couples, and it would disparage their choices and diminish their personhood to deny them this right."[37] Consent runs broadly throughout the rest of family law as well; it can be the difference between a loving sexual act and sexual assault or rape. The age at which it becomes legal to engage in sexual activity is of course known as the "age of

29. Judge v. Saltz Plastic Surgery, 330 P.3d 126 (Utah Ct. App. 2014).

30. RESTATEMENT (SECOND) OF TORTS § 652C (1977).

31. NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES FOR THE DIGITAL AGE 158 (2015).

32. *E.g.*, State v. Pixley, 200 A.3d 174, 177 (Vt. 2018) (explaining that trespass requires a person to enter the land without legal authority or consent).

33. *E.g.*, Grimminger v. Maitra, 887 A.2d 276, 279 (Sup. Ct. Pa. 2005) (patient consent serves as an affirmative defense to a claim of a breach of physician-patient confidentiality).

34. *Recent Cases: Marriage — Validity — Common-Law Marriage — Mistake as to Existence of Prior Marriage Between the Parties*, 34 HARV. L. REV. 561, 561 (1921) (summarizing the holding of Great N. Ry. Co. v. Johnson, 254 F. 683 (8th Cir. 1918)).

35. 135 S. Ct. 2584, 2605 (2015).

36. *Id.* at 2597.

37. *Id.* at 2602.

consent."[38] Consent is also the key feature in the legality of some sexual activities in BDSM[39] and is also an issue when elderly married couples engage in sexual activity when one partner has lost the capacity to legally consent.[40]

Beyond the common law, consent also plays a critical role in the context of digital privacy regulation. In the United States, the dominant regime of privacy regulation is known as "notice and choice." As interpreted by the Federal Trade Commission under its Unfair and Deceptive Trade Practices authority, this has meant that consumers are presumed to have consented to data practices as long as there has been some kind of "notice" to the consumer about what is happening and some kind of "choice" about whether they want it to happen. A recent FTC report on company surveillance of consumers across digital devices (for example tracking laptop web browsing activity to deliver targeted ads to the same consumer on a cell phone) is illustrative of the FTC's approach:

> As with traditional forms of tracking, companies should offer consumers choices about how their cross-device activity is tracked. And, when companies offer such choices, the FTC Act requires that the companies respect them. To the extent opt-out tools are provided, any material limitations on how they apply or are implemented with respect to cross-device tracking must be clearly and conspicuously disclosed.[41]

In practice, however, such requirements are relatively easy to comply with, as all a company needs to do to avoid FTC liability for unfair or deceptive trade practices if challenged is show that their use of consent is neither deceptive nor unfair.[42] Thus "notice" can mean a vague but not false description of data practices buried deep within a long privacy policy and "choice" can mean no more than the choice to use the service in the first place (Apple, Android, or no phone at all, for example).[43] It is perhaps for

---

38. *E.g.*, State v. Holloway, 916 N.W.2d 338, 345 (Minn. 2018) ("What has been known as statutory rape—sexual conduct with a person not of the age of consent—has been a crime in Minnesota since it was first organized as a territory.").

39. *See* William Eskridge, *The Many Faces of Sexual Consent*, 37 WM. & MARY L. REV. 47, 49–50 (1995); Margo Kaplan, *Sex-Positive Law*, 89 N.Y.U. L. REV. 89, 117 (2014).

40. Alexander Boni-Saenz, *Sexual Advance Directives*, 68 ALA. L. REV. 1, 3–4 (2016).

41. FED. TRADE COMM'N, CROSS-DEVICE TRACKING: AN FTC REPORT 13 (Jan. 2017).

42. *Cf.* 15 U.S.C. § 45(a)(1) (prohibiting the use of "unfair" or "deceptive" trade practices in or affecting interstate commerce).

43. WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 58–72 (2017) [hereinafter HARTZOG, PRIVACY'S BLUEPRINT].

this reason that when Facebook CEO Mark Zuckerberg testified before Congress in response to a series of privacy scandals involving his company, his defense, first and foremost, was that Facebook puts its users in "control,"[44] a good sound bite, but one that can be all but meaningless as a legal requirement.

Consent within Europe's data protection frameworks is more rigorous than in parts of US privacy law. Indeed, unlike US law, the European Union (EU) treats privacy and the related but distinct concept of data protection as fundamental rights. Consent remains central to this fundamental rights-based approach, although Europe's modern data protection regime is skeptical of over-relying on the notion.[45] Recital Seven of the EU General Data Protection Regulation (GDPR explicitly states that "Natural persons should have control of their own personal data."[46] This control is effectuated significantly through the mechanism of "informed consent" as a basis for legitimizing data processing.[47] Beyond the GDPR, the reasoning behind the

---

44. Written Testimony from Facebook to House Energy and Commerce Committee for Record of April 11, 2018 Hearing (June 29, 2018), https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf [https://perma.cc/B7LR-L7XU] (note: the word 'control' is mentioned over 1,000 times). It goes on like this for a while. *See also* Dan Fletcher, *How Facebook is Redefining Privacy*, TIME (May 20, 2010), http://content.time.com/time/magazine/article/0,9171,1990798-4,00.html [https://perma.cc/D66L-4FG3] ("'The way that people think about privacy is changing a bit . . . . What people want isn't complete privacy. It isn't that they want secrecy. It's that they want control over what they share and what they don't.'"); Anita Balakrishnan, Matt Hunter & Sara Salinas, *Mark Zuckerberg Has Been Talking About Privacy for 15 Years—Here's Almost Everything He's Said*, CNBC (Apr. 9, 2018), https://www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html [https://perma.cc/Q4QM-JGFA] ("'When I built the first version of Facebook, almost nobody I knew wanted a public page on the internet. That seemed scary. But as long as they could make their page private, they felt safe sharing with their friends online. Control was key.'"); Emily Stewart, *The Privacy Question Mark Zuckerberg Kept Dodging*, VOX (Apr. 11, 2018), https://www.vox.com/policy-and-politics/2018/4/11/17225518/mark-zuckerberg-testimony-facebook-privacy-settings-sharing [https://perma.cc/DQ84-Q2GD] ("'Every time that a person chooses to share something on Facebook, they're proactively going to the service and choosing that they want to share a photo, write a message to someone, and every time, there is a control right there, not buried in settings somewhere but right there when they're posting, about who they're sharing with.'").

45. *See* Edenberg & Jones, *supra* note 1; *see also* Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is And What It Means*, 28 INFO. & COMM. TECH. L. 65, 68 (2019) ("[T]he GDPR is constitutionally skeptical of U.S. lawyers' favorite tool: consent, particularly of the low-quality or 'take it or leave it' variety. The GDPR's architects realized that if low-voluntariness consent could justify data activities, the GDPR would just become another exercise in clicking 'I agree' to unread, unnegotiable terms. The GDPR requires high-quality consent, on par with important life decisions, such as consent to medical treatment. In many contexts, the burdens the GDPR places on consent make consent impossible as mechanism to make data uses legal. Moreover, many rules in the GDPR are not waivable and continue to apply after somebody has consented to data use.").

46. Regulation 2016/679, pmbl. ¶ 7, 2016 O.J. (L 119) 1, 2.

47. Regulation 2016/679, art. 7, 2016 O.J. (L 119) 1, 37.

EU ePrivacy Directive is that it "enhances end-user's control by clarifying that consent can be expressed through appropriate technical settings."[48] But as we will discuss in the Parts that follow, hard-coding consent through legal or technical code is fraught at best. It also probably makes things worse because it offers an illusion of control that dulls impetus for meaningful change while entrenching the pathologies of the concept into the very design of information technologies.[49]

American constitutional law does not recognize a broad constitutional right to privacy the way the EU does. But when constitutional rights are at issue in privacy or elsewhere, U.S. law (like the EU) puts consent at the core of rights jurisprudence. Indeed, consent is at the very core of American constitutionalism. Consider these familiar founding words from the beginning of the Declaration of Independence: "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.—That to secure these rights, Governments are instituted among Men, deriving their just powers *from the consent of the governed*."[50]

Consent's importance runs throughout constitutional law, particularly with respect to the doctrine of waiver. Constitutional rights can be waived, and waiver is essentially the consent to give up that right. When it comes to waiver, however, the Supreme Court has made clear that consent to waiver must be clearly and freely given. Sometimes this is textual, such as where the Third Amendment expressly includes consent as a defense to the quartering of soldiers in private homes: "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[51] More significantly, numerous constitutional rights can only be waived where there is a showing that such waivers are *knowing*, *intelligent*, and *voluntary*. This is the case,

---

48. *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC*, at 3.4, COM (2017) 10 final (Jan. 10, 2017).

49. *See, e.g.*, HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 43; Lee Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, 4 OSLO L. REV. 105 (2017); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROTECT. L. REV. 423 (2018), https://edpl.lexxion.eu/article/edpl/2018/4/5/display/html [https://perma.cc/T4LA-HNE8] [hereinafter Hartzog, *The Case Against Idealising Control*].

50. THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776) (emphasis added).

51. U.S. CONST. amend. III.

for example, for both the right to counsel[52] and the right to trial by jury.[53] Many constitutional rights can also be contracted around. For example, the First Amendment permits non-disclosure agreements—contracts not to speak—such as where journalists agree with confidential sources not to disclose their names in exchange for a story.[54] The Supreme Court has held that such contracts are enforceable against the press consistent with the First Amendment even where the identity of the source is itself newsworthy.[55]

Consent is also a critical element of health law. Reflecting the importance of the human interests involved, rules for consent in the health context are strict in ways resembling constitutional law, often requiring a heightened form of consent known as "informed consent." One of the foundations of modern biomedical ethics is the Belmont Report, a product of the National Research Act of 1974, which established a commission to study the basic ethical principles that should undergird biomedical and behavioral research involving human subjects.[56] The Belmont report announced three "Basic Ethical Principles" of "respect for persons," "beneficence," and "justice," and it offered three "applications" of these principles, the first of which was "informed consent."[57] The Belmont Report's definition of informed consent states "[r]espect for persons requires that subjects, to the degree that they are capable, be given the opportunity to choose what shall or shall not happen to them."[58] In practice, the Report urged that subjects be given the relevant *information* on which to make their decision, that researchers ensure that test subjects have *comprehension* of the information surrounding their decision, and that decisions be made in accordance with the idea of *voluntariness*.

The Belmont Report has been tremendously influential in the field of biomedical ethics, and today its recommendations are reflected in the Common Rule, the ethical rule that governs U.S. government funded biomedical and behavioral research. The Common Rule prescribes detailed

52. Davis v. United States, 512 U.S. 452, 458 (1994).
53. Adams v. United States ex rel. McCann, 317 U.S. 269, 275 (1942).
54. Cohen v. Cowles Media, 501 U.S. 663, 669–70 (1991).
55. *Id. See generally* Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650 (2009).
56. The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, 44 Fed. Reg. 23,192 (Apr. 18, 1979).
57. *Id.* at 23,193.
58. *Id.* at 23,195.

substantive and documentary requirements for "informed consent."[59] There are extensive professional and academic literatures on informed consent in a variety of medical contexts reflecting substantial work and reflection. One classic treatise, for example, identifies five critical elements for truly informed consent—disclosure; comprehension or understanding; voluntariness; decision-making capacity or competence; and authorization.[60]

The "knowing and voluntary" waiver standard from constitutional law and the informed consent standard from biomedical ethics each represent a kind of what we might think of as a "gold standard" consent. One could add another such example from the commercial context—freely negotiated agreements between sophisticated parties who have equal bargaining power, significant resources, and who knowingly and voluntary agree to assume contractual or other legal obligations. These are the models from which consent derives its strength—decisions to engage in activity based upon full information and free, voluntary, and informed choice. They are consent in its strongest and most legitimate form.

Let's take a step back at this point and look at the forest rather than the trees. Our review of consent models in the law can be distilled into three important principles. First, consent requirements are prevalent in many—if not most—areas of American law, running throughout common law, constitutional law, and regulatory law. Second, consent models vary in how strictly they protect consenting individuals, from the stringent consent requirements in constitutional law and health and human subjects research all the way down to the opt-out consents in commercial transactions that are so common in the digital environment. Third, despite this variance, there does exist a "gold standard" of consent, which is stringent and highly protective of individuals, whether we call it "informed consent," "knowing and voluntary" agreement or waiver, or something else entirely. We would suggest that in spite of consent's variance in practice, it is this gold standard of consent that policymakers, advocates, and others refer to when they talk about consent. Indeed, even Facebook's public statements about "control" in the abstract evoke a much stronger notion of consent than the watered-down legal requirements under which the company operates in practice (at least in the United States). When companies like Facebook negotiate

59. *See* Common Rule, 45 C.F.R. §§ 46.116 (general requirements for informed consent), 46.117 (documentation requirements for informed consent).

60. RUTH R. FADEN & TOM L. BEAUCHAMP, A HISTORY AND THEORY OF INFORMED CONSENT 274 (1986); *see also* Natalie Ram, *Tiered Consent and the Tyranny of Choice*, 48 JURIMETRICS 253, 259–60 (2008).

acquisitions or commercial deals with other companies, they typically enjoy (for themselves) gold standard consent informed by the finest lawyers money can buy. Yet when their individual human customers agree to use their services, it is fair to say that the level of information and power available to those individual humans is some distance away from the gold standard. It is to this gap between the gold standard of consent companies enjoy and the weaker kinds of consent many consumers "enjoy" in the digital environment that we will now turn.

II. THREE PATHOLOGIES OF CONSENT

When he was a young academic, the American economist Richard Thaler kept a list of ways in which people consistently acted irrationally. Thaler's list was not merely a lark by a bored iconoclastic graduate student. His list documented a series of human behaviors that the dominant theory of economics, the rational actor theory, failed to adequately explain. Again and again, Thaler kept encountering observable patterns of human behavior that were squarely at odds with the foundational assumption of economics that human beings act rationally to maximize their utility.

Thaler's list became a research agenda, as he and others began experimental studies of the behaviors he had observed. This community of scholars kept working, and these critiques of the dominant rational actor model helped to create the field of behavioral economics.[61] This field proceeds from the evidence that human beings do not always behave as the rational actor model assumes that they would—Thaler refers to these fictional humans as "econs." Instead, the field assumes that people behave in an observable and empirically-demonstrable way like "humans": sometimes acting rationally, sometimes less than fully rationally, and sometimes irrationally. Behavioral economists, building on the work of Thaler and his mentors Daniel Kahneman and Amos Tversky, attribute these behaviors to cognitive structures—and limitations—in the human brain.[62] They argue that humans, in the words of another leading scholar in the field, are not merely irrational, but predictably so.[63] Kahneman offers helpful metaphor for understanding how the human mind works. Most of the time, we operate using "System One," an automatic system of cognition that relies upon heuristics and assumptions to help us navigate the world.

61. *See generally* THALER, *supra* note 11.

62. *See* DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2011); Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124 (1974).

63. *See* DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS (2008).

Other times, when we encounter something new or really want to think something through, we use what Kahneman calls "System Two." System Two is more analytical and rational, but it is also lazy and relies as much as it can on System One because "thinking slow" is taxing on our energies and on the sugar reserves in our brain. System One allows us to drive to work while what we think of as our mind ("System Two") is occupied by the news. System One allows us to carefully read a law review article, even though we might derive more pleasure when we breeze through a novel (or a Netflix stream) using System Two.[64]

In this Part, we adapt Thaler's list methodology to privacy law—specifically to three scenarios we have observed in which consumers in the digital environment "consent" to data practices in ways that seem irrational. We offer these cases as "Pathologies of Consent" and conclude that sometimes the behavior can be explained by defects in the law, especially where the law requires less than "gold standard" consent, whereas other times the behavior may be explained by particular features of human cognition. Nevertheless, like Thaler's list, our suggestions are theoretical. To the extent we make empirical claims, such claims are primarily anecdotal rather than (at present) proven by experimental social science. In this respect, we follow a similar privacy law methodology to the one used by Anita Allen in her classic work *Unpopular Privacy*.[65]

Thaler's list complicated a relatively simplistic story that the rational actor model told about human behavior. We believe that our list of consent pathologies complicates a more specific (but equally simplistic) rational actor story that has circulated in privacy circles for a number of years as the "privacy paradox." The "privacy paradox" is the assertion that although people might express a concern for privacy in the abstract, their actual behavior suggests that they do not actually care about their privacy in practice. Observers coming from a rational actor perspective suggest that the actions of consumers (what an economist would call their *revealed preferences*) indicate that consumers do not really care about privacy at all, and that concerns about privacy in the consumer context are overblown.[66] To return to Mark Zuckerberg's testimony before Congress, if Facebook puts consumers in *control* of their privacy, but consumers continue to consent to privacy-revealing practices and act in privacy-destructive ways, they have no one to blame but themselves. Buyers beware.

---

64. KAHNEMAN, *supra* note 62, at 20–24.

65. *See* ALLEN, *supra* note 11.

66. *E.g.*, Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, 41 J. CONSUMER AFF. 100 (2007).

We believe that the three pathologies we offer in this Part complicate this simplistic and self-serving story, and we explain why consumers might understandably care about their privacy *and* agree to data practices that undermine their privacy and expose them to the risks of informational harms. (We also note that scholars working in the Thaler tradition have already begun the process of experimental testing of the ways in which consumers understand privacy in practice, with initial findings that confirm the intuitive and theoretical model we offer here.)[67]

There are certainly more than three ways in which consent in practice can deviate from gold standard consent, but for present purposes the three we offer here will suffice. They are *unwitting consent*, *coerced consent*, and *incapacitated consent*.

A. Unwitting Consent

Let's say that you are signing up for a new account with a tech company whose app or web site will let you do something. Perhaps you are signing up for a loyalty club at your local coffee or bagel shop, perhaps you are signing up for a new taxi app, dating app, or social network, or perhaps your iPhone or Android needs a security update that you fear will lead to a data breach if you don't agree. Like most consumers, you're in a hurry. (In the bagel example, maybe the people queuing behind you want to buy their bagels,[68] or maybe you are just hungry and want to finish the transaction so you can eat.) In any event, most consumer transactions these days have an informational component—the social network you join, the bagel app you download, the web sites you read, or the car you buy. The problem is, most consumers don't know what data practices are possible, what they have agreed to, or what the informational risks of the transaction are.

This is the problem of *unwitting consent*. In the complex technological and legal landscape in which the contemporary digital consumer finds herself, understanding what is going on can be challenging. Yet people are harried, busy, and distracted, so they understandably click the "I agree" button and move on with their day, hoping that all will be well. This is

---

67. For excellent reviews of the theoretical and empirical research in this field, see Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442 (2016); Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015).

68. In full disclosure, this is exactly what happened to one of the authors of this article recently, at an Einstein Brother's Bagels. The friendly clerk urged him to install the loyalty app at the point of sale, while the hungry customers behind him pressured him into clicking "I agree."

unwitting consent. Unwitting consent takes the "knowing" out of "knowing and voluntary." Simply put, far too often, far too many people in the digital environment have little to no idea about what data practices or exposure that they are consenting to. Compounding this problem (and enabling business practices that create and prey upon unwitting consent) is the conclusion reached by several courts that privacy policies, standing alone, are simply not enforceable as contracts.[69] At the same time, privacy policies that are incorporated into the terms of use that people consent to by clicking "I agree" are generally recognized as part of a binding contractual agreement.[70]

In fact, one of the reasons consent is such a poor fit for data practices is that boilerplate contract law is largely agnostic to whether people actually know what they are agreeing to. This is known as the objective theory of contracts. Under this theory, the intent of the parties, for example, 'I thought I was agreeing to "X," is irrelevant. Instead, the contract is formed based on what a reasonable person would have been led to believe in the relevant context (an objective standard).[71] Although this doctrine is criticized by many as it applies to boilerplate contracts,[72] generally parties need not have a "meeting of the minds" in the classic contractual sense. Rather, a "reasonable communication" of the terms will suffice.[73] In data processing contexts with lengthy terms of use agreements, this dynamic puts all of the risk on the user, because consent can be effective even if you have no idea what you just agreed to. Once again, buyer beware.

Unwitting consent can take several forms. First, *consumers can fail to understand the legal agreement* governing the information relationship they now have with the company. This can happen when the legal agreement is

---

69. *In re* Nw. Airlines Privacy Litig., No. 04-126, 2004 WL 1278459, at *16–18 (D. Minn. 2004); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 316–18 (E.D.N.Y. 2005).

70. Hartzog, *The New Price to Play*, *supra* note 4, at 408; Woodrow Hartzog, *Website Design As Contract*, 60 AM. U. L. REV. 1635, 1635 (2011) ("When courts seek to determine a website user's privacy expectations and the website's promises to that user, they almost invariably look to the terms of use agreement or to the privacy policy.").

71. Hartzog, *The New Price to Play*, *supra* note 4, at 416; *see also* Wickberg v. Lyft, No. 18-12094-RGS, 2018 U.S. Dist. LEXIS 213281 (D. Mass. Dec. 19, 2018)

72. *See* KIM, WRAP CONTRACTS, *supra* note 3; RADIN, *supra* note 3; Hartzog, *The New Price to Play*, *supra* note 4.

73. *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 429 (2d Cir. 2004); Molnar v. 1-800-Flowers.com, No. 08-cv-0542, 2008 WL 4772125, at *7 (C.D. Cal. Sept. 29, 2008) (stating that "courts have held that a party's use of a website may be sufficient to give rise to an inference of assent to the terms of use contained therein"); Southwest Airlines Co. v. Boardfirst, LLC, No. 3:06-cv-0891, 2007 U.S. Dist. LEXIS 96230, at *5 (N.D. Tex. Sept. 12, 2007); Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974, 982 (E.D. Cal. 2000) (stating that "the browser wrap license agreement may be arguably valid and enforceable").

too long (such as Apple's notoriously lengthy Terms of Services Agreement),[74] the legal agreement uses confusing language, structure, and syntax (such as when consent forms deploy double and triple negatives or switch from "opt out" to "opt in" options in a series of choices),[75] the legal agreement is too technical for ordinary readers to understand (many privacy policies reference technologies like pixel tags and MAC addresses, which are likely foreign concepts to the average user),[76] or the legal agreement is too vague to specify exactly what is being agreed to (consider Amazon's notoriously vague "Privacy Notice" which features terms like "we share your information with third parties, to permit them to send you marketing communications."). [77]

A second dimension of unwitting consent is where *consumers do not understand the technology* that mediates their relationship with the company. For example, most people don't realize that telecommunications

---

74. Apple's iOS Terms of Service (TOS) is notoriously long. Its current version, for iOS12, is 6,901 words long. *iOS Software Agreement*, APPLE, https://www.apple.com/legal/sla/docs/iOS12.pdf [https:// perma.cc/VC8B-8V48]. However, Apple's web site also contains thirteen other TOS agreements for iOS 3.1, 4.1, 5.0, 5.1, 6.0, 7.0, 8.0, 8.1, 9.0, 9.1, 10, 11, and 11.2. In 2017, cartoonist R. Sikoroyak turned the related Apple iTunes TOS agreement into a 96-page comic book starring Steve Jobs as its hero and featuring classic comic book styles and characters from The Simpsons to Snoopy to Family Circus. *See* Bonnie Burton, *Steve Jobs, Superhero: Graphic Novel Meets iTunes Service Terms*, CNET (Mar. 8, 2017), https://www.cnet.com/news/itunes-terms-of-service-graphic-novel-comic-r-sikoroyak/ [http://perma.cc /DC88-8PS5].

75. Consider this example from a request by a California school system regarding student directory information:

4. Decline Release of Directory Information **(Note: most parents do not choose this option)**

Decline Release of Directory Information	
I **do not** want the District to release "directory information" (see Packet for examples) to qualified individuals or groups, such as official parent-teacher organizations, college recruiters, Oakland Education Fund, or employers.	
Student's Name	
Parent/Guardian's Signature	

HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 43, at 145. Or this confusing series of choices from "opt out" to "opt in":

☐ Please do not send me details of products and offers from Currys.co.uk

☐ Please send me details of products and offers from third party organisations recommended by Currys.co.uk

Trick Questions, DARK PATTERNS, https://darkpatterns.org/types-of-dark-pattern/trick-questions [https://perma.cc/7R7F-6FYD].

76. *Privacy Policy,* THE STREET, INC., http://corporate.thestreet.com/privacy [https://perma.cc/3WS9-RMT3].

77. *Amazon.com Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 [https://perma.cc/2AE4-B4L7].

systems are remarkably insecure.[78] We give consent to these companies upon the assumption that their systems will protect us, but we are often mistaken about how those systems are configured. A prominent recent example is the scandal over Facebook's user interface that allowed for the exfiltration of massive amounts of data to Cambridge Analytica, the data firm accused of, among other things, dubious data practices with respect to electoral politics.[79]

Technically, Facebook users "consented" to the collection and sharing of this data via their privacy settings.[80] Facebook went to great lengths to emphasize this fact, stating "Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information."[81] But a closer look reveals that this consent was basically manufactured through obfuscation, abstraction, and sleight of hand via a user interface. Users likely had little idea what they were agreeing to, in no small part because the way the technology actually worked was opaque to users.

Professor Ian Bogost, who also had an application using the same interface as that at issue in the Cambridge Analytica scandal, wrote of Facebook's system:

> App authorizations are not exceptionally clear. For one thing, the user must accept the app's request to share data with it as soon as they open it for the first time, even before knowing what the app does or why. For another, the authorization is presented by Facebook, not by the third party, making it seem official, safe, and even endorsed.[82]

---

78. Sarah Jamie Lewis (@SarahJamieLewis), TWITTER (Jan. 8, 2019, 10:34 PM), https://twitter.com/SarahJamieLewis/status/1082888359008120832 [https://perma.cc/U632-3P5F]; Joseph Cox, *Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911 Calls,* VICE, (Feb. 6, 2019), https://motherboard.vice.com/en_us/article/a3b3dg/big-telecom-sold-customer-gps-data-911-calls [https://perma.cc/DDH8-HEMH].

79. *See, e.g.*, *The Cambridge Analytical Files,* GUARDIAN, https://www.theguardian.com/news/series/cambridge-analytica-files [https://perma.cc/TL6P-PA3Y].

80. Ian Bogost, *My Cow Game Extracted Your Facebook Data,* ATLANTIC (Mar. 22, 2018), https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214/ [https://perma.cc/CN2R-9LD4].

81. Paul Grewal, *Suspending Cambridge Analytica and SCL Group from Facebook*, FACEBOOK: NEWSROOM (Mar. 17, 2018), https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytic a/ [https://perma.cc/76FD-7MUR].

82. Bogost, *supra* note 80.

Bogost was critical of Facebook's flimsy consent structure, explaining that "[t]he part of the Facebook website where apps appear, under the blue top navigation (as seen above), introduces further confusion. To the average web user, especially a decade ago, it looked like the game or app was just a part of Facebook itself."[83] Bogost noted the seamless nature of the website that lacked a clear boundary between Facebook's navigation and the third-party app. He explained that "[i]f you look at the browser address bar while using a Facebook app on the website, the URL begins with "apps.facebook.com," further cementing the impression that the user was safely ensconced in the comforting, blue cradle of Facebook's care.[84]

Of course, that impression bore little relationship to reality. When people opened a third-party app, Facebook's servers passed along a request to the server where the app developer hosts their services. Then, the app sent all of its responses back to Facebook, which formatted the responses as if they were coming from Facebook rather than the third party.[85] Through this setup, the third-party app was able to access significant amounts of personal and potentially sensitive information.[86]

As the previous description suggests, consumer are unlikely to understand the complexities of layered applications and their correlated, opaque, data flows. We certainly are no experts. Lacking such knowledge, the "consent" requested by Facebook in this manner seems farcical. Bogost accused Facebook of "presenting apps as quasi-endorsed extensions of its core service to users who couldn't have been expected to know better."[87] The reason people felt so violated by Facebook could be that "they might never have realized that they were even using foreign, non-Facebook applications in the first place, let alone ones that were siphoning off and selling their data. The website always just looked like Facebook."[88]

Another prominent example of unwitting consent involves third party tracking through the use of advertising technology, or "ad tech," as it is

83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.* (describing that as an app developer using Facebook's interface "I was able to access two potentially sensitive pieces of data without even trying. The first is a player's Facebook ID. . . . Those data could be correlated against other information—data collected from Facebook, fashioned by the app, or acquired elsewhere. . . . The second type of information is a piece of profile data [my app] received without asking for it. Back in 2010, Facebook still allowed users to join "networks" —affiliations like schools, workplaces, and organizations. In some cases, those affiliations required authorization, for example having an email address at a domain that corresponds with a university.").
87. *Id.*
88. *Id.*

known in the industry. Ad tech involves technologies like ad networks, which serve "as a broker between a group of publishers and a group of advertisers,"[89] and ad servers, which are "used by ad networks, publishers, advertisers, and ad agencies to manage, run, and report on their advertising campaigns."[90] These networks and technologies are remarkably complex, with auctions conducted in milliseconds and involve a bevy of different companies processing your data to serve ads personalized on the basis of that data.[91] Even advocates of consent regimes realize how daunting this problem is, conjuring up euphemisms like "consent strings" for ad tech to simplify and streamline compliance.[92]

In January 2017, the FTC released a staff report on the problem of cross-device tracking, the practice discussed above in which "platforms, publishers, and ad tech companies try to connect a consumer's activity across her smartphones, tablets, desktop computers, and other connected devices. The goal of cross-device tracking is to enable companies to link a consumer's behavior across her devices."[93] The FTC's proposed solutions to this problem, however, were underwhelming. It recommended merely that "companies engaged in cross-device tracking: (1) be transparent about their data collection and use practices; (2) provide choice mechanisms that give consumers control over their data; (3) provide heightened protections for sensitive information, including health, financial, and children's information; and (4) maintain reasonable security of collected data."[94] Consistent with much of American privacy law, this amounted to notice, choice, heightened notice and choice for a few sensitive areas, and data security.

---

89. Maciej Zawadziński, *What is an Ad Network and How Does It Work?*, CLEARCODE (Mar. 7, 2018), https://clearcode.cc/blog/what-is-an-ad-network-and-how-does-it-work/ [https://perma.cc/4D64-DP7D].

90. *Id.*

91. *Id.*

92. Nicole Lindsey, *Could GDPR Consent String Fraud Bring Down the Whole Ad Tech Ecosystem?,* CPO MAGAZINE (Dec. 5, 2018), https://www.cpomagazine.com/data-protection/could-gdpr-consent-string-fraud-bring-down-the-whole-ad-tech-ecosystem/ [https://perma.cc/V5MT-VUGF] ("A consent string is a unique series of numbers generated by a publisher's consent management platform (CMP) and then shared with all digital ad partners. The consent string includes information such as the identity of a vendor, whether or not they have user consent to use data to serve them personalized ads, and how any identifying personal data can be used. The most important consent data is a single bit (a '1' or a '0') that tells an ad tech vendor whether they can serve up personalized ads. If the value is '1,' then the ad tech vendor has user consent; if the value is '0,' then the ad tech vendor does not have user consent.").

93. FED. TRADE COMM'N, *supra* note 41, at i.

94. *Id.* at ii.

But given the complexity of ad tech, this puts companies in a nearly impossible situation: either they must simplify enough to keep the information digestible or be detailed enough to fully explain data collection and use practices, which requires some explanation of how the technology actually works. This approach will let everyone down, and consumers will be lost either way. As one of us has explained:

> The modern data ecosystem is mind-bogglingly complex, with many different kinds of information collected in many different ways, stored in many different places, processed for many different functions, and shared with many other parties. All that nuance gets glossed over when companies try to simplify and shorten information, the risk hidden or made to seem more benign through abstraction.[95]

But if companies are *too* specific, people will suffer from decision fatigue and depleted limited resources to actually reach or process the tomes of information thrown at them. Unwitting consent lies in every direction.

A third version of unwitting consent is that *consumers might not understand the consequences or risks of the informational relationship*. As a general rule, people have difficulty assessing future risks created by present decisions.[96] We're far too optimistic; we rely too much on the past and lived experience over reliable, generalizable data; we discount future costs too much; and we think the way things are now will stay that way.[97]

But this is what we are asked to do every time a company asks for consent to collect and process our data. Even on good days where people are feeling sharp and contemplative, they are asked to construct scenarios where the granting of consent might come back to bite them or somehow be used in an adverse way against them. But unlike playing football or having surgery, where at least people can get a ballpark sense of risk through guestimation,

---

95. Woodrow Hartzog, *User Agreements are Betraying You*, MEDIUM (June 5, 2018), https://medium.com/s/trustissues/user-agreements-are-betraying-you-19db7135441f [https://perma.cc/2MWQ-JCJC].

96. *See, e.g.*, Caroline Beaton, *Humans Are Bad at Predicting Futures That Don't Benefit Them,* ATLANTIC (Nov. 2, 2017), https://www.theatlantic.com/science/archive/2017/11/humans-are-bad-at-predicting-futures-that-dont-benefit-them/544709/ [https://perma.cc/4NPP-KHQG]; Kate Morgan, *Why You're So Bad at Predicting the Future,* MEDIUM (Jan. 3, 2019), https://medium.com/s/2069/why-youre-so-bad-at-predicting-the-future-68e14a5f41a4 [https://perma.cc/3SKY-CXN5]; Bruce Schneier, *Why the Human Brain is a Poor Judge of Risk,* WIRED (Mar. 22, 2007), https://www.wired.com/2007/03/security-matters0322/ [https://perma.cc/4PLD-DQQ7].

97. *See* Beaton, *supra* note 96.

there's an entire universe of consequences that most people don't even think about when asked for consent to data practices.

Privacy—the rules governing human information—is valuable because it helps protect against a wide array of harms. Privacy protects against so many harms, in fact, that it can be easy to overlook them. Some harms occur far downstream from the points of salience for people, like the point of collection, initial disclosure, or data breach. Consider consent to things like biometrics, particularly facial recognition technology.[98] These surveillance technologies intuitively implicate the dangers of surveillance: the chilling effect of being watched and a generalized fear of retaliation or adverse consequences that might follow.[99] But many of the harms of facial recognition might not immediately spring to mind when people ask for consent to use this technology. People's faceprints can make harassment and stalking easier.[100] They can gradually shift communally supported due process values like "presumed innocent" to "people who have yet to be found guilty of a crime."[101] They can facilitate the suffocation that follows when rules are perfectly enforced.[102] They can reduce the cost of sorting, categorizing, discriminating, and denying opportunities, benefits, or needed support and treatment in furtherance of surveillance capitalism.[103]

Data analytics and advertising surveillance can also involve this kind of unwitting consent. For example, consider how many times people are asked to click "I agree" to certain advertising technologies. There are credible allegations that the process used to target advertisements to internet users

---

98. Woodrow Hartzog & Evan Selinger, *Facial Recognition is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/45RL-6HXD].

99. *See* Neil Richards, *The Dangers of Surveillance,* 126 HARV. L. REV. 1934 (2013).

100. *See* Kevin Rothrock, *Facial Recognition Service Becomes a Weapon Against Russian Porn Actresses,* ARS TECHNICA (Apr. 26, 2016), https://arstechnica.com/tech-policy/2016/04/facial-recognition-service-becomes-a-weapon-against-russian-porn-actresses/ [https://perma.cc/F4HG-6SXF].

101. Anne-Marie Slaughter & Stephanie Hare, *Our Bodies or Ourselves,* PROJECT SYNDICATE (July 23, 2018), https://www.project-syndicate.org/commentary/dangers-of-biometric-data-by-anne-marie-sla ughter-and-stephanie-hare-2018-07?barrier=accesspaylog [https://perma.cc/4N8L-8FC9].

102. *See* Tara Francis Chan, *22 Eerie Photos Show How China Uses Facial Recognition to Track Its Citizens as They Travel, Shop—And Even Use Toilet Paper*, BUSINESS INSIDER (Feb. 12, 2018), http://www.businessinsider.com/how-china-uses-facial-recognition-technology-surveillance-2018-2 [http://perma.cc /TE5E-3HVX].

103. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2018); Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75 (2015); Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/47699 1/ [https://perma.cc/N64Q-ZYG7].

based upon surveillance of their reading habits allows inferences (and targeting) based upon sensitive characteristics, such as race, sexual orientation, health, pregnancy status, and other factors.[104] The possibly apocryphal big data anecdote that is now infamous in tech circles involves a story in the *New York Times Magazine* describing how retail giant Target was able to use a young woman's purchase history and other seemingly benign pieces of information to accurately guess that she was pregnant (and subsequently send her targeted advertisements) before the teenager's father found out.[105] In any event, predictive analytics are no doubt outstripping most peoples' notions of what is capable with data.[106] Asking people to consent to risks that seem like science fiction is another example of consent's sickness. But the bottom line remains that much if not most consent in the digital context suffers from the pathology of unwitting consent.

B. Coerced Consent

Sometimes a choice is not really a choice; it can be an unpleasant game of "would you rather" with a choice between a bad option and a terrible one. This is the problem of *coerced consent*, a choice that takes the "voluntary" out of "knowing and voluntary." Coerced consent can occur, for example, where a person is confronted with a choice between consent and the loss of an important asset such as their life or their job. "Coercion" is of course a provocative term. We use it intentionally here to describe a number of cases on the continuum from fully "voluntary" consent to truly involuntary "sign or die" consent. The closer we get to "sign or die," the more coercive a consent will be. While this category might include traditional forms of coercion that would invalidate agreements under the doctrine of duress, mediated environments that manufacture consent can also be coercive in more manipulative and subtle ways.

---

104. *See* Natasha Tiku, *Privacy Groups Claim Online Ads Can Target Abuse Victims*, WIRED (Jan. 27, 2019), https://www.wired.com/story/privacy-groups-claim-online-ads-can-target-abuse-victims/ [https://perma.cc/AE4D-8T4V].

105. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp [https://perma.cc/K247-ZGHZ]; *see also* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#7f3530266686 [https://perma.cc/B7FJ-7JX7].

106. *See, e.g.*, Hideyuki Matsumi, *Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?*, 48 CUMB. LAW REV. 149, 159–69 (2017).

Like the case of unwitting consent, coerced consent uses the language of gold standard consent to obscure unpleasant consequences. For example, in 2017 the U.S. Congress eliminated Obama Administration privacy protections limiting what cable providers like Verizon and Comcast could do with consumer internet browsing history. At a town meeting with constituents, Congressman James Sensenbrenner declared that when it comes to ISP privacy:

> Nobody's got to use the Internet. . . . Internet companies have invested an awful lot of money in having almost universal service now. The fact is that, you know, I don't think it's my job to tell you that you cannot get advertising for your information being sold. My job, I think, is to tell you that you have the opportunity to do it, and then you take it upon yourself to make that choice. . . . [sic] That's what the law has been, and I think we ought to have more choices rather than fewer choices with the government controlling our everyday lives.[107]

When pressed for clarification by the press, Sensenbrenner's office explained that "people can choose whether or not they want to use certain websites. For instance, in using Facebook, people have the option to agree (or not agree) with its terms of agreement, which covers what kind of information the social media site collects from its users."[108]

There are of course obvious problems with this logic—the very logic that has been used by industry and regulators to avoid meaningful privacy regulation in the United States for decades. First, to "choose" not to use the Internet is in a very real sense to "choose" not to participate in modern society or the modern economy. This might not quite be "sign or die," but it's close to "sign or not live like most people." Second, when it comes to Internet Service Providers, consumers often face no practical choice between providers. ISPs like Comcast or Verizon often operate in virtual or actual monopolies for broadband services. To "choose" not to use one's monopolist cable company for wired broadband is functionally to "choose" once again not to use the Internet at home. (Good luck streaming Netflix on your phone data plan.) Third, even with respect to individual services at the platform layer, there is once again a paucity of choice. If you want to use social networking to connect to your friends or family, Facebook is often

107. Kristine Phillips, *'Nobody's Got to Use the Internet': GOP Lawmaker Who Voted to Scrape Web Privacy Rules*, CHICAGO TRIB. (Apr. 15, 2017), https://www.chicagotribune.com/news/nationworld/politics/ct-sensenbrenner-web-privacy-20170415-story.html [https://perma.cc/JZS9-AZSS].

108. *Id.*

the only real choice. And even if your friends are on Instagram, Facebook (and its data practices) own that too.

Our point is that most consumers in the digital environment have highly limited options for consent, much less for bargaining. This is particularly the case where monopoly power or something like it applies. Even where there is some choice among services (Lyft versus Uber, for example), those services may offer functionally identical data terms. Finally, even where there is "choice" among alternatives, this is by no means the end of the ways in which firms can structure, influence, and nudge consumer choice in ways they desire. The coercion continuum is a function not only of the market power of companies, but also of those companies' power over the design of interfaces to shape and to influence consumer decision-making. This results in "dark patterns," a term coined by user experience designer Harry Brignull. According to Brignull, dark patterns are "tricks used in websites and apps that make you buy or sign up for things that you didn't mean to."[109] Security researcher Greg Conti calls these patterns "malicious" or "evil interfaces."[110] Conti and Edward Sobiesk define malicious interfaces simply as those that "deliberately violate usable design best practices in order to manipulate, exploit, or attack the user."[111] And they are *everywhere*.

Common examples of malicious interfaces include "disabled back buttons, browsers with 'sponsored' default bookmarks, unexpected and unnecessary forms, blinking advertisements, and pop-ups covering desired content."[112] These malicious interfaces often coerce users into disclosing private information.[113] Conti and Sobiesk identified eleven kinds of malicious interfaces:

Coercion – Threatening or mandating the user's compliance.

---

109. DARK PATTERNS, https://darkpatterns.org/ [https://perma.cc/7322-X5ME].

110. Gregory Conti & Edward Sobiesk, *Malicious Interface Design: Exploiting the User*, 2010 WORLD WIDE WEB CONFERENCE 271, 271 (2010), http://www.gregconti.com/publications/201004_malchi.pdf [https://perma.cc/5HN4-HUWY] [hereinafter Conti & Sobiesk, *Malicious Interface Design*] (arguing that security and human-computer interaction committees need to come together to fix deceptive designs); *see also* Tim Jones, *Facebook's 'Evil Interfaces,'* ELEC. FRONTIER FOUND. (Apr. 29, 2010), https://www.eff.org/deeplinks/2010/04/facebooks-evil-interfaces [https://perma.cc/PQT6-MSEV].

111. Conti & Sobiesk, *Malicious Interface Design*, *supra* note 110, at 271 (arguing that security and human-computer interaction committees need to come together to fix deceptive designs).

112. Gregory Conti & Edward Sobiesk, *Malicious Interfaces and Personalization's Uninviting Future*, IEEE COMPUT. SOC'Y & RELIABILITY SOC'Y 72, 72 (May/June 2009), http://www.rumint.org/gregconti/publications/j3pri.pdf [https://perma.cc/WWD2-S6B5] [hereinafter Conti & Sobiesk, *Malicious Interfaces and Personalization's Uninviting Future*] (noting that many individuals are tricked or coerced into divulging information they do not intend or do not want to divulge).

113. *Id.*

Confusion – Asking the user questions or providing information that they do not understand.

Distraction – Attracting the user's attention away from their current task by exploiting perception, particularly pre-attentive processing.

Exploiting Errors – Taking advantage of user errors to facilitate the interface designer's goals.

Forced Work – Deliberately increasing work for the user.

Interruption – Interrupting the user's task flow.

Manipulating Navigation – Creating information architectures and navigation mechanisms that guide the user toward interface designer task accomplishment.

Obfuscation – Hiding desired information and interface elements.

Restricting Functionality – Limiting or omitting controls that would facilitate user task accomplishment.

Shock – Presenting disturbing content to the user.

Trick – Misleading the user or other attempts at deception.[114]

Because companies have strong incentives to obtain consent, it is no surprise many of these malicious interfaces are used to coerce, wheedle, and manipulate people to grant it. Examples ranging in severity abound. Some terms of use agreements just won't let you say no. They only let you put off saying yes until "later." Other kinds of mediated consent leverage psychological pressure to manufacture consent. Consider the concept of what Brignull calls "confirmshaming," that is, "the act of guilting the user into opting into something. The option to decline is worded in such a way as to shame the user into compliance."[115] Consider the request from MyMedic to send users notifications, which forces those who do not wish to receive notification to click a button labeled "no, I prefer to bleed to death."[116] It's a subtle form of psychological coercion, but at scale these attempts can deplete our resolve.

---

114. Conti & Sobiesk, *Malicious Interface Design*, *supra* note 110, at 273.

115. *Confirmshaming*, DARKPATTERNS, https://darkpatterns.org/types-of-dark-pattern/confirmshaming [https://perma.cc/5BEZ-RCQL]; *see also Confirmshaming*, TUMBLR http://confirmshaming.tumblr.com/ [https://perma.cc/K8UA-N963].

116. MYMEDIC, https://mymedic.com/ [https://perma.cc/TZY3-HCTG].

Other examples abound. "Roach motels" make it easy to enroll or give consent, but difficult to leave.[117] "Forced continuity" quietly extends your consent past initial authorizations with affirmative opt-out obligations.[118] While Richard Thaler and Cass Sunstein's book *Nudge* offered an optimistic account of how to use the insights of behavioral economics to influence "choice architecture" for social good through what they called "benevolent paternalism," many tech companies today seem to be using it as a cookbook for coercive and manipulative decision structures.[119]

C. Incapacitated Consent

The third pathology of consent is incapacitated consent. Like coerced consent, incapacitated consent takes the "voluntary" out of "knowing and voluntary," but in this case it does so as a matter of law rather than as a matter of circumstance. Incapacitated consents are those where *voluntariness is simply not available as a matter of law*, such as with children and others who are categorically incapable of legally consenting.

While incapacitated consent may be the easiest of the pathologies to understand, here, too, some examples will help to illuminate the problem. Laws in the United States and Europe have regulated the ways in which companies can collect data about children for some time, though with limited effectiveness.[120] For example, the one area in which the United States has a generally applicable Internet data protection regime is the Children's Online Privacy Protection Act of 1998 (COPPA), which regulates online data collection from children. Yet even though the general age of contractual consent in the United States is 18, COPPA only regulates collection from children under the age of 13.[121] This means that even though children from 13–18 are legally incapable of contractual consent, it is perfectly legal to treat them as consenting adults for data collection purposes under the prevailing "notice and consent" regime.[122]

---

117. *Types of Dark Pattern*, DARKPATTERNS, https://darkpatterns.org/types-of-dark-pattern [https://perma.cc/G89G-FZDN].

118. *Id.*

119. *See* RICHARD R. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008); *see also* Conti & Sobiesk, *Malicious Interfaces and Personalization's Uninviting Future*, *supra* note 112.

120. *See* Simone van der Hof, *I Agree, Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World*, 34 WIS. INT'L L.J. 409, 412, 425 (2016).

121. 5 U.S.C. §§ 6501–6505 (2019); 16 C.F.R. § 312.2 (2018).

122. While an amendment to COPPA has been proposed that contains additional protections, the statute would still heavily rely upon consent. *See* Makena Kelly, *New Privacy Bill Would Give Parents*

In practice, moreover, whether legally or illegally, it has been trivially easy to circumvent the consent of legally incapacitated minors in ways that have led to serious financial and even physical harm. For example, both Apple and Facebook have come under fire for making it too easy for children to run up large debts in app stores or in-app purchases using their parents' credit cards.[123] More recently, the dating apps Tinder and Grindr were investigated by the UK government after police investigated more than thirty cases of child rape resulting from children avoiding the age checks on the application interfaces.[124] Companies may protest after such incidents that they do not intend minors to use their services (and that they put in place measures to forestall this). However, the combination of easy-to-install applications and a permissive regulatory regime makes it all but inevitable that minors will use apps and engage in online and offline activities, ranging from data collection to sex, that they lack the legal capacity to consent to. Simply put, a notice and choice regime coupled with the general goal of "putting users in control" cannot solve the problem of incapacitated consent.

While the Mark Zuckerbergs of the world might lionize control and consent, the digital consumers of the world face a very different reality than the idealized one presented by the CEOs and marketing departments of technology companies. The idealized model paints a picture of consent that evokes the knowing and voluntary gold standard, and relies upon the gold standard's power for its legitimacy. In practice, however, the version of consent that most consumers face is a significant and pathological departure from the gold standard. Unwitting consent takes the "knowing" out of "knowing and voluntary;" coerced and incapacitated consent take the "voluntary" out of "knowing and voluntary." Our articulation of this vocabulary for pathologies of consent is intended to provide a useful way to identify and critique the ways in which consents in practice fall short of the gold standard in theory. Once we can identify the problems, we will be better placed to prescribe solutions, and it is to this that we now turn.

---

an 'Eraser Button' and Ban Ads Targeting Children, VERGE (Mar. 12, 2019), https://www.theverge.com/2019/3/12/18261181/eraser-button-bill-children-privacy-coppa-hawley-markey [https://perma.cc/UU9X-LLG7].

123. *See* Nathan Halverson, *Facebook Knowingly Duped Game-Playing Kids and Their Parents Out of Money*, REVEAL NEWS (Jan. 24, 2019), https://www.revealnews.org/article/facebook-knowingly-duped-game-playing-kids-and-their-parents-out-of-money/ [https://perma.cc/4KLK-7QTR]; Press Release, Fed. Trade Comm'n, Apple Inc. Will Provide Full Consumer Refunds of at Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent (Jan. 15, 2014), https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million [https://perma.cc/P5UJ-4E2R].

124. *See* Ben Quinn, *Tinder and Grindr Face Questions Over Age Checks After Rape Cases*, GUARDIAN (Feb. 10, 2019), https://www.theguardian.com/society/2019/feb/10/tinder-and-grindr-face-questions-over-age-checks-children [https://perma.cc/Z5ED-8NKK].

III. IDEAL CIRCUMSTANCES FOR CONSENT

Although the notion of informed consent in digital environments is deeply problematic, it could still play an important role under the right circumstances. The key is to understand the conditions under which consent can meaningfully enhance autonomy and self-determination. Of course, as discussed above, the foundational notion of informed consent to data practices is that it must be "freely given, specific, informed and unambiguous." This includes notions of voluntariness and revocability.

However, we contend that the problem with consent for data practices isn't necessarily in the *form* or *substance* of the consent itself. Many scholars have examined how to substantively improve requests for informed consent.[125] But an additional, sometimes fatal, problem lies with the circumstances in which consent is given. Informed consent is only useful in particular contexts. If the circumstances and structure under which consent is asked and given are wrong, that consent will be ineffective even if it is "freely given, specific, informed and unambiguous." In this Part, we propose three circumstances necessary for an ideal environment for effective consent. To be meaningful, requests for consent must be *infrequent*, the risks of giving consent must be *vivid* and easy to envision, and data subjects must have an *incentive to take each request seriously*. Sadly, these conditions are scarce in modern data exchanges, but we believe that identifying the problems consumers face in these transactions allows us to identify the contexts in which consent can do valuable and legitimate work.

A. Infrequent Requests

One key to understanding why the pathologies of consent to data practices are so problematic in the digital environment is the fact that there are no limits on the number of requests for consent. Every day, every digital consumer is implicitly or explicitly asked to consent to data collection and processing practices for many, if not most, of the websites they visit, the online accounts they create, the services they sign up for, and the apps they use. Consider your web browsing on laptop and phone, GPS navigation, search engines, smartphone operating systems, social networks, taxi services, travel booking, video and audio streaming services, and all of the

125. *See, e.g.*, Florian Schaub, Rebecca Balebako, Adam Durity & Lorrie Faith Cranor, *A Design Space for Effective Privacy Notices*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 365 (Evan Selinger et al. eds., 2018); Batya Friedman, Peyina Lin & Jessica K. Miller, *Informed Consent by Design*, *in* SECURITY AND USABILITY 495 (Lorrie Faith Cranor & Simson Garfinkel eds., 2005).

other "free" or paid services you use which serve you ads or otherwise collect your data. The result is a casual familiarity turned ennui that leads us to gloss over the terms because we know that another request is just around the corner. Because each consent request is a drain on our time and cognitive load, we wisely choose to conserve our efforts. As one of us has written elsewhere,

> Anyone that has turned off notifications for apps like Facebook's Messenger can attest to the relentless, grinding requests for the user to turn them back on almost every time the app is opened. Many can relate to the experience of a child asking for candy, over and over, until the requests become too much to ignore and we give in, simply to quiet them. Willpower can feel like a finite, vulnerable, and subjective resource, and systems are designed to deplete and erode it. Once our willpower and ability to make choices has been compromised, the control users have been given is meaningless.[126]

Compare this depressing state of affairs to environments with informed consent, such as medical treatment, clinical trials, surgeries, and scientific research. Request for consent to these practices do not come often, by sheer virtue of the fact that treatment and trials are relatively uncommon. Thankfully, surgery is not a daily routine. This provides a necessary downtime and the space to both take consent requests seriously and go about living the rest of our lives. People have the ability to consider informed consent to surgery carefully because they know that they will not be asked for consent to another surgery in a few minutes. Critically, if they decline to give consent to a surgery, people know that they won't be pestered again and again until they say yes. Necessary medical intervention is something of a flashpoint in time: people either agree or don't agree to treatment and then get on with it. Practically speaking, the very need to ask for consent to surgery just doesn't present itself very often.

There is no such practical constraint for consent requests for data collection and processing. Data collection and sharing in the modern world is frequent, and is becoming as routine as walking, eating, and breathing. Data subjects are ceaselessly bombarded with requests for consent. There are no limits on the number of times a company is allowed to ask for a

---

126. *See, e.g.*, Hartzog, *The Case Against Idealising Control*, *supra* note 49, at 429 (footnote omitted) (citing AM. PSYCHOL. ASSOC., WHAT YOU NEED TO KNOW ABOUT WILLPOWER: THE PSYCHOLOGICAL SCIENCE OF SELF-CONTROL (2012), https://www.apa.org/helpcenter/willpower.pdf [https://perma.cc/A2DH-QBE8]); John Tierney, *Do You Suffer From Decision Fatigue?*, N.Y. TIMES (Aug. 17, 2011), https://www.nytimes.com/2011/08/21/magazine/do-you-suffer-from-decision-fatigue.html [https://perma.cc/LJ68-4MJ6].

person's consent, and there are no limits on the number of companies that may simultaneously ask for it. Even if we could consider each individual request rationally, our cognitive bandwidth is overwhelmed.

If consent is to be effective, it must happen infrequently. This means hard choices regarding which requests are more important than others and which kinds of companies should be prioritized. This might feel inherently paternalistic. Who are lawmakers to demote the importance of particular requests? But when all consent requests are important, none of them are. Failing to limit who can ask for informed consent, when they can ask, and how many times ignores the reality that people need time and space if their choices are to be meaningful. When choices are too frequent, consent loses its moral legitimacy as a justification for action.

B. Vivid Risks

At the JFK Medical Center, the consent form for open heart surgery explicitly states that the risks for the procedure include "bleeding requiring blood transfusion or return to surgery for repair, nerve damage, heart, liver, kidney or lung complication and/or even in rare cases death."[127] That's serious stuff. But the list goes on, including "complications arising in the post-operative period preventing normal recuperation. . . . [including] long term ventilation, confusion, fluid accumulation of the lungs, pneumonia, cardiac arrhythmias, fever and abnormal laboratory results. Also infection, long term healing and/or scarring of the surgical site incisions may occur and may require further treatment including surgical repair."[128]

Scars, bleeding, fluid accumulation, and death. These are *vivid*—and thus easy—risks for us to envision. So is the risk of consenting to things like government searches, which might result in imprisonment. These risks might even be *too* vivid, as once we've thought of them they can be difficult to push out of our heads.[129] We even consent to accept the risk of harm in everyday goods and services like rental car agreements that hold the driver

---

127. JFK MEDICAL CENTER, CONSENT FORM FOR OPEN HEART SURGERY 1, https://jfkmc.com/util/forms/Consent-for-Open-Heart-Surgery.pdf [https://perma.cc/QA4V-GKLC].

128. *Id.*

129. *Cf.* KAHNEMAN, *supra* note 62, at 326 (discussing experimental research suggesting that such so-called "vivid" outcomes tend to be viewed as more likely by human brains than a strict rationality calculus would suggest). One of the ongoing debates for informed consent to surgery is that the more vivid risks, even if incredibly unlikely, might have undue sway over a patient's decision. *See* David Thomasma, *Telling the Truth to Patients: A Clinical Ethics Exploration*, 3 CAMBRIDGE Q. HEALTHCARE ETHICS 375 (1994).

responsible for losses or dry cleaners who limit liability for damage to clothes to things like replacing or repairing. But personal data is different from bodily integrity or damage to our liberty or property. The risks of data practices are so opaque that there's an ongoing debate as to whether they should even be legally recognized.[130] Certain kinds of surveillance and data practices might be "creepy," but that's the word we use when we have difficulty specifying exactly the risks we are facing.[131] In fact, most of the risks we face from modern data practices arrive not with a bang but a whimper, if we hear them at all. Information is accumulated bit by bit, with risk accruing incrementally. This makes envisioning the plethora of harms difficult because there is rarely a single moment in time that people can point to when the envisioned risk materializes. Unlike severed arteries and being put in prison, how can people envision "databases of ruin" that have reached the critical mass of jeopardy?[132] Informed consent regimes for data will only work if the risks are vivid.

Even worse, these risks that we are being asked to waive through consent might materialize without our even knowing it. People typically know when they have a heart attack or suffer complications from surgery or pharmaceuticals. But our data could be being used against us this very moment, and we wouldn't know it. Hackers could, right now, be opening credit cards in your name as a result of that data breach last year that you didn't know you were involved in either. That lack of feedback further frustrates our ability to adequately envision the risks. Even when manifested, data harms often stay hidden. And our risk calculus is further funneled into wild speculation, paranoia, or overconfidence.

Of course, some data-related harms are easy to envision, such as being humiliated because a deeply-held secret is revealed, having your identity stolen, or being fired or denied insurance coverage on the basis of a personal data dossier or big data prediction. But the problem is that these harms are difficult to predict and difficult to trace from particular disclosures of information. This leads us to our final pre-condition for gold standard consent.

---

130. *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1 (2011) (offering a theory of privacy harm as legally-cognizable); Daniel Solove & Danielle Keats Citron, *Risk & Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018) (same).

131. Evan Selinger, *Why Do We Love to Call New Technologies "Creepy?,"* SLATE (Aug. 22, 2012), https://slate.com/technology/2012/08/facial-recognition-software-targeted-advertising-we-love-to-call-new-technologies-creepy.html [https://perma.cc/KXT6-7UMY]; *see also* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 3.

132. Paul Ohm, *Don't Build a Database of Ruin*, HARV. BUS. REV. (Aug. 23, 2012), https://hbr.org/2012/08/dont-build-a-database-of-ruin [https://perma.cc/G2MS-QR48].

C. Incentives to Take Each Request Seriously

Certain decisions demand to be taken seriously. The reason people hesitate before consenting to skydiving and surgery is that if it goes wrong, they could die. Mental and physical safety are powerful motivators to understand the risks of particular decisions. Imprisonment and exoneration are powerful motivators to weigh when granting consent to government searches. Even some frequent decisions to grant consent demand to be taken seriously, like participating in sports involving physical contact. It's not just that the choices are infrequent and the risks are vivid. It's that for gold standard consent there must be a clear incentive to critically analyze and deliberate the request for consent because of the magnitude of the stakes involved and the close relationship between the consent and those stakes.

Requests for informed consent are, by definition, individualized and atomized. The moral weight of these frameworks is concentrated in the information delivered to the subject and the subject's voluntary execution of a legally significant choice. Through this call and response, people's autonomy is ostensibly respected, which can justify a host of actions that would otherwise be objectionable. But these justifications break down when people have little incentive to meaningfully consider what is being asked of them. This incentive can be diminished either because the stakes appear insignificant or because people cannot easily see how their decision is consequential because the relationship between the consent and the risks is too remote. Others simply have little incentive to take each request seriously because they feel powerless.[133]

Consider the common fatalistic sentiment that privacy is already dead.[134] Ian Bogost argues that it's hopeless to try and opt out of surveillance capitalism, proclaiming that "the age of privacy nihilism is here."[135] Bogost

---

133. Kimberlee Morrison, *Pew: Internet Users Feel Powerless Against Digital Data Mining*, ADWEEK (Nov. 12, 2014), https://www.adweek.com/digital/pew-internet-users-feel-powerless-digital-data-mining/ [https://perma.cc/manage/create?folder=4014-40406-40412-48449] (describing PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA (Nov. 12, 2014), https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [perma.cc/6VDK-5UFP]); Brian Byer, *Internet Users Worry About Online Privacy But Feel Powerless to Do Much About It*, ENTREPRENEUR (June 20, 2018), https://www.entrepreneur.com/article/314524 [https://perma.cc/2YR6-ZLQS].

134. *See* Neil M. Richards, *Four Privacy Myths*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 33 (Austin Sarat ed., 2015) (debunking the "Privacy is Dead" myth).

135. *See* Ian Bogost, *Welcome to the Age of Privacy Nihilism*, ATLANTIC (Aug. 23, 2018), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198/ [https://perma.cc/A83C-GEJE].

paints a bleak picture, in which "[e]verything you have done has been recorded, munged, and spat back at you to benefit sellers, advertisers, and the brokers who service them. It has been for a long time, and it's not going to stop."[136]

It's hard to blame anyone who feels this way, even if there's so much privacy left to fight for.[137] Tech companies are now the backbone of the American economy. They are multi-billion dollar companies that have their fingers in nearly every aspect of our lives. Even if people were merely skeptical of the tech giants with the most personal data, sometimes called the "Big Five" (Amazon, Google, Facebook, Apple, and Microsoft), people would likely find it difficult, if not impossible, to live a normal, modern life without interacting with them.[138] For the ninety-one percent of Americans that feel that they have lost control over their data, why should any single request for consent compel any forethought at all?[139] Under this view, our consent is a *fait accompli*—something to quickly agree to without deliberation, because there is little point in resistance.

Another way consent can break down is it can be very difficult to draw a line from the practices that need consent to the stakes of the decision. Data harms, unlike physical harms, are not localized. They occur offstage and far away, on servers in remote countries and in boardrooms in faraway cities. The Internet is littered with infographics attempting to chart the flow of data from users to platforms to third party vendors and onward downstream.[140] The expanse of it all is mind boggling. In this light, data subjects have little reason to avoid clicking "I agree" because the services they are using are local, such as the Facebook or Uber app, and the risks are remote, such as unobserved data flows on the other side of the world. Again, people would have little incentive to deliberate because, frankly, they have little notion of the stakes, and the benefits of consent are right at their fingertips.

Finally, consent justifications are weakened when each particular request is just one tiny piece of the larger risk puzzle. Our consent to data practices

---

136. *Id.*

137. Evan Selinger, *Stop Saying Privacy is Dead*, MEDIUM (Oct. 11, 2018), https://medium.com/s/story/stop-saying-privacy-is-dead-513dda573071 [https://perma.cc/WD74-6DUZ].

138. For an in-depth exploration of the difficulties of escaping the Big Five, see Kashmir Hill, *Life Without the Tech Giants*, GIZMODO (Jan. 22, 2019), https://gizmodo.com/life-without-the-tech-giants-1830258056 [https://perma.cc/2P4E-E9J6].

139. *See* Kimberlee Morrison, *Pew: Internet Users Feel Powerless Against Digital Data Mining*, ADWEEK (Nov. 12, 2014), https://www.adweek.com/digital/pew-internet-users-feel-powerless-digital-data-mining/ [https://perma.cc/2SNP-F296].

140. *See, e.g.*, ImBrentJames, *A Healthcare Data Flow Diagram Showing the Complexity That TKY Could Help Simplify*, REDDIT (Aug. 2017), https://www.reddit.com/r/THEKEYOFFICIAL/comments/99q4ny/a_healthcare_data_flow_diagram_showing_the/ [https://perma.cc/2V22-98M4].

is astonishingly dispersed. Thousands of apps and services ask us for small, incremental disclosures, few of which involve the kind of information collection that might give people pause. While dating apps and platforms that collect sensitive and large amounts of personal data might cause some people to consider their risks, it's not as though people share all their information at once. Instead, it trickles out over time, such that our incentives to deliberate at the point of agreement are small because we don't know how much information we will ultimately end up sharing. Most of the time, it probably seems like a small amount. This is like the problem of death by a thousand cuts. And there's little guidance for people regarding which individual cuts matter. So people make the transaction-rational decision to chalk up each individual request for consent as "no big deal" in perpetuity. Such an environment is no place to condition our well-being.

Finally, people don't have great incentives to weigh the externalities of consent. That is, typically people only consider how a particular consented-to action will affect themselves. By allowing consent to companies to collect and process my data, those companies can then better target ads to everyone else who uses the service. One person's data becomes a point of comparison that allows for refined targeting, processing, and use elsewhere in the system. People probably don't take into account this externality when deciding whether to agree or not to give consent for data processing. There just aren't enough incentives for people to consider the implications of data processing for other people on a consistent basis, which creates a collective action problem, another pathology of consent to data practices to add to the list.

IV. BEYOND CONSENT

America desperately needs a new direction for its privacy rules. Notions of consent, control, and transparency have dominated data protection discussions for years, and the result is a sea of "I agree" buttons, drop-down menus, and switches that we are unable to navigate.[141]

In terms of meaningfully protecting our privacy, this approach has been a spectacular failure. The shortcomings of consent and transparency are

141. We have offered a preliminary version of these thoughts here: Woodrow Hartzog & Neil Richards, *It's Time to Try Something Different on Internet Privacy*, WASH. POST (Dec. 20, 2018), https://www.washingtonpost.com/opinions/its-time-to-try-something-different-on-internet-privacy/2018/12/20/bc1d71c0-0315-11e9-9122-82e98f91ee6f_story.html?utm_term=.5cd05e778a52 [https://perma.cc/F67G-DF5Y].

particularly visible in the United States. Congress is still trying to settle on its approach to privacy, but most of the current proposals still build off the notice and choice model.[142] The FTC has made a heroic effort to be the top U.S. privacy cop, but it has been starved of the legal tools and financial resources it needs to do a proper job.

America has a bad reputation for privacy.[143] The world is watching and judging, and the economic stakes are enormous. International data flows are essential for the global economy to function without fundamentally—and expensively—restructuring the Internet to America's huge financial detriment. American tech companies depend on being able to smoothly import European data for processing. But, in 2015, a European Court ruled that America's privacy protections were so poor that it struck down the "Safe Harbor" agreement, which helped enable an international flow of data.[144] Our current data sharing agreement with Europe, called the EU/U.S. "Privacy Shield," is in jeopardy.[145] If it fails, we will need a good replacement.

Europe and others have encouraged the U.S. to adopt a law similar to the EU's new General Data Protection Regulation. But a "U.S. GDPR" seems destined to suffer from the same consent pathologies we have explored in this article. As discussed above, the GDPR and forthcoming ePrivacy directive borrow too heavily from the control and transparency playbook.

---

142. CAMERON F. KERRY, BROOKINGS INSTITUTE, BREAKING DOWN PROPOSALS FOR PRIVACY LEGISLATION: HOW DO THEY REGULATE? (Mar. 8, 2019), https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate/ [https://perma.cc/QGR9-FUYL]; CAMERON F. KERRY, BROOKINGS INSTITUTE, WHY PROTECTING PRIVACY IS A LOSING GAME TODAY—AND HOW TO CHANGE THE GAME (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/5HVK-FLHS]; CONSUMERS INT'L, THE STATE OF DATE PROTECTION RULES AROUND THE WORLD (2018), https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf [https://perma.cc/6N5L-DRLR].

143. MARY MADDEN, PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA (Nov. 12, 2014), https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [perma.cc/6VDK-5UFP]; *Copy That: America Should Borrow From Europe's Data-Privacy Law*, ECONOMIST (Apr. 5, 2018), https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law [https://perma.cc/RKM2-3ENN]; Samuel Gibbs, *What Is 'Safe Harbour' and Why Did the EUCJ Just Declare It Invalid?*, GUARDIAN (Oct. 6, 2015), https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection [https://perma.cc/B4PS-SFV8].

144. *See* Ellen Nakashima, *Top E.U. Court Strikes Down Major Data-Sharing Pact Between U.S. and Europe*, WASH. POST (Oct. 6, 2015), https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html?utm_term=.9ac8bcde9495 [https://perma.cc/SUK3-WD6M].

145. *See* Hayley Evans & Shannon Togawa Mercer, *Privacy Shield on Shaky Ground: What's Up With EU-U.S. Data Privacy Regulations*, LAWFARE (Sept. 2, 2018, 2:31 PM), https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations [https://perma.cc/895C-Y3EW].

Our current approach too often results in nothing more than cluttered minds and inboxes, with people resigned to take-it-or-leave it choices for ad-supported web or social media. Relying upon consent to justify data practices rests on the dubious assumptions that people understand what they are being told, and we can meaningfully calculate the risk of our choices online and exercise agency through mediated technologies.

It should be no wonder that under this framework, privacy—our human information policy—has begun to fall apart, often in breathtaking ways. We've seen a cascade of high-profile privacy failures like the Edward Snowden disclosures, the Cambridge Analytica scandal, the targeting of fake news based on data about political preferences, and data breach after data breach after data breach. Backing this up is an entire ecosystem dependent upon an illusion of control and wheedling, cajoling, and extracting consent by any method possible.

In spite of the failures of control and transparency, some lawmakers are considering doubling down on this failed strategy. But no matter how much control we are given, it will never work online. As we've tried to show in this essay, consent regimes burden data subjects with all of the risks of understanding and self-protection while keeping the data machine humming. Consent does not scale without losing its legitimacy.[146] The control that consent regimes promise us ends up being illusory and overwhelming. Even when companies are transparent, it doesn't lead to reform. Big tech platforms and shadowy advertising companies make their fortunes while the rest of us are watched, nudged, exploited, and exposed to data breaches and the manipulation of politics and elections.

There is a better way.

We should have rules that are more sensitive to relationships and power disparities. One way to do this is for lawmakers to create rules designed to protect our trust—trust in the Internet, trust in those entities that hold our data and promise to use it for our benefit, trust in our economy and in our digital society.[147] Being trustworthy in the digital age means being *discreet* with our data, *honest* about the risk of data practices, *protective* of our personal information, and, above all, *loyal* to us, the data subjects.[148]

There are some indications that lawmakers are willing to consider a trust-based approach to modern privacy rules. In late 2018, U.S. Senator Brian

146. *See, e.g.*, Julie Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1 (2019).
147. *See* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 3.
148. *Id.*

Schatz introduced the "Data Care Act of 2018."[149] Among other things, the bill goes beyond control and transparency goals in favor of three key non-waivable trust-based obligations for companies that use the Internet to collect personal information about people: duties of care, loyalty, and confidentiality. These duties are modeled after what is required of those in a fiduciary relationship, such as a trustee designed to care for a trust on behalf of a beneficiary, but they would apply more broadly if this bill were to pass.[150] They would require tech companies of all kinds to act more like doctors than telemarketers.

Trust rules would eschew consent regimes in favor of obligations to be protective and discrete and refrain from manipulative practices. They would aim to keep tech companies from elevating their short-term profits over our long-term interests. And ideally, legislative efforts built around trust would give regulators the resources they need and prohibit companies from using dense terms of use agreements to get us to waive those obligations. An explicit rejection of flimsy "consent" regimes is an important step forward for American privacy regimes.[151] Companies should be obligated to be trustworthy regardless of what we clicked to "agree" to online.

Another way lawmakers could address some of the pathologies of consent is by targeting abusive trade practices. Sunstein and Thaler's *Nudge* is not a cookbook for manipulators, but it has been used as such, and the law should step in to negate these practices. One of us has argued elsewhere that rules against abusive trade practices and abusive design of information technologies can help mitigate some of the inherent vulnerabilities of control regimes.[152]

The notion of abusive design can be found in consumer protection law, which aims to protect 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

149. S. 3744, 115th Cong. (2018). (In full disclosure, we provided feedback on this bill in draft form.)

150. *See* HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 43, at 99.

151. The bill specifically provides that "The rights and remedies provided under this Act may not be waived or limited by contract or otherwise." S. 3744, 115th Cong. § 5 (2018).

152. HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 43.

> (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.[153]

Rules against abusive trade practices look to the problems people have in assessing risks and benefits even with accurate, truthful information. They should begin with an internal inquiry into how we process information.[154] Since the pathologies of consent are all related to our limitations in processing information, this seems as good of a place as any for privacy reform to begin with.

It's time to take a bold step forward. America has an opportunity to redefine itself as the country that protects the trust that people give to companies. By embracing trust, America can become a leader on privacy instead of following the path of false promises, diminishing returns, and the tedium and vicious banality of mindless clicks of "I agree" buttons. Call it legal innovation, if that's what it takes. But whatever we call it, by requiring that companies respect our trust, America can pave the way for a safe, sustainable, and profitable digital future.

CONCLUSION

Tools are only fit for certain purposes. Legal tools are no different from physical tools in this respect. Frederick Schauer once likened legal tools to the problem of driving a nail into a board when you have a pipe wrench but no hammer. Pipe wrenches are great for tightening or loosening pipes, but

---

153. 12 U.S.C.A. § 5531 (West 2019) (emphasis added).

154. Patrick M. Corrigan, *"Abusive" Acts and Practices: Dodd-Frank's Behaviorally Informed Authority over Consumer Credit Markets and Its Application to Teaser Rates*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 125, 127 (2015) ("While shopping for the best offer, consumers may misperceive the real costs and benefits of a consumer product or service because of a lack of information about the product or service or due to a misunderstanding of the information available to them. The former is said to be a problem of imperfect information, while the latter is said to be a problem of imperfect or bounded rationality. Problems of imperfect information are extrinsic to the consumer, while problems of imperfect rationality are intrinsic.").

they make lousy hammers. You could certainly try to drive the nail into the board with a pipe wrench, but you probably wouldn't get it in straight, if you get it in at all. And you'd probably damage the pipe wrench.[155] Schauer was talking about the First Amendment, but consent is a bit like a pipe wrench as well—it is incredibly useful, even necessary, where it's the right tool for the job, but it can be easily overused, to the detriment of both the task and the tool.

We have over-used the tool of consent to the point that it has become badly damaged. Consent does and should play an essential role in our law, but it cannot do everything well all the time. The over-use of consent in the digital context, combined with limited legal policing of the sufficiency of consent has allowed great fortunes to be created on the basis of personal data, but it has also exposed consumers to data breaches, identity theft, and a surveillance economy unprecedented in human history, one which stretches the very notion of "consent" to say that it was ever actually agreed to. More fundamentally, the manufacturing of consent by exploiting consent's pathologies has diminished the trust in our digital environment that is the key ingredient toward a better future. We can do better, but in order to do so, we need to recognize the pathologies of consent, and limit consent to the contexts in which it is most justified. Going forward, we must rely on strategies other than fictive, manufactured, or coerced consent to minimize the risks and harms of our information economy, if we seek to take advantage of its benefits in a sustainable, ethical, and progressive way.

155. Frederick Schauer, *First Amendment Opportunism*, *in* ETERNALLY VIGILANT: FREE SPEECH IN THE MODERN ERA 175 (Lee C. Bollinger & Geoffrey R. Stone eds., 2002).

A Relational Turn for Data Protection?

*Neil Richards and Woodrow Hartzog**

If there's one thing everyone in the data protection debate can agree on, it's that it's all about the data. All over the world, data protection regimes fixate on when data can be collected, how it is being processed, when it can be accessed or should be deleted, and whether it is personal, sensitive, or deidentified. This is true even for approaches that seem quite different at first glance, such as the U.S. and EU.[1]

But what if our shared focus on the data is too narrow? Data protection as a concept is a relatively new response to a specific technology: the database. In the decades following the Second World War, societies began to realize that data could be aggregated, made searchable, and stored in a pristine state for a remarkably low cost. Lawmakers needed a plan to make sure data could be collected and stored in these databases in a safe and sustainable way. The Fair Information Practices Principle (FIPs), developed with contributions from Americans and Europeans, laid the blueprint for privacy on both sides of the Atlantic.[2] These principles focus on procedural rights like transparency, consent, safeguards, purpose limitations, and data minimization, in service of informational self-determination and a sustainable environment for data processing. Because they emphasize choice and individual autonomy, FIP-based regimes tend to lack substantive prohibitions on particular kinds of data practices. The concept of data protection has been wildly successful in terms of adoption by government and industry. But has it been effective? The jury is still out.

The strongest implementation of the FIPs to date is the GDPR, which has been lauded for its robust and holistic approach. But the GDPR has also failed to reckon with the sheer power of the modern data industrial complex. These companies risk more than just our dignitary interests in our personal data – they control what we see, what we click, and in many cases what we believe. Data is dangerous in the hands of these

* Neil Richards, Koch Distinguished Professor in Law and Director, Cordell Institute, Washington University in St. Louis. Woodrow Hartzog, Professor of Law and Computer Science, Northeastern University.

1 Woodrow Hartzog and Neil Richards, 'Privacy's Constitutional Moment and the Limits of Data Protection' (2020) 61 B C L Rev 1687, 1690-92; James Q Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale L J; Paul Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 NYU L Rev 771; Paul Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy' (2017) 106 Geo L J 115; Paul Schwartz, 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures' (2013) 125 Harv L Rev 1966; See William McGeveran, 'Friending the Privacy Regulators' (2016) 58 Ariz L Rev 960 noting some surprising similarities between U.S. and EU approaches; Anupam Chander, Margo Kaminski and William McGeveran, 'Catalyzing Privacy Law' (forthcoming 2021) Minn L Rev.

2 Woodrow Hartzog, 'The Inadequate, Invaluable Fair Information Practices' (2017) 76 Md L Rev 952; Colin J Bennett and Charles D Raab, 'The Governance of Privacy: Policy Instruments in Global Perspective' (2006) 12; Graham Greenleaf, 'Asian Data Privacy Laws: Trade and Human Rights Perspectives' (2014) 6–7; Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press, 2007); Robert Gellman, 'Fair Information Practices: A Basic History' (2016) (unpublished manuscript), <http://bobgellman.com/rg-docs/rg-FIPshistory.pdf>; Chris Hoofnagle, 'The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)' (2014) (unpublished manuscript) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466418>.

Electronic copy available at: https://ssrn.com/abstract=3745973

companies not just because it is personal to us, but because in their hands it becomes power that can be wielded to control people and institutions.[3] It exposes us in ways that risk more than just identification or denial of control. Data protection regimes were not designed to confront this kind of adversary.[4] Originating in the 1970s, when home computing and mobile phones were still science fiction in the mode of *Star Trek*, the FIPs were a managerial approach for an analog age. Their approach never questioned that data processing might not always be a worthy endeavor, or that what seemed like large amounts of data in the 1970s might seem quaint a half-century later. Most importantly, the FIPs approach never considered that future consumers and citizens might create so much data and have so many commercial and government accounts that informational self-determination could become impossible. Today, unfortunately, we are living in that never-considered future.

There is, however, a different way to approach data privacy. It has less to do with the data itself and more to do with people and their relationships. Specifically, it looks at how the people who expose themselves and the people that are inviting that disclosure relate to each other. It is concerned with what powerful parties owe to vulnerable parties not just with their personal information, but with the things they see, the things they can click, the decisions that are made about them. It's less about the nature of data and more about the nature of power. And it can make data protection work better. We call this *the relational turn in privacy law*. The folly of our modern privacy predicament is our failure to anticipate the sheer power that results from the scale and size of these large tech companies. We had our eyes trained so much on the data that we lost sight of the power that comes from inequality and inequity in relationships, even when data is fairly processed. But it wasn't always this way.

Long before databases or even film cameras, privacy law was primarily about relationships. American understandings of privacy are traditionally dated to Warren and Brandeis' influential 1890 law review article 'The Right to Privacy,' which called for a cause of action against the press for spreading true but private facts.[5] The authors rested their argument on a large and sometimes ancient body of law protecting information in the context of relationships, including evidentiary privileges, confidential relations, blackmail law, and government records.[6] But unlike studio photographers, married couples, pen-pals, and trustees, the new, aggressive press of the Gilded Age didn't have a relationship with the subjects of its reportage. Warren and Brandeis thus conceived of 'the right to privacy' as tort-based rather than relationship-based, applying weakly to all the world rather than strongly in the context of existing relationships.[7] It focused on

3 Hartzog and Richards (n 1); Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries L 1; Lisa M Austin, 'Enough About Me: Why Privacy is About Power, Not Consent (or Harm), A World Without Privacy? What Can/Should Law Do' (Cambridge University Press, 2014); Daniel J Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2000) 53 Stan L Rev 1393; Carissa Véliz, *Privacy is Power: Why and How You Should Take Back Control of Your Data* (Transworld Digital, 2020).

4 See Hartzog and Richards (n 1); Bert-Jaap Koops, 'The Trouble with European Data Proteciton Law' (2014) 4 Int'l Data Privacy L 250.

5 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harv L Rev 193.

6 Neil M Richards and Daniel J Solove, 'Privacy's Other Path: Recovering the Law of Confidentiality' (2007) 96 Geo LJ 123.

7 ibid, 128-45.

Electronic copy available at: https://ssrn.com/abstract=3745973

the nature of the data and whether it was public or private, which became a focus on whether data uses were 'highly offensive to a reasonable person' in American tort law, and whether the data being processed was 'sensitive' or not in data protection regimes.[8]

Although the database shifted the focus of privacy law away from relationships of trust for quite some time, America seems to be rekindling its appreciation for them, perhaps recognizing the limits of focusing too closely on the nature of the data and too little on the relationships in which that data is used. A scholarly movement taking relationships seriously in privacy law that began over decade ago is increasingly active and visible.[9] Some scholars (including the authors of this paper), have advocated for legal rules that draw upon the law of fiduciaries to impose duties of loyalty, confidentiality, and care on tech companies as a way of curbing harmful self-dealing and reckless behavior from tech companies in their data processing and the design of their products.[10] Lawmakers in the U.S. have also proposed legislation that cements these duties within information relationships of trust.[11]

The clear advantage of a relational approach is that it is acutely sensitive to the power disparities within information relationships. Tech companies control what we see, what we can click on, and what sorts of information they want to extract from their customers. They have incredible resources that help them predict and nudge our behavior and have the financial incentive to keep us ever more exposed. Duties of loy-

8 ibid, 151, 175.

9 Neil Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stan Tech L Rev 431; Neil Richards and Woodrow Hartzog, 'A Duty of Loyalty in Privacy Law' (2020) (unpublished manuscript) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217>; Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (forthcoming 2019) Wash U L Rev <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433>; Neil Richards, Woodrow Hartzog, 'Privacy's Trust Gap' (2017) 126 Yale L J 1180, 1183; Neil Richards and Woodrow Hartzog, 'Trusting Big Data Research' (2017) 66 DePaul L Rev 579; Jack M Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49 UC Davis L Rev 1183, 1185; Jack Balkin and Jonathan Zittrain, 'A Grand Bargain to Make Tech Companies Trustworthy' (2016) The Atlantic (2016), <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/>; Jonathan Zittrain, 'Engineering an Election' (2014) 127 Harv L Rev F 335, 340; Lindsey Barrett, 'Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries' (2019) 42 Seattle U L Rev 1057; Ariel Dobkin, 'Information Fiduciaries in Practice: Data Privacy and User Expectations' (2018) 33 Berkeley Tech LJ 1, 1; Cameron F Kerry, 'Why Protecting Privacy Is a Losing Game Today—and How to Change the Game' Brookings (2018) <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>; Ian Kerr, 'The Legal Relationship Between Online Service Providers and Users' (2001) 35 Can Bus LJ 419; Daniel Solove, *The Digital Person* (New York University Press, 2006); Richard S Whitt, 'Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era' (2019) 36 Santa Clara Computer & High Tech LJ 75; Kiel Brennan-Marquez, 'Fourth Amendment Fiduciaries' (2015) 84 Fordham L Rev 611, 612; Lauren Scholz, 'Fiduciary Boilerplate' (2018) J Corp L (forthcoming 2020); Ari Waldman, Privacy as Trust (Cambridge University Press, 2018); Ari Ezra Waldman, 'Privacy As Trust: Sharing Personal Information in A Networked World' (2015) 69 U Miami L Rev 559, 560; Ari Ezra Waldman, 'Privacy, Sharing, and Trust: The Facebook Study' (2016) 67 Case W Res L Rev 193; Christopher W Savage, 'Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy' (2019) 22 Stan Tech L Rev 95.

10 See, eg, Jack Balkin, 'The Fiduciary Model of Privacy' (2020) Harv L Rev F 11; Neil Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stan Tech L Rev 431; Neil Richards and Woodrow Hartzog, 'A Duty of Loyalty in Privacy Law' (2020) (unpublished manuscript), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217>; Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018); Neil Richards, *Why Privacy Matters* (forthcoming 2021); *but see* Lina M Khan and David E Pozen, 'A Skeptical View of Information Fiduciaries' (2019) 133 Harv L Rev 497, 498.

11 *See* Data Care Act of 2019, S. 2961, 116th Cong. § 2 (2019) ('Duty of Loyalty: An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B) (i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user.'), <https://www.congress.gov/bill/116th-congress/senate-bill/2961/text>; Consumer Online Privacy Rights Act, S.2968, 116th Cong. § 101 ('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.'), <https://www.congress.gov/bill/116th-congress/senate-bill/2968/text#toc-idd95044fbea1d498f888e130c44e92067>; New York Privacy Act, S. 5642 (2019), <https://www.nysenate.gov/legislation/bills/2019/s5642> ('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.').

Electronic copy available at: https://ssrn.com/abstract=3745973

alty protect against self-dealing and duties of care protect against dangerous behavior. The greater the power imbalance and the more people are made vulnerable through exposure, the stricter the duty to which the trusted party is held.[12]

Data protection regimes, by contrast target, imbalances of power within relationships more indirectly by looking to the nature of the data. Rules under the data protection model are largely procedural ones, with a few important exceptions. These provisions are combined with data subject rights against all who process their data, and structural proportions, under the idea fair processing is, in and of itself, a way to mitigate power. But these frameworks are not primarily intended to restrict processing, rather to ensure that processing happens in a legitimate manner.[13] Thus, while relational duties explicitly prioritize the best interests of vulnerable parties, data protection regimes ostensibly pre-code the best interests of data subjects into rules and rights built around the fair information practices. But data privacy should be about more than just the FIPs and informational self-determination.[14] Properly understood, data privacy is about civil rights, free expression, freedom from harassment, collective autonomy interests, and how personal information is leveraged to erode our attention spans, our mental well-being, and our public institutions. The GDPR, CCPA, and other data protection regimes around the world fail to undertake a holistic inquiry that is sufficiently sensitive to such values except in the case of 'legitimate interest' processing.

Data protection frameworks are not agnostic to the status and power of actors, of course. Much hinges on whether people are processors, controllers, or data subjects. But these frameworks typically do not account for the power imbalances between these parties. They essentially treat all relationships between data subjects and controllers the same. Put another way, data protection law flattens the power dynamics of specific relationships, treating your relationship with Google the same the one you have with your grocer. And while Google and your grocer might collect some similar kinds of information in the abstract – your shopping habits and credit card information, for example – you are significantly more vulnerable to Google or any tech platform than you are to your grocer. By controlling your mediated environments in ways that expose you, these companies are able to leverage information they have about you, your network, and people it thinks are similar to you to choose what ads you see, whose posts you see, how you are able to interact with them, and what other people see about you. The relational turn in data privacy rachets up the obligations based in a way that is proportional to this exposure.

We think a relational turn for data protection would be superior to the current model, even of the GDPR, which is still FIPs-based in its bones. A relational turn would provide a path towards more substantive rules that would limit how peoples' data could

12 Balkin, (n 10) 13-14.

13 Eg, Bart van der Sloot, 'The General Data Protection Regulation in Plain Language' (2020) 28-29.

14 Woodrow Hartzog, 'The Inadequate, Invaluable Fair Information Practices' 76 Md L Rev 952 (2017); Hartzog and Richards (n 1).

Electronic copy available at: https://ssrn.com/abstract=3745973

be used against them. It would focus on the real problem that privacy and data protection law should tackle – the power consequences of information relationships, making legitimacy of processing a question of fundamental fairness rather than data hygiene. Substantive data rules would demand more than that data serve a 'legitimate interest' of the data processor.[15] They would focus on the power consequences of processing on the data subject, whether we apply some version of the classic fiduciary duties of care, confidentiality, and loyalty, or the trust-promoting duties of honesty, protection, discretion, and loyalty that we have called for in other work.[16]

Perhaps equally important, duties of loyalty and care would allow data protection regimes to finally jettison the concept of consent, which it has long been skeptical of. Instead of obsessing over whether the consent people gave was a truly meaningful, informed, and revocable choice, relational duties allow for a decoupling of choice and consent. People would be protected no matter what they choose.[17]

Notably, the European Commission might have just taken the first major step towards a relational turn in E.U. data protection law. On Nov. 25, 2020, the Commission issued a proposal for a regulation on European data governance (Data Governance Act).[18] This proposal includes a remarkable number of bold data privacy interventions designed to increase trust in data intermediaries, including the idea that 'Data sharing providers that intermediate the exchange of data between individuals as data holders and legal persons should, in addition, bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data holders.'[19] We have long argued for a similarly articulated duty for those entrusted with our information and our online experiences. We think this duty should be the foundation of modern data privacy frameworks and should be applied in a much broader way to encompass all information relationships with significant power disparities.

Much work remains to be done in fleshing out some of the practical the details of the relational turn.[20] Neither Rome nor the FIPs were built in a day, and for all of its flaws, the FIPs model does have the advantage of a half-century's head start. But we worry that if we continue to head down the path of focusing solely on data in service of informational self-determination, it will actually have the effect of continuing to disempower human beings rather than helping them. Ultimately we face a question of what we want the law to do here, and we believe strongly that the informational self-deter-

15 Cf GDPR Art 6.

16 Eg, Neil Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stan Tech L Rev 431; Neil Richards and Woodrow Hartzog, 'A Duty of Loyalty in Privacy Law' (2020) (unpublished manuscript) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217>.

17 For an extended critique of consent-based models for data processing, see Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (forthcoming 2019) Wash U L Rev <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433>.

18 European Commission, Proposal for a Regulation on European data governance (Data Governance Act), <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act> (2020).

19 ibid

20 Neil Richards and Woodrow Hartzog, 'A Duty of Loyalty in Privacy Law' (2020) (unpublished manuscript) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217>; Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (forthcoming 2019) Wash U L Rev <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433>.

Electronic copy available at: https://ssrn.com/abstract=3745973

mination model has been a failure in practice and promises more failure as it confronts the new problems on the horizon: ever-increasing volumes of processing, algorithmic decisionmaking, artificial intelligence, and augmented reality. It's time to try something different. Lawmakers and judges should focus on power and vulnerability and place substantive limitations on the ability of the powerful to manipulate us against our interests. After all, the goal of data protection law should be to promote trust in the digital environment, rather than stoke fear, anxiety, and a sense of being overwhelmed by its complexity. Building trust requires us to focus directly on power imbalances in relationships rather than indirectly through data rules. It's time for data protection's relational turn.

Electronic copy available at: https://ssrn.com/abstract=3745973

Boston College Law Review

Volume 61 | Issue 5 Article 3

5-29-2020

Privacy's Constitutional Moment and the Limits of Data Protection

Woodrow Hartzog
Northeastern University, w.hartzog@northeastern.edu

Neil Richards
Washington University, nrichards@wustl.edu

Follow this and additional works at: https://lawdigitalcommons.bc.edu/bclr

Part of the Constitutional Law Commons, European Law Commons, Internet Law Commons, and the Privacy Law Commons

Recommended Citation

Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C.L. Rev. 1687 (2020), https://lawdigitalcommons.bc.edu/bclr/vol61/iss5/3

This Article is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@bc.edu.

PRIVACY'S CONSTITUTIONAL MOMENT AND THE LIMITS OF DATA PROTECTION

WOODROW HARTZOG
NEIL RICHARDS

INTRODUCTION 1689
I. THE PRIVACY BILL FINALLY COMES DUE 1697
A. The FIPs and the Birth of Data Protection 1699
B. The Internal and External Pressures for Action 1705
C. Data Protection Three Ways 1712
II. THE VIRTUES OF DATA PROTECTION 1717
A. Refined and Sturdy 1717
B. Conformity and Interoperability 1718
C. Formidable and Empowering 1719
III. WHY AMERICAN DATA PROTECTION WILL NOT BE ENOUGH 1721
A. FIPs Assume Data Processing Is Always a Worthy Goal 1722
B. The United States Is Not Europe 1727
1. Data Protection as a Human Right 1727
2. Spurious and Real First Amendment Objections 1729
3. Spurious and Real Standing Objections 1731
C. Data Protection Is Myopic 1733
IV. A NEW FRAMEWORK FOR AMERICAN PRIVACY 1738
A. Corporal 1742
1. Competition 1743
2. Corporate Structure 1744
B. Relational 1745
1. Discretion 1746
2. Honesty 1747
3. Protection 1749
4. Loyalty 1750
C. Informational 1752
D. External 1755
1. Environmental Protection 1755
2. Mental Health 1756
3. Digital Civil Rights 1758
4. Democracy 1759
CONCLUSION 1760

PRIVACY'S CONSTITUTIONAL MOMENT AND THE LIMITS OF DATA PROTECTION

WOODROW HARTZOG*
NEIL RICHARDS**

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

© 2020, Woodrow Hartzog & Neil Richards. All rights reserved.

* Professor of Law and Computer Science, Northeastern University.

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

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

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

INTRODUCTION

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

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

---

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

I. THE PRIVACY BILL FINALLY COMES DUE

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

A. The FIPs and the Birth of Data Protection

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

[48] *Id.*

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

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

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

---

[49] *Id.*

[50] *Id.*

[51] *Id.* at xxi.

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

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

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

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

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

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

---

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

B. The Internal and External Pressures for Action

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

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

---

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

[77] *Id.* at 45–46.

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

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

---

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

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

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

[81] *Id.* at 15.

[82] *Id.* at 11–12.

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

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

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

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

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

---

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

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

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

[88] *Id.*

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

[98] *Id.*

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

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

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

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

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

---

[99] *Id.*

[100] *Id.*

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

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

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

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

[105] *Id.*

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

C. Data Protection Three Ways

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

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

---

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

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

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

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

[110] Noordyke, *supra* note 9.

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

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

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

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

[115] *Id.*

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

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

---

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

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

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.*

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

[128] Kerry, *supra* note 70.

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

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

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

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

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

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

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

---

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

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

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

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

II. THE VIRTUES OF DATA PROTECTION

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

A. Refined and Sturdy

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

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

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

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

---

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

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

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

B. Conformity and Interoperability

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

---

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

[143] *Id.* at 1583.

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

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

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

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

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

C. Formidable and Empowering

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

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

---

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

[156] *Id.*

[157] *Id.*

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

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

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

III. WHY AMERICAN DATA PROTECTION WILL NOT BE ENOUGH

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

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

---

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

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

A. FIPs Assume Data Processing Is Always a Worthy Goal

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

---

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

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

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

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

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

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

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

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

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

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

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

---

[169] *Id.* at 32.

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

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

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

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

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

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

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

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

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

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

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

---

[176] *Id.* at 8.

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

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

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

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

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

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

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

---

[181] *Id.* at 23.

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

[183] *Id.*

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

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

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

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

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

---

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

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

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

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

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

B. The United States Is Not Europe

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

1. Data Protection as a Human Right

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

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

---

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

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

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

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

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

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

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

---

[195] *Id.* at 406.

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

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

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

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

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

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

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

2. Spurious and Real First Amendment Objections

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

3. Spurious and Real Standing Objections

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

---

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

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

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

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

[215] *Id.* at 409.

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

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

---

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

[217] 568 U.S. at 409–10.

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

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

C. Data Protection Is Myopic

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

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

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

---

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

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

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

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

[224] *Id.*

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

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

[227] *Id.*

[228] *Id.*

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

---

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

[236] *Id.*

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

[238] *Id.*

[239] *Id.* at 427.

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

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

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

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

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

[245] *Id.* at 975.

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

IV. A NEW FRAMEWORK FOR AMERICAN PRIVACY

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

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

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

---

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

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

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

[260] *See* LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 27–34 (1999) (noting that Anti-Federalists, including Thomas Jefferson, believed a majority-driven government could abuse its power if a bill of rights were not added to the Constitution).

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

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

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

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

---

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

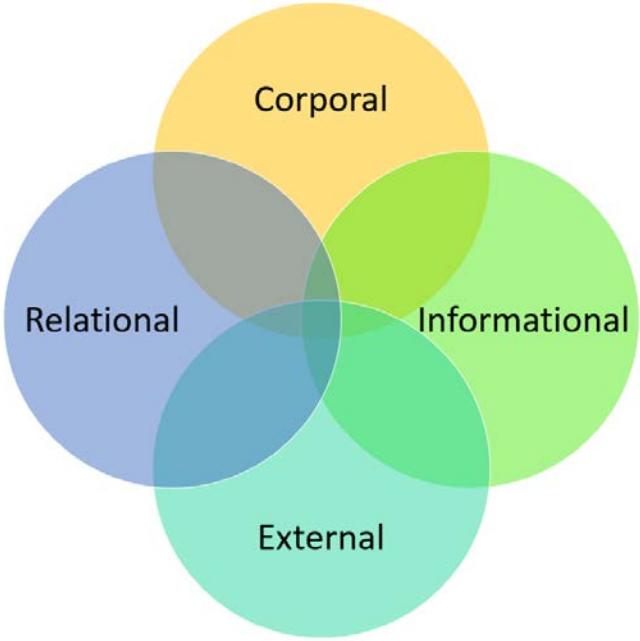
[263] *See, e.g.*, Chander et al., *supra* note 103, at 12–13 (arguing that the new GDPR in Europe is a natural outgrowth of the European constitutional documents that recognize data protection as a "fundamental human right").

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

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

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

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



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

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

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

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

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

---

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

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

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

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

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

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

A. Corporal

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

---

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

[275] *Id.*

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

[277] 15 U.S.C. § 45(a)(1) (2018).

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

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

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

1. Competition

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

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

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

---

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

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

2. Corporate Structure

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

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

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

---

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

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

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

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

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

B. Relational

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

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

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

---

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

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

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

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

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

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

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

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

1. Discretion

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

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

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

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

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

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

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

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

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

2. Honesty

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

---

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

3. Protection

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

---

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

[311] *Id.* at 472–73.

[312] *Id.* at 473.

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

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

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

4. Loyalty

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

C. Informational

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

Cohen, *supra* note 332, at 1927.

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

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

---

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

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

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

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

D. External

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

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

1. Environmental Protection

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

---

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

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

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

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

2. Mental Health

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

[346] Bowles, *supra* note 344.

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

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

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

3. Digital Civil Rights

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

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

---

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

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

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

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

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

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

4. Democracy

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

---

[353] *Id.*

[354] *Id.*

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

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

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

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

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

CONCLUSION

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

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

---

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

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

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 963
I. CORPORATE DATA OPPORTUNISM 969
A. *Profiling and Sorting* 970
B. *Nudging* 973
C. *Manipulation* 975
II. THE NEED FOR A DUTY OF LOYALTY IN PRIVACY LAW 977
A. *Privacy Law Misses Opportunism* 978
B. *A Duty of Care Is Not Enough* 984
III. A THEORY OF LOYALTY FOR INFORMATION RELATIONSHIPS 986
A. *Existing Loyalty Proposals* 987
B. *The Mission of a Duty of Loyalty for Privacy* 989
C. *The Substance of a Duty of Loyalty for Privacy* 995
1. *Rules to Compel or Constrain Behavior* 996
2. *Rebuttable Presumptions of Disloyal Activities* 1001
3. *Guidance and Support for Other Duties* 1002
IV. IMPLEMENTING A DUTY OF LOYALTY IN PRIVACY LAW 1003
A. *When the Duty of Loyalty Should Arise* 1003
1. *When Trust Is Invited* 1004
2. *From People Made Vulnerable by Exposure* 1005
3. *And When Trust Is Given* 1007
B. *Possible Loyalty Frameworks* 1008
1. *General and Ad-Hoc Relational Duties* 1008
2. *Rules Encouraging Loyal Behavior* 1010
3. *Remedies* 1012
V. POTENTIAL OBJECTIONS 1012
A. *Loyalty Is Too Vague* 1013
B. *The Problems of Conflicting Loyalties* 1014
C. *The Problem Is Broader than Just Data Collectors* 1016
D. *Fiduciary Models Risk Entrenching the Status Quo* 1018
E. *The End of Targeted Ads?* 1019
CONCLUSION 1020

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.

EMORY | LAW

Emory Law Journal

Volume 71 | Issue 5

2022

The Surprising Virtues of Data Loyalty

Woodrow Hartzog

Neil Richards

Follow this and additional works at: https://scholarlycommons.law.emory.edu/elj

Part of the Law Commons

Recommended Citation

Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 Emory L. J. 985 (2022).
Available at: https://scholarlycommons.law.emory.edu/elj/vol71/iss5/4

This Article is brought to you for free and open access by the Journals at Emory Law Scholarly Commons. It has been accepted for inclusion in Emory Law Journal by an authorized editor of Emory Law Scholarly Commons. For more information, please contact law-scholarly-commons@emory.edu.

THE SURPRISING VIRTUES OF DATA LOYALTY

Woodrow Hartzog[*]
Neil Richards[**]

ABSTRACT

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

---

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

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

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

INTRODUCTION

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

[1] *See, e.g.*, Data Care Act of 2019, S. 2961, 116th Cong. § 2 (2019) ("Duty of Loyalty: An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B)(i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user."); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 101 (2019) ("Duty of Loyalty: (a) In General.—A covered entity shall not—(1) engage in a deceptive data practice or a harmful data practice; or (2) process or transfer covered data in a manner that violates any provision of this Act."); New York Privacy Act, S. 5642, 2019 Leg., Reg. Sess., § 1102 (N.Y. 2019) ("Every legal entity . . . which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or

duties of loyalty represent both an alternative to the failed "notice and choice" regime in the United States and a supplement to the more robust General Data Protection Regulation (GDPR) model in the EU.[2] Scholars have proposed duties of loyalty—in a variety of forms, including loyalty duties for data collectors, "information fiduciaries," design rules, and fiduciary boilerplates—in part because loyalty represents a substantive check on the ability of companies to use human data to nudge, influence, coerce, and amass vast profits from the exploitation of human information and experiences.[3] Loyalty, thus, holds the potential to be a powerful response to what Julie Cohen calls "informational capitalism" and Shoshana Zuboff calls "surveillance capitalism": the claiming of "human experience as free raw material for hidden commercial practices of extraction, prediction, and sales."[4]

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

---

data broker, in a manner expected by a reasonable consumer under the circumstances."); Commission Proposal for a Regulation of the European Parliament and of the Council on European Data Governance, at 18, COM (2020) 767 final (Nov. 25, 2020); Data Protection Act 2018, c. 12, § 123(1) (Eng.); An Act to Provide Facial Recognition Accountability and Comprehensive Enforcement, H. 117, 2021 Leg., 192d Gen. Ct. Mass., § 2(a) (Mass. 2021) ("A covered entity shall be prohibited from taking any actions with respect to processing facial recognition data or designing facial recognition technologies that conflict with an end user's best interests.").

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

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

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

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

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

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

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

---

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

[7] *Id.* at 504.

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

[9] *Id.* at 12.

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

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

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

affect; not just on procedural requirements for data processing but also on substantive rules restricting dangerous applications; and not merely on the interests of individuals but also on the interests of groups with the same relational vulnerabilities. Loyalty can thus be a powerful state of mind with real analytical and political consequences. Even loyalty's supposed fatal flaw—its indeterminate vagueness[13]—is actually a great strength of flexibility and adaptability across contexts, cultures, and time. Simply put, loyalty as a relational approach allows us to deal substantively with the problem of platforms and human information at both a systemic and an individual level.

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

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

---

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

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

In Part III, we address the critique that a duty of loyalty is *unworkable*, either because it conflicts with a corporation's fiduciary obligation to prioritize shareholder interests over those of human customers or because of the potential clash of individual interests between multiple parties all trusting the same entity. We conclude that these potential conflicts are not only resolvable by lawmakers but also that a turn to relational protections—instead of deferring to informational self-determination[14]—would facilitate a substantive embrace of a broad array of human values over privacy law's reflexive deference to individual choice, consent, and control. Data loyalty would also allow lawmakers to create a uniform definition of "best interests" and thereby prioritize a collective, systemic understanding of this concept over individual, idiosyncratic ones. In this way, a duty of loyalty could be highly functional and consistent with other legal rules across a host of areas.

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

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

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

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

Our response begins with a survey of our law's rich and long-standing experience with loyalty duties in other areas—such as guardians, trusts, professionals, and corporate shareholders—to show how lawmakers and judges have refined the duty to make it clearer and easier to implement in certain contexts while retaining its breadth and flexibility. Lawmakers use a two-step process to implement loyalty obligations in a fair and just way. First, they articulate a primary, general duty of loyalty for a group of actors. Next, courts and lawmakers go about the task of creating and refining what has been referred to as "subsidiary" duties that are more specific and sensitive to context. These subsidiary duties target the most opportunistic contexts for self-dealing and typically result in a mix of overlapping, open-ended rules, maxims, detailed standards, and highly specific rules.[15]

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

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

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

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

I. LOYALTY FOCUSES ON RELATIONSHIPS

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

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

A. Arms-Length Relationships vs. Relationships of Trust

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

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

---

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

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

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

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

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

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

---

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

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

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

[30] *Id.*

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

B. Key Traits of Modern Information Relationships

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

1. Ongoing

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

---

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

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

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

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

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

2. *Frequent*

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

---

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

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

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

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

3. *Constructed*

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

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

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

---

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

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

[40] *Id.* at 35.

[41] *Id.*

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

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

[44] *See* HARTZOG, *supra* note 39.

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

4. *Interactive*

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

5. *Responsive*

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

---

[45] *See id.* chs. 2 & 6.

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

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

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

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

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

II. LOYALTY ACHIEVES WHAT CARE CANNOT

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

---

[48] *See, e.g.*, Calo, *supra* note 43.

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

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

A. Loyalty Makes People's Choices Less Dangerous

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

---

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

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

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

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

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

B. *Loyalty Complements Other Interventions*

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

C. *Loyalty Avoids the Harm Trap*

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

---

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

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

[56] *See, e.g.*, Judson MacLaury, *Government Regulation of Workers' Safety and Health, 1877-1917*, U.S. DEP'T OF LAB., https://www.dol.gov/general/aboutdol/history/mono-regsafeintrotoc (last visited Apr. 26, 2022); Xaq Frohlich, *The Informational Turn in Food Politics: The U.S. FDA's Nutrition Label as Information Infrastructure*, 47 SOC. STUD. SCI. 145 (2017); Dee Pridgen, *The Dynamic Duo of Consumer Protection: State and Private Enforcement of Unfair and Deceptive Trade Practices Laws*, 81 ANTITRUST L.J. 911, 912–14 (2017) (discussing the development of state and federal trade practice laws, which began well after the end of the Industrial Revolution in the United States).

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

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

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

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

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

---

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

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

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

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

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

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

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

[66] To complete the set, the legal wrong in a breach of a duty of confidentiality is an improper *disclosure* of confidential information. *See* Richard Painter, *Fiduciary Principles in Legal Representation*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW 265, 269–71 (Evan J. Criddle et al. eds., 2019); TAMAR FRANKEL, FIDUCIARY LAW, 107–08 (2008) ("The duty of loyalty supports the main purpose of fiduciary law: to prohibit fiduciaries from misappropriating or misusing entrusted property or power. Thus, the duty of loyalty is manifested by important preventative rules. Such rules prohibit actions even though they are not necessarily injurious to

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

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

---

entrustors.").

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

[68] To get a bit technical, in *Spokeo* terms, then, a breach of a legally-imposed duty of loyalty would be a "concrete" intangible harm. To satisfy this requirement, *Spokeo* requires courts "to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* at 1549. But because a breach of a duty of loyalty has been recognized as such a basis for centuries, duties of loyalty do not raise this *Spokeo* problem. *See, e.g.*, Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 860–61 (2022); TAMAR FRANKEL, FIDUCIARY LAW 107–08 (2011) ("The duty of loyalty supports the main purpose of fiduciary law: to prohibit fiduciaries from misappropriating or misusing entrusted property or power. Thus, the duty of loyalty is manifested by important preventative rules. Such rules prohibit actions even though they are not necessarily injurious to entrustors."). By contrast, although duties of care in general would be concrete, statutory causes of action rooted in novel theories of harm would seem to have to run through the *Spokeo* test.

[69] *See* Data Care Act of 2019, S. 2961, 116th Cong. §§ 2–3(b)(2) (2019) ("Duty of Loyalty: An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B) (i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user."); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 101 (2019) ("Duty of Loyalty: (a) In General.—A covered entity shall not—(1) engage in a deceptive data practice

D. Loyalty Animates Legislation and Enforcement

Fourth, and finally, while the notion of a U.S. GDPR may have intuitive appeal in theory, we believe that any such law would be insufficiently protective in practice. There are several reasons for this conclusion, but the most important one is that U.S. privacy rights against companies are different from those in the European Union. In the United States, such rights would likely be consumer protection rights protecting economic interests and could be whittled down in the legislative process by tech company lobbying efforts. By contrast, the GDPR rests upon a solid constitutional footing of fundamental rights to privacy that are simply not present under current American law. In sharp contrast to the United States, E.U. fundamental rights law has long protected privacy as an explicit constitutional right.[70] Today, the E.U. Charter recognizes two separate fundamental rights to privacy: a right to "respect for his or her private and family life," in Article 7, and a separate right to "protection of personal data," in Article 8.[71] Moreover, these European rights are subject to the doctrine of "horizontal effect." Under this doctrine, a member state can violate a person's fundamental rights when it fails to protect it sufficiently against violations by other members of society.[72] Thus, the GDPR's guarantee of privacy and data protection rights against companies is more than mere commercial regulation—because it is the direct implementation and extension of constitutional rights, the GDPR should be understood as having constitutional status.

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

---

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

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

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

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

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

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

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

---

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

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

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

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

[78] *Id.* at 1717–21.

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

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

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

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

---

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

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

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

idea that commercial data processing carries First Amendment value. If companies owe us duties of loyalty, then "innovative" uses of data to exploit us start to resemble betrayal and fraud, and claims of First Amendment protection for manipulative uses of data look appropriately laughable. Loyalty also has the virtue of placing the obligation for ethical data processing right where it belongs, ensuring those to whom we expose our data vulnerabilities do not betray us. In this way, loyalty can be a state of mind; one that has revolutionary potential to stimulate meaningful privacy reform.

III. LOYALTY PRIORITIZES HUMAN VALUES

One of the most prominent critiques levied against the idea of imposing duties of data loyalty on companies is Khan and Pozen's claim that relational rules might create conflicting loyalties. The authors assert that "[t]he tension between what it would take to implement a fiduciary duty of loyalty to users, on the one hand, and these companies' economic incentives and duties to shareholders, on the other, is too deep to resolve without fundamental reform."[82] Khan and Pozen reject the idea of conflicting loyalties as well as the possibility of prioritizing the interests of customers over shareholders, which they contend would conflict with the dominant understanding of corporate law.

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

[82] Khan & Pozen, *supra* note 6, at 534. The authors also note that "the information-fiduciary proposal could cure at most a small fraction of the problems associated with online platforms—and to the extent it does, only by undercutting directors' duties to shareholders, undermining foundational principles of fiduciary law, or both." *Id.* at 529.

A. Data Loyalty's Illusory Conflicts

As an initial matter, the "divided loyalties" argument against relational duties is debatable and, at most, can be fixed by lawmakers without substantially remaking corporate law.[83] Andrew Tuch argues that Khan and Pozen "significantly overstate the threat that corporate and fiduciary law pose for the information fiduciary model."[84] Tuch explains that "imposing user-regarding obligations on corporations will not create untenable frictions between duties to users and duties to shareholders. . . . [T]he primary criticism—that Delaware corporate law undermines the information fiduciary regime—should be dismissed."[85]

Tuch also argues that "the plausible outcome of an information fiduciary regime is exactly the opposite of what Khan and Pozen fear. Under the information fiduciary model, corporate law would require compliance with user-regarding obligations, creating incentives for directors to favor users' interests over those of shareholders."[86] In other words, the loyalty that directors owe to shareholders takes a backseat to all other legal obligations placed upon the corporation, including duties of loyalty to customers.[87] In fact, if a duty of data

---

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

[84] Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. 1897, 1902, 1909–10 (2021). Tuch argues that corporate law only imposes duties on *directors*, not corporations, and the information fiduciaries proposal imposes duties on *corporations*, not directors. *Id.* Relational duties would not create a set of inconsistent obligations among a *single* fiduciary. The issue of parallel fiduciary obligations owed by corporations as a whole to clients and directors to shareholders is routine. Not only is "the likelihood of fiduciary breach that Khan and Pozen point to in claiming tension between Balkin's proposal and corporate law . . . theoretically remote," it is "in practical terms, nonexistent." *Id.* at 1915. Additionally, if lawmakers obligate a duty of loyalty, then directors are bound to privilege it over shareholder interests. *Id.* at 1916–17 ("Delaware law altogether avoids tension with regimes such as Balkin's. Delaware corporate law requires directors to exercise their discretion within legal limits imposed on the corporation; it does not license or excuse non-compliance with corporate obligations, even if directors believe that doing so would maximize shareholder value. And Delaware law offers no suggestion that a corporation's duties or responsibilities should be diluted or otherwise shaped by the content of directors' duties. Instead, case law indicates clearly that directors must act 'within the law.'").

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

[86] *Id.*

[87] *Id*. at 1917–18 ("Reflecting corporate law's attitude toward legal compliance, former Harvard Law Dean Robert Clark identifies the corporation's purpose as to 'maximize the value of the company's shares,

loyalty owed by platforms to people is made positive law, a director that acts with the intent to act in conflict with a customer's best interests or who fails to act in the face of a known loyalty obligation may be liable for breach to shareholders of *their* fiduciary obligation as well as their duty to customers.[88]

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

But what about conflicts between different kinds of customers? James Grimmelmann noted that platforms like eBay serve both buyers and sellers, serving up potentially conflicting loyalties.[89] To Grimmelmann's example, we could also add Uber and Lyft serving drivers and passengers, AirBnb serving renters and leasers, and even Google serving advertiser and human users of its services. This, too, is a common problem in the law of fiduciaries, which has developed several ways to deal with such inevitable conflicts. Andrew Gold explains that "conflicts among best interests obligations [owed to multiple beneficiaries] are unavoidable. Where such conflicts exist, one answer is to find that loyalty must manifest itself as fairness and reasonableness. Another answer is to impose a duty of impartiality," which would demand "due regard" (though not necessarily equality).[90] The "best interests" polestar of loyalty, by design, accommodates all kinds of self-serving behavior. It simply makes self-serving

---

subject to the constraint that the corporation must meet all its legal obligations to others who are related to or affected by it.' . . . Even the most ardent advocates of shareholder primacy have not suggested that corporate law requires, or should require, corporations or directors to maximize shareholder value in violation of a corporation's legal obligations.").

[88] *See id.* at 1919 n.120 (citing *In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 67 (Del. 2006)); *see also* Stone v. Ritter, 911 A.2d 362, 369–70 (Del. 2006) ("The failure to act in good faith may result in liability [for directors] because the requirement to act in good faith 'is a subsidiary element[,]' i.e., a condition, 'of the fundamental duty of loyalty.'" (citing Guttman v. Huang, 823 A.2d 492, 506 n.34 (Del. Ch. 2003))).

[89] Grimmelmann, *supra* note 10.

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

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

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

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

---

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

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

approach would also be consistent with the parallel duty of care and sensitive to the fact that tech companies deal in bulk and batched relationships. A reasonableness, context-sensitive approach would require loyalty obligations that are proportional to the risks of abuse. The duty would be the most robust where the volume of data collected, the company's role in mediating other transactions and relationships, and the potential for manipulation are the greatest. Because this duty of loyalty would be new and novel for privacy law and would need to be tailored to the unique characteristics of modern information relationships, lawmakers can craft a unique and tailored approach that borrows from how duties of loyalty operate in other contexts without being bound by them.

B. The Diverse Value-Forcing Function of Data Loyalty

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

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

[93] Zeynep Tufecki, *The Latest Data Privacy Debacle*, N.Y. TIMES (Jan. 30, 2018), https://www.nytimes.

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

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

IV. LOYALTY CAN BE BOTH FLEXIBLE AND CLEAR

Of all the objections to a duty of loyalty for privacy law, the most frequent and prominent is that the duty is just too vague.[97] In a hearing on the future of transatlantic data flows called by the U.S. Senate Committee on Commerce, Science, and Transportation, Senator Wicker asked of a panelist who advocated for a duty of loyalty in privacy law, "Where is there a working duty of loyalty in place in law somewhere that we can look to[?] . . . When we're able to be specific in those instances, then we're getting somewhere. But beyond that, it's hard actually to define [a duty of loyalty.]"[98] James Grimmelmann also suggests

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

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

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

[96] Gold, *supra* note 90, at 385, 390, 398 (discussing the hierarchy of obligations approach to how "common shares might ordinarily benefit from fiduciary obligations while preferred shares will only benefit in exceptional circumstances").

[97] Grimmelmann, *supra* note 10.

[98] *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing Before the S. Comm. on Com., Sci. & Transp.*, 116th Cong. (Dec. 9, 2020), https://www.commerce.senate.gov/2020/12/the-invalidation-of-the-eu-us-privacy-shield-and-the-future-of-transatlantic-data-flows (statement of Sen. Wicker at 2:05:42–02:07:48). Senator Wicker is the sponsor of one of the most prominent proposals for an omnibus federal privacy law in the United States. The Senator actually expressed tentative support for a duty of

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

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

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

---

loyalty, even though such a duty does not explicitly appear in the bill he sponsored. And in full disclosure, the panelist was one of the authors of this Article. Also, thank you for reading so deeply in our paper—and its footnotes.

[99] Grimmelmann, *supra* note 10.

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

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

[102] *Id*. at 64.

[103] *Id.* at 64–65.

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

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

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

A. "Best Interests" Standard Clarified by Specific Rules

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

---

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

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

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

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

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

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

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

---

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

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

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

[112] *Id.*

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

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

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

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

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

431, 433 (2016).

[115] *See* Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA HIGH TECH. L.J. 75, 89 (2019) ("So, the 'what' of fiduciary power extends to information derived from the underlying relationship. . . . '[R]elational knowledge'—special information that fiduciaries acquire about their beneficiaries—is key to the economic logic and the law supporting these relationships.").

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

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

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

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

---

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

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

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

[120] *Id.*

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

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

We recommend two ways to limit what constitutes a person's "best interests" within the context of data loyalty. First, the "best interests" should be limited to the interests affected by the entrustment of data and attention, instead of an overall well-being standard. Organizations would be directed to ask which interests were implicated by the affordances of the data and design of user interfaces. So, while it might be disloyal for a company to design a system that used trusting parties location data to allow pharmaceutical companies to target them when they are currently in the hospital (and thus vulnerable), it would probably not be disloyal for that company to generally allow pharmaceutical companies to place advertisements on their app or website. Systems that allow for such microtargeted advertising based on highly detailed profiles rather than

---

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

122 *Id.*

123 *Id.* at 894–95.

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

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

Another key aspect of loyalty is that, in conjunction with a duty of care, it can animate a number of different broad subsidiary duties, such as duties of candor, good faith, nondelegation of key services, and confidentiality.[127] But, once again, legislatures and courts often go further and create or delegate authority for the creation of a series of clearer subsidiary obligations that are more like rules than vague standards. Robert Sitkoff explains that "[t]he duties of loyalty and care, which we might call the *primary* fiduciary duties, are typically structured as broad, open-ended standards that speak generally."[128] He notes that "[b]y contrast, the *other* fiduciary duties, which we might call the *subsidiary* or *implementing* fiduciary duties, are typically structured as *rules*, or at least as *more specific standards* that speak with greater specificity."[129]

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

---

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

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

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

[127] *See* Whitt, *supra* note 115, at 94–95 ("Additional fiduciary obligations recognized by courts of equity over many centuries include the duty of candor, duty of good faith, duty not to delegate the services to others, and the duty of confidentiality. Typically they are subsumed as 'subsidiary' or 'implementing' obligations under either the duty of care or of loyalty. However, in some legal quarters the duty of confidentiality has been deemed an important supportive component of the 'primary' fiduciary duties. . . . [T]he duty of confidentiality deserves special status in the digital environment as an 'enabling' obligation that strengthens the more well-established fiduciary duties of care and of loyalty.").

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

[129] *Id.*

maintaining flexibility for new and changed rules in the future.[130] As applied to privacy law, it would allow lawmakers to target large platforms or social media companies that presented specific problems of gatekeeping for third parties or self-dealing due to two-way markets without applying the same specific rules to traditional e-commerce or media streaming companies bound by a general duty of loyalty. Companies not bound by specific subsidiary rules would still be bound by a general duty of loyalty.

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

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

---

[130] Sitkoff gives the prudent investor rule as an example of how subsidiary rules develop in trust law. *Id.* at 420–21 ("Structurally, the prudent investor rule is an elaborated standard that, by focusing on risk-and-return and diversification, gives specific content to the open-ended, primary duty of care, called prudence in trust parlance, as applied to the investment function of trusteeship. . . . [W]ithin the fiduciary fields that do include an investment function, the prudent investor rule encompasses the accumulated learning on what the duty of care requires in fiduciary investment. In consequence, rather than start from scratch in every fiduciary investment matter, fiduciaries, beneficiaries, and courts may look to the elaboration with the prudent investor rule to discern the application of a duty of care.").

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

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

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

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

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

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

---

134 *Id.* at 430.
135 *Id.*
136 *Id.*
137 *Id.*
138 *Id.*
139 *Id.*
140 *Id.* at 431–32.

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

Lawmakers need not stop there. One of the most important subsidiary duties to stem opportunistic behavior would be a robust prohibition on abusive trade practices. As we have detailed in prior work, companies turning people's own cognitive and resource limitations against them to wrongfully extract data and labor is an endemic problem online.[141] Subsidiary rules prohibiting abusive trade practices would prohibit entrustees from materially interfering with the ability of trusting parties to understand the terms of the relationship and lower the risk associated with exposure and engagement. Rules against abuse would also prohibit entrustees from taking unreasonable advantage of a trusting party's lack of understanding about the material risks, costs, or conditions of the service or the inability of trusting parties to protect their interests within the relationship. Finally, anti-abuse rules could prohibit entrustees from taking unreasonable advantage of the reasonable reliance by trusting parties on an entrustee's representation to act in the trusting party's interests.

Lawmakers might also consider rigid prohibitions on specific practices, like the deployment of unreasonably dangerous automated tools or the use of personal data to train those automated systems. They could create subsidiary rules for inherently dangerous practices and technologies that, at the systemic level, are in fundamental conflict with the best interests of trusting parties, such as microtargeting (a practice that paves the way for third party abuse and imposes more externalities than benefits for trusting parties) or affect recognition (the use of machines to read emotional states so as to enhance technology-based persuasion).[142] Lawmakers could craft even more rules designed for specific parties, such as a rule that "social media platforms may not deploy affect recognition technologies on photos or videos submitted by trusting

---

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

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

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

Lawmakers could, of course, impose all these rules even without couching them within an umbrella duty of loyalty. We have proposed in previous research that trust-building and trust-enforcing rules could be meaningful complements or the next best thing to broad and strong relational obligations.[144] Many of these rules, such as generally applicable data protection obligations, should have sibling rules that apply regardless of whether data controllers are in an information relationship with a trusting party. But we believe, as argued in Part I, that a duty of loyalty would act as an important animating force, interpretive guide, and catchall provision to bring more coherence, flexibility, and accountability through enforcement than these rules would as standalone laws.

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

B. Five Areas for Subsidiary Data Loyalty Rules

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

---

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

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

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

[146] *See, e.g.*, Balkin, *Fiduciary Model of Privacy*, *supra* note 3, at 15 ("The nature of fiduciary obligations depends on . . . the potential dangers of abuse, manipulation, self-dealing, and overreaching by the more powerful party."); Scholz, *supra* note 3, at 197; Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 17 (2018) (identifying four major ways of breaching an information fiduciary duty: "manipulation, discrimination, third-party sharing, and violating a company's own privacy policy"); Barrett, *supra* note 125, at 1100 ("[A]n information fiduciary framework should also address manipulation and discrimination in order to ensure that people are protected from the full array of modern digital

five main areas to provide even more specificity to the kinds of subsidiary rules that could give protection to those contexts that are the ripest for abuse. First, entrustees should be loyal when *collecting* information. Even in relationships of trust, data should only be collected when it is in the best interests of trusting parties. Second, entrustees should be loyal when *personalizing* (i.e., treating people differently based upon personal information or characteristics). Third, entrustees should be loyal when *gatekeeping*, avoiding conflicts when allowing government and other third-party access to trusting parties and their data. Fourth, entrustees should be loyal when *influencing* trusting parties, such as when they leverage personal data and digital tools to exert sway over people to achieve particular results. Fifth and finally, entrustees should be loyal when *mediating* interactions between their human customers, specifically in the creation and administration of systems that govern how people are allowed to interact with each other. These contexts often overlap and involve issues like discriminatory microtargeting, harmful amplification of misinformation, failure of process for content moderation, and abusive dark patterns. We propose that lawmakers create an overlapping web of subsidiary loyalty rules to mitigate these kinds of disloyal behavior.

1. Loyal Collection

A duty of loyalty should begin the moment a trusted party invites disclosure and makes the decision to collect personal information. In this way, data loyalty could embolden the fair information principle of data minimization. This principle holds that data collectors should only identify the minimum amount of personal information needed to fulfill a legitimate purpose and collection, and hold that much information and no more.[147] Combined with the storage limitation principle, which holds that organizations should not keep data longer than needed for their stated purpose, data minimization is a central pillar in data protection regimes around the world, but it too often fails to find traction.[148]

Data loyalty could provide a normative vision for when companies have exceeded their duty to minimize collection and retention—when it conflicts with a trusting party's (or collective trusting parties') best interests. Under general

threats that they face.").

[147] *Data Minimisation*, INFO. COMM'RS OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/#data_minimisation (last visited Apr. 26, 2022).

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

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

2. *Loyal Personalization*

The modern Internet routinely and systemically treats people differently based upon their personal information or characteristics. Targeted and behavioral advertising are the most infamous examples of this, but first-party product and streaming recommendations, news feeds, default settings, layouts, and more are all designed to automatically look and act differently based on a person's personal characteristics. Some of this personalization, such as targeted recommendations for networked connections based upon intentionally revealed data (for example, where you work or attended high school), would probably be loyal. Other personalization systems, however, such as those that wrongfully discriminate or have a disparate impact on protected, marginalized, or vulnerable groups of people, would likely conflict with that trusting collective's best

---

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

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

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

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

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

3. *Loyal Gatekeeping*

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

---

151 Dobkin, *supra* note 146, at 26.

152 *Id.*

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

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

access for third parties. Some access granted by trustees to third parties is not in conflict with trusting parties' best interests. For example, contextual advertising usually does not significantly turn people's own data or limitations against them, nor does it usually expose trusting parties to significant privacy harms. Protocols for interoperability to help people transfer data from one place to another also serve the interests (and often the wishes) of trusting parties.

However, certain lax gatekeeping practices would be disloyal because of how they endanger trusting parties by obscuring risk and breaking promises while facilitating access to third parties for organizational gains or to avoid costs. The three most resonant privacy scandals in the past decade—the government surveillance revelations by Edward Snowden, the FBI's request that Apple help them bypass encryption protections, and Cambridge Analytica's massive Facebook data exfiltration—all involved gatekeeping issues.[155] Facebook's system for facilitating third-party applications' access to their customer base was a clear example of making collective user interests subservient to growth metrics, as the company touted to its human customers the virtues of being able to control their audiences while obscuring the true risk of exposure and the steps needed to limit it.[156] Similarly, although companies typically have little choice in respecting legal process compelling customer data, a duty of loyalty would justify rules that mandated additional process for certain kinds of relationships.[157] Kiel Brennan-Marquez argues the following:

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

---

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

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

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

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

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

4. Loyal Influencing

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

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

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

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

---

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

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

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

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

interests.[162] Companies deploy "effort traps" to make deleting an account confusing and difficult. They make "cancel" buttons hard to see and press, obscure important details in tiny fonts or walls of boilerplate, and leverage our deeply-entrenched and empirically-validated overconfidence regarding risk, deference for conformity, endowment effects, status quo bias, and other biases and mental shortcuts to manipulate us to their ends. ("Are you sure you want to delete and miss valuable offers? Your friends will also be so sad to see you go!")

Jamie Luguri and Lior Strahilevitz recently published some of the first comparative evidence quantifying the effectiveness of dark patterns. The scholars explain that "dark patterns are strikingly effective in getting consumers to do what they would not do when confronted with more neutral user interfaces."[163] Luguri and Strahilevitz found that "[r]elatively mild dark patterns more than doubled the percentage of consumers who signed up for a dubious identity theft protection service, . . . and aggressive dark patterns nearly quadrupled the percentage of consumers signing up. In social science terms, the magnitudes of these treatment effects are enormous."[164]

---

[162] *See, e.g.*, HARTZOG, *supra* note 39, at 161; Jamie Luguri & Lior Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 44 (2021); Calo, *Digital Market Manipulation*, supra note 43, at 1005–06; Gregory Conti & Edward Sobiesk, *Malicious Interfaces and Personalization's Uninviting Future*, IEEE SEC. & PRIV., May–June 2009, at 72–73, http://www.rumint.org/gregconti/publications/j3pri.pdf; Johanna Gunawan, David Choffnes, Woodrow Hartzog & Christo Wilson, *Towards an Understanding of Dark Patterns Privacy Harms*, *in* CHI WORKSHOP, WHAT CAN CHI DO ABOUT DARK PATTERNS? 1, 1 (2021), https://darkpatternsindesign.com/position-papers/; Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, A LIST APART (Nov. 1, 2011), https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/; Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt & Austin L. Toombs, *The Dark (Patterns) Side of UX Design*, *in* PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 1, 1, 8–9 (2018), http://dl.acm.org/citation.cfm?doid=3173574.3174108; Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM HUM-COMPUT. INTERACTIONS 1, 4 (2019); Arunesh Mathur, Jonathan Mayer & Mihir Kshirsagar, *What Makes a Dark Pattern . . . Dark? Design Attributes, Normative Considerations, and Measurement Methods*, *in* PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, *supra*, at 1, 13, http://arxiv.org/abs/2101.04843; Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp & Stefan Pfattheicher, *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, 4 PROC. ON PRIV. ENHANCING TECHS. 237, 248–49 (2016); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the "Privacy Paradox*,*"* 31 CURRENT OP. PSYCH. 105, 105, 107–08 (2020).

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

[164] *Id.* They add, "We found that the most effective dark pattern strategies were hidden information (smaller print in a less visually prominent location), obstruction (making users jump through unnecessary hoops to reject a service), trick questions (intentionally confusing prompts), and social proof (efforts to generate a bandwagon effect). Other effective strategies included loaded questions and making acceptance the default. . . . In many cases, consumers exposed to dark patterns did not understand that they had signed up for a costly service." *Id.* at 47.

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

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

---

[165] *Id*. at 46–47.

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

[167] *See* Luguri & Strahilevitz, *supra* note 162, at 99–102 (analyzing constitutional issues presented by dark pattern regulation); *see also* Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 3 (2019) ("[A]t its core, manipulation is hidden influence—the covert subversion of another person's decision-making power. In contrast with persuasion, which is the forthright appeal to another person's decision-making power, or coercion, which is the restriction of acceptable options from which another person might choose, manipulation functions by exploiting the manipulee's cognitive (or affective) weaknesses and vulnerabilities in order to steer his or her decision-making process towards the manipulator's ends.").

[168] Luguri and Strahilevitz recommend a multi-factor test to help determine when dark patterns cross the line that looks to considerations such as "(i) evidence of a defendant's malicious intent or knowledge of detrimental aspects of the user interface's design, (ii) whether vulnerable populations—like less educated consumers, the elderly, or people suffering from chronic medical conditions—are particularly susceptible to the dark pattern, and (iii) the magnitude of the costs and benefits produced by the dark pattern." Luguri & Strahilevitz, *supra* note 162, at 99.

[169] Balkin has proposed looking to "techniques of persuasion and influence that (1) prey on another person's emotional vulnerabilities and lack of knowledge (2) to benefit oneself or one's allies and (3) reduce the welfare of the other person." Jack M. Balkin, *Fixing Social Media's Grand Bargain* 4 (Hoover Working Grp. on Nat'l Sec., Tech, & L., Aegis Series Paper No. 1814, 2018), https://www.hoover.org/sites/default/files/research/docs/balkin_webreadypdf.pdf.

5. *Loyal Mediation*

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

But things can go off the rails quickly if companies feel pressured to achieve continual and endless growth. They create systems that reward virality and the most outrageous or venomous "hot takes" instead of the alleged purpose of meaningful social interaction and social, emotional, and intellectual nourishment. They optimize their algorithms and interfaces to reward our most impulsive and petty reactions. Amplification of certain kinds of information—combined with strategic roadblocks that make it difficult to report harmful speech and hide from other users—leads to acute individual harms like harassment as well as systemic harms like polarization, reduced ability to engage in self-governance, negative public health outcomes, and chilling effects for large groups of vulnerable people.[170]

A duty of loyalty cannot solve all the complex problems of content moderation or harassment. As we have maintained, a duty of loyalty is merely one important tool in a larger toolkit. But companies do have remarkable power to influence how people using their systems interact with each other.[171] They are disloyal when they exert this power to optimize growth in ways that conflict with the best interests of their customers. Subsidiary rules for loyal mediation are, of course, complicated because of the potentially conflicting interests amongst actors and those potentially adversely affected by the act. One trusting party wants to speak while the others are made worse because of it. This is where our proposed systemic focus and the traditional fiduciary law method of developing a hierarchy of loyalties would help clarify lawmakers' actions and firm's obligations.

---

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

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

CONCLUSION

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

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

---

[172] COHEN, *supra* note 4, at 270.

LEGISLATING DATA LOYALTY

Woodrow Hartzog & Neil Richards***

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

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

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

INTRODUCTION

American privacy law is in a rut. It has no privacy identity. Its traditional rules mandating transparency and consent are outdated,

---

© 2022 Woodrow Hartzog & Neil Richards. Individuals and nonprofit institutions may reproduce and distribute copies of this Essay in any format at or below cost, for educational purposes, so long as each copy identifies the authors, provides a citation to the *Notre Dame Law Review Reflection*, and includes this provision in the copyright notice.

* Professor of Law and Computer Science, Northeastern University.

** Koch Distinguished Professor in Law and Director, Cordell Institute, Washington University in St. Louis. Portions and ideas in this Essay are adapted from and developed in much greater detail in the authors' other articles: *A Relational Turn for Data Protection?*, 6 EUR. DATA PROT. L. REV. 492 (2020); *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021); and *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. (forthcoming 2022).

The authors would like to thank Giuliana Green, Sara Hubaishi, Alexis Johnson, and Nina Sprenger for their research assistance. This research was supported by an award from the Notre Dame-IBM Tech Ethics Lab and by Notre Dame-IBM Tech Ethics Lab and by NSF award 1956393/1955227/1956435/2103439: "SaTC: Frontiers: Collaborative: Protecting Personal Data Flow on the Internet" as part of the ProperData project.

porous, and poorly enforced. It is a far cry from the "adequacy" necessary for a profitable and sustainable data trade with the European Union (EU) and Britain. It has, in short, proven no match for the likes of the modern tech giants and a world awash in data and devices. What's worse, while privacy reform appears to be on the agenda, many of the existing proposals—particularly those touted as "business-friendly"—are so weak as to risk codifying a privacy rights status quo that virtually everyone agrees is unacceptable.[1] In searching for a meaningful new approach to regulating data privacy, lawmakers have begun to seriously explore the idea that tech companies should be bound by a duty of loyalty to those who trust them with their data and online experiences.[2]

Scholars have proposed versions of a duty of loyalty for the past twenty years, but not all lawmakers are convinced.[3] Some may be

---

1 This is an argument we have been making for several years. *See e.g.*, Woodrow Hartzog & Neil Richards, Opinion, *There's a Lot to Like About the Senate Privacy Bill, if It's Not Watered Down*, THE HILL (Dec. 6, 2019), https://thehill.com/opinion/technology/472892-theres-a-lot-to-like-about-the-senate-privacy-bill-if-its-not-watered [https://perma.cc/W87Y-ZGPG]; Woodrow Hartzog & Neil Richards, Opinion, *It's Time to Try Something Different on Internet Privacy*, WASH. POST (Dec. 20, 2018), https://www.washingtonpost.com/opinions/its-time-to-try-something-different-on-internet-privacy/2018/12/20/bc1d71c0-0315-11e9-9122-82e98f91ee6f_story.html [https://perma.cc/W63X-UHCP].

2 *See, e.g.*, Data Care Act of 2019, S. 2961, 116th Cong. § 3(b)(2) (2019) (Duty of Loyalty—An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B) (i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 101 (2019) (Duty of Loyalty. (a) In General.—A covered entity shall not—(1) engage in a deceptive data practice or a harmful data practice; or (2) process or transfer covered data in a manner that violates any provision of this Act); New York Privacy Act, S. 5642, 2019–2020 Reg. Sess. (N.Y. 2019) ("Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances."); *Commission Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, COM (2020) 767 final (Nov. 25, 2020); Data Protection Act 2018, c. 123 (UK); An Act to Provide Facial Recognition Accountability and Comprehensive Enforcement, H.R. 117, 192d Gen. Ct., §2(a) (Mass. 2021) ("A covered entity shall be prohibited from taking any actions with respect to processing facial recognition data or designing facial recognition technologies that conflict with an end user's best interests.").

3 *See, e.g.*, Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020) [hereinafter Balkin, *The Fiduciary Model*]; Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016) [hereinafter Balkin, *Information Fiduciaries*]; Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021) [hereinafter Richards & Hartzog, *Duty of Loyalty*]; Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*,

concerned that it is too vague, or that it would be bad for business. Others wonder what data loyalty would get us that we couldn't get from EU or California-style statutes. Others are uncertain about how a duty of loyalty would work and what specific legislation for data loyalty should look like.

In this short Essay, we propose a model for legislating data loyalty. Our model takes advantage of loyalty's strengths—it is well-established in our law, it is flexible, and it can accommodate conflicting values. Our Essay also explains how data loyalty can and should fit within the existing fabric of information privacy law, building on our research exploring how better privacy rules can protect and build trust in relationships between consumers and companies. It lays out the *what* and the *why* of data loyalty for legislators seeking a robust alternative to the failed "notice-and-choice" regime in the United States.

Our argument is simple—a duty of data loyalty is not just appealing in theory—it can be effectively implemented in practice just like the other duties of loyalty our law has recognized for hundreds of years. Loyalty is not only flexible, but it is capable of breathing life into America's historically tepid privacy efforts. It is a meaningful alternative to ineffective regimes that rely too much upon illusory notions of consent and restrictive notions of harm, while being flexible enough to confront new privacy challenges and accommodating mutually beneficial data practices. A properly implemented duty of loyalty could thus represent an answer to many of the problems of information privacy, creating real value for consumers, businesses, and our society as a whole.

---

46 J. CORP. L. 143 (2020); *see also* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34 (2020); Lilian Edwards, *The Problem with Privacy: A Modest Proposal*, 18 INT'L REV. L. COMPUTS. & TECH. 309 (2004); Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95 (2019); Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 340 (2014); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057 (2019); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 1 (2018); Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/L8DQ-SK79]; Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CANADIAN BUS. L.J. 419 (2001); Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA HIGH TECH. L.J. 75 (2020); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 612 (2015); DANIEL J. SOLOVE, THE DIGITAL PERSON (2004); *but see* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019).

I. WHAT IS DATA LOYALTY?

Data loyalty is the simple idea that the organizations we trust should not process our data or design their tools in ways that conflict with our best interests. It borrows from notions of loyalty in fiduciary law, but it is distinct from them. The model we propose here would be crafted by legislators to the specific vulnerabilities and incentives in the relationships between consumers and the data-extractive companies they deal with every day.

Scholars have proposed duties of loyalty in a variety of forms—including loyalty duties for data collectors, "information fiduciaries," or fiduciary boilerplate—in part because loyalty represents a substantive check on the ability of companies to use human data to nudge, influence, coerce, and amass vast profits from the exploitation of human information.[4] It cannot be avoided by trickery, hidden fine print, or manipulative interfaces known as "dark patterns." At its core, it protects the expectations consumers bring to relationships with companies, and it builds trust in those relationships that allows them to flourish to the benefit of both parties.

In other work we have articulated a duty for loyalty for privacy law as the duty of data collectors to act in the best interests of those whose data they collect.[5] A duty of loyalty for privacy law is neither perfect nor a tool for all tasks. But loyalty has one great virtue: it places the focus for information age problems on the relationships that define our social lives rather than on the data which is the byproduct of those relationships. Loyalty shifts the law's attention from the procedural rules of privacy law that are too easy to manipulate ("Did you hide a vague sentence in the privacy policy?" "Did the consumer fail to hit the tiny opt-out button?") to the substantive question of what practices go too far. It is flexible and adaptable across contexts, cultures, and times. Loyalty can thus be a powerful response to what Shoshana

---

4 *See, e.g.*, Balkin, *The Fiduciary Model*, *supra* note 3; Balkin, *Information Fiduciaries*, *supra* note 3; Richards & Hartzog, *Duty of Loyalty*, *supra* note 3; Scholz, *supra* note 3; *see also* WALDMAN, *supra* note 3; Haupt, *supra* note 3; Edwards, *supra* note 3; Savage, *supra* note 3; Zittrain, *supra* note 3, at 340; Barrett, *supra* note 3; Dobkin, *supra* note 3, at 1; Kerry, *supra* note 3; Kerr, *supra* note 3; Whitt, *supra* note 3; Brennan-Marquez, *supra* note 3, at 612; SOLOVE, *supra* note 3.

5 *See, e.g.*, Richards & Hartzog, *Duty of Loyalty*, *supra* note 3; Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. (forthcoming 2022); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020) [hereinafter Hartzog & Richards, *Privacy's Constitutional Moment*]; Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*]; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019) [hereinafter Richards & Hartzog, *Pathologies of Digital Consent*]; Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180 (2017) (book review).

Zuboff calls "surveillance capitalism," the claiming of "human experience as free raw material for hidden commercial practices of extraction, prediction, and sales . . . As significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth."[6]

Data loyalty has three key features—it is a (1) *relational duty* (2) that *prohibits self-dealing* (3) at the *expense of a trusting party.* Let's break these three features apart.

A. A Relational Duty

Lawmakers who decide they want to regulate privacy can begin their task by focusing on at least three different things. First, they could focus on the data itself, like what can be collected and whether datasets are deidentified. This is the approach that most federal and European privacy laws have taken to date with laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Second, there are structural concerns, like requiring companies to appoint a data privacy officer or focusing on monopoly power. This is the approach familiar to antitrust and corporate law. There's also a third option—lawmakers could focus on our relationships, like requiring confidentiality from physicians, lawyers, and other professionals.[7]

In addition to being one of the oldest contexts for privacy to flourish, relationships have a few distinct advantages for lawmakers looking to fight the excesses and abuses of data-hungry organizations. First, relational duties are acutely sensitive to the *power disparities* within information relationships. Tech companies control what we see, what we can click on, and what sorts of information they want to extract from their customers. They have incredible resources that help them predict and nudge our behavior and have the financial incentive to keep us ever more exposed. Duties of loyalty protect against self-dealing, while related duties of care placed on relationships protect against dangerous behavior and the risks of harm. The greater the power imbalance and the more vulnerable people are through exposure, so should the duty to which the trusted party is held be greater.[8]

Second, relational duties are a way out of *privacy's consent trap.* For years lawmakers, regulators, and companies have been obsessing over whether the consent people gave was a truly meaningful, informed, and revocable choice. People click "I Agree" buttons and slightly

---

6 SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER, at vii (2019).

7 *See* Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 5, at 1697.

8 *See, e.g.*, Balkin, *The Fiduciary Model*, *supra* note 3, at 13–14.

wince without reading the terms because it is impossible to do so, even when what they click states that they read and understand the terms. Consent is broken, but lawmakers have stuck to notice and consent regimes anyway, even though it is common knowledge that digital consent is rarely meaningful. Relational duties allow for a decoupling of choice and consent. These duties allow trusting parties to enter into information relationships without accepting the risks of whatever harmful data practices and consequences lurk in the fine print, the business model, or the technology. They can also allow trusting parties to select from a range of choices without fear of betrayal because they would be protected no matter what they chose.[9]

Finally, relationships open the possibility of more *robust enforcement rules* because they are voluntarily entered into and hold a unique place in the law as a result. The concept of contractual privity could also be used to extend relational duties beyond the initial trusting party and entrustee. Under a "chain-link" approach to relational privacy rules, lawmakers could directly—or using mandated terms in data-sharing contracts—link the disclosure of personal information to obligations of loyalty to protect information as it is disclosed downstream.[10] To create the chain of protection, contracts would be used to link each new recipient of information to a previous recipient who wished to disclose the information. At the same time, relational duties raise even fewer free expression issues than other forms of data regulation because they regulate relationships rather than information flows. In relationships, parties assume these duties by soliciting trust and voluntarily entering into these relationships. Moreover, protections for power-imbalanced relationships have a deep tradition in U.S. law in harmony with free expression frameworks. This is, for example, why lawyers do not have a First Amendment right to disclose client confidences, no matter how "newsworthy" they might be.[11]

For these reasons, shifting the focus of privacy law from data to relationships offers significant advantages for effective policy.

---

9 For an extended critique of consent-based models for data processing, see Richards & Hartzog, *Pathologies of Digital Consent*, *supra* note 5.

10 *See* Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 658–61 (2012).

11 *Cf.* Balkin, *Information Fiduciaries*, *supra* note 3; Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1057–58 (2000) (explaining that enforcement of contracts to maintain confidentiality create no First Amendment problems); Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887 (2006). *But see* Khan & Pozen, *supra* note 3.

B. That Prohibits Self-Dealing

Many of the problems of surveillance capitalism come down to the problem of self-dealing, where an organization exploits an advantage over a trusting party to its own benefit.[12] The failures of American privacy law have enabled such corporate opportunism and manipulation of consumers using human information. This problem is particularly serious in the context of "personalized" technologies that promise to know us so that they can better satisfy our needs and wants. Insufficiently constrained by privacy law and driven to maximize quarterly profits by corporate law, companies can deploy a potent cocktail of techniques derived from cognitive and behavioral science to "nudge" or otherwise influence the choices we make.[13] These highly capitalized tech companies have not acted like the benevolent choice architects some had hoped for.[14] Technologies—and choice architecture—advertised as serving consumers have instead become weaponized, serving commodified consumers up to the companies and their commercial and political advertiser clients.[15]

Loyalty rules directly prohibit conflicted self-dealing. In so doing, they can change the incentives and business models of entire industries. Many critics believe that U.S. data privacy law has failed to change the corrosive business models that endanger, manipulate, mislead, misinform, and polarize people every day. The law, these critics suggest, merely prunes the edges of wrongdoing rather than getting to the core of the problem.[16] A duty of data loyalty would directly address this problem by taking self-dealing off the table as a general matter. More specific, subsidiary data loyalty rules for targeted advertising, web scraping, manipulative interfaces, and optimized human engagement metrics could revolutionize entire industries with clearer rules of the road. They could make certain abusive business models obsolete overnight. This would be a sharp contrast to the piecemeal and procedural approach of current U.S. data privacy law, which presupposes that all possible extraction models can be valid if they follow the right procedures and give people some semblance of control over their information. Data loyalty rules instead look directly to corporate profit motives and ask if they conflict with a trusting

---

12 *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); ZUBOFF, *supra* note 6.

13 *See* NEIL RICHARDS, WHY PRIVACY MATTERS 39–50 (2022).

14 *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 11–13 (2008).

15 *See* RICHARDS, *supra* note 13, at 46–49.

16 *See, e.g.*, Facebook, Inc., F.T.C. No. 1823109 (July 24, 2019) (Chopra, Comm'r, dissenting); Facebook, Inc., F.T.C. No. 1823109 (July 24, 2019) (Kelly, Comm'r, dissenting).

party's best interests. They require profit models to be based on the provision of valuable services rather than exploitation and extraction.

C. At the Expense of a Trusting Party

Loyalty rules safeguard trusting parties from betrayal, looking to whether a trusting party has been disadvantaged by an organization's self-dealing. When organizations enrich themselves with trusting parties' data, people consistently end up paying with their time, attention, mental well-being, reputation, and significant life opportunities.[17] These costs include everything from notifications interrupting our attention to advance the interests of the platform, to manipulative advertising that causes people to buy (or vote) differently in ways that serve advertisers, to the well-documented emotional injuries wrought by engagement-driven social media. Crucially, these costs, impositions, and manipulations are made substantially more damaging by "personalization" enabled by self-dealing in personal data. Thus, it's not just a random notification or one serving your interests like a reminder to attend a meeting, but one teasing you out of the blue that someone you know may have done something cool. It's not just an ad or a political message, but one calculated to your precisely known psychology and vulnerabilities.[18] And it's not just social media telling you what your friends are doing, it's being done in a way that is calibrated to push your buttons to keep you scrolling (or doom-scrolling) with a reckless indifference to your mental health.[19]

The scope of protection that loyalty rules safeguard includes, but is broader than, recognized privacy harms like identity theft, emotional harms, breaches of confidence, and dangerous exposure.[20] It also includes more subtle individual and collective costs to our identity, our ability to create relationships, our collectively held truths, and the obscurity that protects our ability to share and move about freely. As

---

17 *See* Neil Richards & Woodrow Hartzog, *Against Engagement* (draft manuscript) (on file with authors).

18 This is precisely what happened in the Cambridge Analytica scandal, in which Facebook data was used to create finely calibrated psychological profiles of voters identified by their real names, suggesting which kinds of arguments would be most effective at getting them to act in the ways that the paying political advertisers wanted them to. *See* RICHARDS, *supra* note 13, at 25–26.

19 These are the allegations Facebook whistleblower Frances Haugen presented under oath before lawmakers in the United States and around the world in 2021. *See, e.g.*, Billy Perrigo, *Inside Frances Haugen's Decision to Take on Facebook*, TIME (Nov. 22, 2021) https://time.com/6121931/frances-haugen-facebook-whistleblower-profile/ [https://perma.cc/L8QN-6GD5].

20 *See, e.g.*, Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011).

such, it protects against the full range of betrayals that powerful parties in an information relationship can engage in.

* * *

Loyalty duties are thus quite straightforward when understood as relational duties that prevent self-dealing at the expense of a trusting party. They accord with basic notions of fairness and decency—if you have power over someone who trusts you, you shouldn't betray them or manipulate them to serve your own interests. It is undoubtedly for these reasons that our law has placed duties of loyalty on relationships with power imbalances for centuries in a wide variety of contexts.

II. WHY DATA LOYALTY?

One common question that proposals for a duty of data loyalty often face is, "What does a duty of loyalty get you that other approaches to regulation do not?" This is an excellent question that asks why a duty of loyalty might be the right regulatory tool rather than some other approach. We believe that duties of data loyalty offer four important advantages that other approaches do not.

First, loyalty represents a central policy commitment that could be the missing ingredient to embolden existing U.S. privacy frameworks. Second, it is substantially more capable than a traditional data protection approach when it comes to modern privacy problems like algorithmic discrimination, manipulation, oppression, and shaming that are caused by unceasing digital contact and the astonishing scale and power of modern technology platforms. Third, loyalty helps solve privacy law's harm problem in a way that is consistent with the direction of current Supreme Court doctrine. Finally, data loyalty has a straightforward and strong rhetorical appeal; it offers a clear explanation for better privacy rules, it could help define America's privacy identity, and it could be used to gather broad popular support for stronger privacy rules.

A. To Embolden Existing Data Privacy Frameworks

Law professor Ryan Calo is fond of saying that technology law's biggest problem is that we lack the political will to enforce the rules we already have.[21] We believe that this problem persists in privacy law as

21 *See, e.g.*, Ryan Calo, *Artificial Intelligence and the Carousel of Soft Law*, 2 IEEE TRANSACTIONS ON TECH. & SOC'Y 171, 171 (2021) ("But ultimately what is missing is not knowledge about the content of ethics as much as political will."); *Enlisting Big Data in the Fight Against Coronavirus: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2020) (statement of Ryan Calo, Law Professor, University of Washington) ("It is also

well. Many privacy regulators lack the same political will and support from lawmakers and the executive branch to enforce existing data rules in a robust way. Many privacy rules are also vague, leaving their interpretation (and enforcement based upon that interpretation) up in the air. For example, what constitutes an "unfair trade practice," a "reasonable expectation of privacy," or the collection of "more data than is necessary" is a perennial topic of debate.

One of the reasons why U.S. data privacy frameworks tend to wilt is that they lack a clear touchstone to guide interpretation that would lead to effective enforcement. The collection of U.S. privacy statutes, enforcement actions, and common law remedies adhere to basic commitments like "do not lie," "do not harm," and "follow the Fair Information Practices (FIPS)."[22] But such edicts tend not to interrogate the wrongful motives of data processors and do little to force companies into any practice beyond bare compliance.

A duty of loyalty could change that. Lawmakers should use loyalty duties to embolden and revitalize *existing* approaches to regulating data privacy, such as robust implementation of data minimization requirements, rules against unfair and deceptive trade practices, and expansion of products liability theories of accountability. Data loyalty can empower lawmakers to use tools that have already been developed, by expanding the contexts in which rules should be followed, who must follow them, and the level of adherence necessary for compliance.

Take as an example data minimization, the idea that organizations should only collect, maintain, and use data that is necessary to fulfill a designated and legitimate purpose. Data minimization rules are a fundamental commitment of data protection and data security laws. They are scattered throughout U.S. law, including the California Consumer Privacy Act,[23] the Wiretap Act,[24] and are implicitly a part of

important to note that a lack of political will is sometimes the greater hurdle than a lack of information.").

22 *See, e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 15 (2018); Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 5, at 1704 & n.66; Richards & Hartzog, *Duty of Loyalty*, *supra* note 3, at 42.

23 CAL. CIV. CODE § 1798.100(c) (2018) ("A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not processed in a manner that is incompatible with those purposes.").

24 18 U.S.C. § 2518(5) (2018) ("No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. . . . Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to

the data security requirements of Section 5 of the FTC Act.[25] Data minimization, if robustly interpreted and enforced as a way for companies to remain loyal to trusting parties, could be a remarkably effective tool for regulators since it targets both collection and use of data and is meant to counter abusive purpose creep by companies.[26] If data loyalty became a guiding obligation for data minimization rules, it would give regulators and judges interpreting potential violations an additional layer of interrogation. Data loyalty would compel an examination of a company's motives *and* the potential adverse consequences to consumers in determining if more data than necessary was collected or if the use of data deviated too far from its original purpose. Such foundational support would prevent an arid and strictly textual analysis by explicitly forcing regulators and judges to look at the big picture of exploitative motives of organizations and the trusting parties' wellbeing.

Another example would be laws based on the Fair Information Practices, the most common standard for privacy laws worldwide. Under current U.S. privacy law, perhaps the most important question for regulators and compliance professionals is whether consumers have been given "notice and choice." In principle, this is a good thing, emphasizing consent to data practices and evoking the gold standard of "knowing and voluntary" consent familiar to lawyers and medical researchers. But in practice, under current American law, "notice and choice" all too often means just that consumers have merely vague "notice" of data practices that are buried in the fine print and illusory "choice" with respect to these practices such as a take-it-or-leave-it choice about whether to use the service.

In practice, such rules not only place few constraints on companies, but they also represent a kind of cookbook to create and justify even deeply disloyal data practices by checking the boxes of fictional notice and illusory consent. This is likely why companies like Amazon have been engaged in aggressive lobbying in many state capitols to get weak notice-and-choice (and only weak notice-and-

interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.").

25 *See* FTC, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT (2014) ("The Commission has also provided educational materials to industry and the public about reasonable data security practices. These materials explain that, while there is no single solution, such a program follows certain basic principles. . . . [Among them,] companies should limit the information they collect and retain based on their legitimate business needs so that needless storage of data does not create unnecessary risks of unauthorized access to the data.").

26 *See, e.g.*, DANIEL SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT (forthcoming 2022).

choice) laws on the books.[27] But here, too, a duty of loyalty could help. If data loyalty became a guiding obligation for data processing, notice-and-choice requirements would become more than a checkbox compliance exercise at best and a cookbook for manipulation at worst. Instead, "notice" would become an obligation of honesty, ensuring that consumers actually understood what was happening with their data before they agreed to it, and preventing companies from all sorts of self-interested practices where meaningful understanding was not present. "Choice" would mean knowing and voluntary agreement to particular data practices among reasonable alternatives that do not conflict with a trusting party's best interests, rather than a "choice" about whether to live in the modern world or not.

In these ways, by reorienting the question for companies from "What can we get away with" to "Are we being loyal to our human customers," a duty of data loyalty could breathe new life into existing regimes that are moribund at best and exploitation-enabling at their worst.

B. To Address Emergent Dangers

A second benefit of data loyalty is that it can safeguard consumers against novel and emerging digital risks. Data loyalty duties can *go beyond* the standard data processing concerns and traditional privacy harms. In crafting such rules, lawmakers should look to the ways in which the affordances of modern technologies endanger people by bestowing power in trusted entities. Data loyalty duties should scrutinize how those organizations have incentives to use the power human information gives them in self-interested ways that conflict with a trusting party's best interests. Duties crafted in this way would meaningfully respond to concerns about manipulative user interfaces (sometimes called "dark patterns"), the wrongful extraction of human labor by dominant platforms, algorithmic discrimination, and protection against third parties and other users while using a service. Duties of data loyalty can thus go beyond often hard-to-quantify injuries of individual pieces of data and address the structural power imbalances and inequalities that characterize the relationships between individual harried consumers and the richest corporations in the history of the world.

---

27 *See* Jeffrey Dastin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, REUTERS (Nov. 19, 2021), https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/ [https://perma.cc/LE8N-PBCM].

C. To Solve Privacy's Harm Problem

Third, and related to the problem of emergent dangers, a duty of data loyalty would help lawmakers solve one of privacy law's most difficult problems: the problem of cognizable harm. Many privacy rules require some kind of economic, physical, emotional, or other kind of concrete and traditionally recognized harm to be legally cognizable. However, loyalty rules look to the trusted party's inequitable conduct of wrongfully exploiting an advantage gained by an information relationship. The exploitation of the relationship against a trusting party's interests can itself be the wrong, such as in a case of conflict of interest, even if no other tangible harm manifests.[28]

In privacy cases, this is significant because American plaintiffs in privacy and data breach lawsuits have struggled to articulate diffuse but real informational injuries, and this situation has been made worse in recent years as courts have tightened the rules for what counts as a legally cognizable injury under Article III standing doctrine.[29] Critically, loyalty duties do not have this problem—not just because the legal injury in loyalty cases is the disloyalty itself, but because this injury is one that has been already recognized by courts as legally sufficient within standing doctrine.[30]

The focus of loyalty is on the integrity of a relationship and removing an incentive and ability to wrongfully profit by taking advantage of a power disparity. Because loyalty duties are rooted in betrayal rather than harm or injury, they have significant consumer

---

28 *See* TAMAR FRANKEL, FIDUCIARY LAW 107–08 (2011) ("The duty of loyalty supports the main purpose of fiduciary law: to prohibit fiduciaries from misappropriating or misusing entrusted property or power. Thus, the duty of loyalty is manifested by important preventative rules. Such rules prohibit actions even though they are not necessarily injurious to entrustors.").

29 *See, e.g.*, TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2214 (2021); Spokeo, Inc. v. Robins, 578 U.S. 330, 342 (2016).

30 To get a bit technical for a moment, in *TransUnion/Spokeo* terms, then, a breach of a legally imposed duty of loyalty would be a "concrete" and "traditionally recognized" intangible harm. To satisfy this requirement, *Spokeo* requires courts "to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Spokeo*, 578 U.S. at 341. *Ramirez* uses a slightly different formulation—asking whether an intangible injury bears "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *Ramirez*, 141 S. Ct. at 2204. But because a breach of a duty of loyalty has been recognized as a basis for lawsuits for centuries, duties of loyalty simply do not raise concreteness problems. *See also* Citron & Solove, *supra* note 20. By contrast, although duties of care in general would be concrete, statutory causes of action rooted in novel theories of harm (including procedural data protection requirements) would seem to have to run through the *Spokeo* test, with an uncertain likelihood of success.

protection advantages over existing privacy rules that demand proof of injury.[31]

D. To Define America's Privacy Identity

Finally, a duty of data loyalty could offer a defining value for America's privacy law identity, rather than forcing it to adopt a watered-down and sometimes ill-fitting version of the European GDPR approach. While American privacy law is weak, permissive, and seemingly rudderless, in Europe, privacy law is on firmer ground. Privacy and data protection are both considered fundamental human rights in the EU.[32] The GDPR is the manifestation of these rights, a commitment to the idea that people should be able to determine their informational fates for themselves. Bilyana Petkova has argued that data protection is "the main tenet of constitutional identity" in the EU.[33] This is why European data protection law often seems so strikingly powerful to American observers compared to domestic consumer privacy rights. As much as anything, then, for Europeans the GDPR is a state of mind. And it is why a U.S. version of the GDPR would inevitably be both a weak and inadequate version of the real GDPR, something we have elsewhere called a "GDPR-lite."[34]

A duty of loyalty could fill this definitional role for U.S. privacy law. It could supply a political lodestar for privacy reform that defines America's privacy identity on its own terms rather than those of the EU. Lawmakers should not underestimate loyalty's rhetorical potential. A rallying cry requiring companies to "act in our best interests" could motivate American privacy reform in the way that "the right to be let alone" did at the turn of the twentieth century. Technocratic terms like "data minimization" and "legitimate interests of the data controller" do little for public imagination or comprehension. By contrast, loyalty is clear, it is easy to understand, and it is potentially robust enough to counterbalance spurious industry claims about the importance of "innovation" or the idea that commercial data processing carries First Amendment value. GDPR-style ideas like requiring companies to undergo data protection impact assessments can feel wonky and feeble, but every person in America likely knows how it feels to be betrayed.

---

31 *See, e.g.*, H.R. 117, 192d Gen. Ct., §2(a) (Mass. 2021) ("A covered entity shall be prohibited from taking any actions with respect to processing facial recognition data or designing facial recognition technologies that conflict with an end user's best interests.").

32 *See, e.g.*, U.N. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221; Charter of Fundamental Rights of the European Union arts. 7–8, 2000 O.J. (C 364).

33 Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L.J. 140, 154 (2019).

34 For an extended version of an argument along these lines, see Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 5, at 1727–32.

If companies owe us duties of loyalty, then "innovative" uses of data to exploit us start to resemble betrayal and fraud, and claims of First Amendment protection for manipulative uses of data look appropriately laughable. Loyalty also has the virtue of placing the obligation for ethical data processing right where it belongs, ensuring those to whom we expose our data vulnerabilities do not betray us. A duty of loyalty in privacy law would be important not just as a set of rules, but as an *idea* capable of rallying democratic support for strong rules.

Finally, loyalty can be good for business. At a U.S. Senate hearing in 2020, Senator Brian Schatz expressed the idea that duties of loyalty are only needed for bad businesses, because good businesses know that the best way to make money over the long term is to be loyal to their customers.[35] On the other hand, if disloyalty is permitted by the law, the pressures on business to show quarterly profits create strong short-term and short-sighted incentives to cheat and behave in disloyal ways. This in many respects is the story of the contemporary digital economy, a story that data loyalty offers the potential to change for the better.

III. A MODEL FOR LEGISLATING DATA LOYALTY

One undeniable virtue of creating a duty of data loyalty is that it would not be necessary to invent it from whole cloth. Loyalty duties have a long and established pedigree in our law, most famously in the law of fiduciaries. A duty of data loyalty could draw heavily from this tradition and its proven ability to protect against the power imbalances in relationships in a fair, principled, and meaningful way.

Fiduciary law scholars have identified a two-step process lawmakers use to implement loyalty obligations in such a fair and just way.[36] Lawmakers initially articulate a primary, general duty of loyalty. Next, courts and lawmakers go about the task of creating and refining what have been referred to as "subsidiary" duties that are more specific and sensitive to context. These subsidiary duties target the most opportunistic contexts for self-dealing and typically result in a mix of overlapping open-ended rules, maxims, more specific standards, and highly specific rules.

---

35 *See Revisiting the Need for Federal Data Privacy Legislation: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2020) (statement of Sen. Brian Schatz).

36 *See, e.g.*, Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW 419 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019) ("The duties of loyalty and care, which we might call the *primary* fiduciary duties, are typically structured as broad, open-ended standards that speak generally. . . . By contrast, the *other* fiduciary duties, which we might call the *subsidiary* or *implementing* fiduciary duties, are typically structured as *rules* or at least as *more specific standards* that speak with greater specificity.").

Thus, we propose that a duty of data loyalty should be implemented on two levels. The first level is a broad and general prohibition on substantial conflicts with the trusting party's best interests. This would prevent the most egregious forms of disloyalty across the board, and it would also serve to orient the company's incentives generally against betrayal rather than micromanaging specific instances. The second level of a duty of loyalty would be more specific and, where necessary, restrictive. This would involve the articulation of specific and substantive subsidiary duties targeting particular contexts and actions that provide clear rules and less wiggle room to ensure accountability and keep the frameworks from becoming watered down. Though this two-step approach, a duty of data loyalty could provide both general applicability as well as sensitivity to individual contexts.

A. First, a General Catchall Duty

We propose a general rule of data loyalty as follows:

Organizations shall not process data or design systems and tools in ways that significantly conflict with trusting parties' best interests that are implicated by their exposure.

Let's break this proposed duty down a little.

1. A No-Conflict Rule for Data and Design

Organizations gain a power advantage over trusting parties in two different ways: collecting and processing data and controlling our mediated experiences.[37] If the duty of loyalty is to accomplish anything, it should prohibit the conflicted design of digital tools and data processing. Avoiding conflicts is loyalty's core mandate and the logical starting point for lawmakers, judges, industry, and civil society. A general rule against conflicted design and data processing could serve as the foundation for a host of regulatory regimes, self-regulatory efforts, and guidance to the public to encourage and nurture its trust.

A general no-conflict rule has the remarkable advantage of directing lawmakers (and trusted parties themselves) to interrogate not just actions but *motives* and *gains*.[38] Established fiduciary no-conflict rules

37 *See, e.g.*, RICHARDS, *supra* note 13; HARTZOG, *supra* note 22.

38 *See* Paul B. Miller & Andrew S. Gold, *Fiduciary Governance*, 57 WM. & MARY L. REV. 513, 557–58 (2015) (quoting Lionel Smith, *The Motive, Not the Deed*, *in* RATIONALIZING PROPERTY, EQUITY AND TRUSTS: ESSAYS IN HONOUR OF EDWARD BURN 53, 67 (Joshua Getzler ed., 2003) ("[T]he motives of the fiduciary are the crucial element in determining whether

> do not require the fiduciary to act in any particular way but are instead thought to establish boundaries within which the fiduciary may reasonably be expected to act loyally, at least to the extent that the rules isolate biasing factors that might induce the fiduciary to subjugate the interests of beneficiaries to the interests of others.[39]

2. People Over Profits

Some lawmakers are reluctant to adopt duties of data loyalty because they fear creating a conflict with the duties of loyalty that directors of organizations owe to shareholders.[40] This is an illusory conflict and, at most, is resolvable by lawmakers without substantially remaking corporate law.[41] The supposed conflict between trusting parties and shareholders has been wildly overstated.[42] Fiduciary law scholar Andrew Tuch explains that "imposing user-regarding

---

the fiduciary has acted loyally, and the requirement of motive is quite specific—the fiduciary 'must act (or not act) in what *he perceives to be* the best interests of the beneficiary.'")).

39 *Id.* at 557.

40 One of the most repeated critiques levied against the idea of imposing duties of data loyalty on companies is Lina Khan and David Pozen's claim that relational rules might create conflicting loyalties. The authors assert that "[t]he tension between what it would take to implement a fiduciary duty of loyalty to users, on the one hand, and these companies' economic incentives and duties to shareholders, on the other, is too deep to resolve without fundamental reform." Khan & Pozen, *supra* note 3, at 529, 534 ("[T]he information-fiduciary proposal could cure at most a small fraction of the problems associated with online platforms—and to the extent it does, only by undercutting directors' duties to shareholders, undermining foundational principles of fiduciary law, or both.").

41 *See, e.g.*, Balkin, *The Fiduciary Model*, *supra* note 3, at 23 ("Management's fiduciary obligations to shareholders *assume* that the corporation will attempt to comply with the legal duties owed to those affected by the corporation's business practices, even if this reduces shareholder value.").

42 *See* Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. 1897, 1902 (2021) (arguing that Khan and Pozen "significantly overstate the threat that corporate and fiduciary law poses for the information fiduciary model."). Tuch argues that corporate law only imposes duties on *directors*, not corporations, and the information fiduciaries proposal imposes duties on *corporations*, not directors. *See id.* at 1909. Relational duties would not create a set of inconsistent obligations among a *single* fiduciary. *See id.* at 1910. The issue of parallel fiduciary obligations owed by corporations as a whole to clients and directors to shareholders is routine. *See id.* Not only is the "likelihood of fiduciary breach that Khan and Pozen point to in claiming tension between Balkin's proposal and corporate law . . . theoretically remote," it is "in practical terms, nonexistent." *Id.* at 1915. Additionally, if lawmakers obligate a duty of loyalty, then directors are bound to privilege it over shareholder interests. *See id.* at 1916–17 ("Delaware law altogether avoids tension with regimes such as Balkin's. Delaware corporate law requires directors to exercise their discretion within legal limits imposed on the corporation; it does not license or excuse non-compliance with corporate obligations, even if directors believe that doing so would maximize shareholder value. And Delaware law offers no suggestion that a corporation's duties or responsibilities should be diluted or otherwise shaped by the content of directors' duties. Instead, case law indicates that directors must act 'within the law.'" (footnotes omitted)).

obligations on corporations will not create untenable frictions between duties to users and duties to shareholders. . . . [T]he primary criticism—that Delaware corporate law undermines the information fiduciary regime—should be dismissed."[43]

If lawmakers were to adopt data loyalty rules, then corporate law would in fact demand that directors adhere to them first and foremost.[44] In other words, the loyalty that directors owe to shareholders takes a backseat to legal obligations placed upon the corporation, including duties of loyalty to customers.[45] In fact, if a duty of data loyalty owed by platforms to people is made positive law, a director that acts with the intent to act in conflict with users' best interests or fails to act in the face of a known loyalty obligation may be liable for breach to shareholders of their fiduciary obligation as well as their duty to users.[46]

If data loyalty is going to work, then trusting parties must be prioritized over other loyalties owed by organizations, such as loyalty duties owed by firms to shareholders. Prioritizing trusting parties over shareholders would resolve any lingering "divided loyalty" concerns, as well as conflicting loyalties between users and third-party vendors. Self-interested actions would be allowed, but only if they didn't conflict with trusting parties' best interests regarding their data and mediated experiences. And of course, it is an elementary principle of U.S.

---

43 *Id.* at 1902 ("The criticism rests on a partial understanding of corporate law doctrine and theory. The criticism sees conflicting obligations where none exist and identifies strategies for resolving these apparent conflicts that are unknown to corporate law. . . . I also argue that Khan and Pozen's arguments are not merely mistaken but, if accepted, may do harm. Applying their case to financial conglomerates—more apt analogues for social media companies than the '[d]octors, lawyers, accountants, and the like' to whom scholars often draw their comparison—shows that Khan and Pozen's arguments, if accepted, would have pernicious effects on broad spheres of corporate regulation." (quoting Khan & Pozen, *supra* note 3, at 506)).

44 Tuch argues that "[u]nder the information fiduciary model, corporate law would require compliance with user-regarding obligations, creating incentives for directors to favor users' interests over those of shareholders." *Id.*

45 *Id.* at 1917–18 ("Reflecting corporate law's attitude toward legal compliance, former Harvard Law Dean Robert Clark identifies the corporation's purpose as to 'maximize the value of the company's shares, subject to the constraint that the corporation must meet all its legal obligations to others who are related to or affected by it.' . . . Even the most ardent advocates of shareholder primacy have not suggested that corporate law requires, or should require, corporations or directors to maximize shareholder value in violation of a corporation's legal obligations." (quoting ROBERT CHARLES CLARK, CORPORATE LAW 17–18 (1986))).

46 *See id.* at 1918–19 (citing *In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 67 (Del. 2006); *see also* Stone v. Ritter, 911 A.2d 362, 369–70 (Del. 2006) ("The failure to act in good faith may result in liability [for directors] because the requirement to act in good faith 'is a subsidiary element[,]' i.e., a condition, 'of the fundamental duty of loyalty.'") (citing Guttman v. Huang, 823 A.2d 492, 506 n.34 (Del. Ch. 2003)).

constitutional law that a federal duty of loyalty would take precedence over any state duties by operation of the Supremacy Clause.

Data loyalty would still allow companies to profit and flourish. The "best interests" polestar of loyalty, by design, accommodates all kinds of self-serving behavior. It simply makes self-serving behavior allowable only in instances where it aligns with the best interests of the primary trusting party.[47]

3. The Collective Best Interests of Trusting Parties

There are a few different ways to deal with inevitable conflicts between trusting parties as well. The first would be to impose a reasonableness and fairness approach, or a duty of impartiality between people who expose themselves to organizations.[48] In trying to accommodate the best interests of billions of individuals, whose "best interests" might differ from person to person, lawmakers could also follow tort law's move to a more objective standard: the reasonable user. Not only would a reasonable user standard help companies better determine the scope of their duties, but it would also inject a normative element into the analysis.

Our proposal adopts a collective approach to "best interests," to better avoid conflicts between trusting parties and help free privacy law from its overly individualistic focus. Allowing lawmakers and regulators to focus on the collective best interests of "trusting parties," they can better respond to systemic harms detected sporadically by individuals but strongly at the group level. We recommend that lawmakers specifically prioritize interests that are held collectively by groups of users, with certain individually held interests holding sway only to the extent they do not conflict with collective user interests.[49]

A more collective best interests approach would be an improvement over the individual self-determination model, which does not compel people to consider the common good or threats to

---

47 *See* John H. Langbein, *Questioning the Trust Law Duty of Loyalty: Sole Interest or Best Interest?*, 114 YALE L.J. 929, 932 (2005) ("[A] transaction prudently undertaken to advance the best interest of the beneficiaries best serves the purpose of the duty of loyalty, even if the trustee also does or might derive some benefit. A transaction in which there has been conflict or overlap of interest should be sustained if the trustee can prove that the transaction was prudently undertaken in the best interest of the beneficiaries.").

48 Andrew S. Gold, *The Fiduciary Duty of Loyalty*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 36, at 398 ("[C]onflicts among best interests obligations [owed to multiple beneficiaries] are unavoidable. Where such conflicts exist, one answer is to find that loyalty must manifest itself as fairness and reasonableness. Another answer is to impose a duty of impartiality," which would demand "due regard" (though not necessarily equality). (footnotes omitted)).

49 *Id.* (discussing the hierarchy of obligations approach to how "common shares might ordinarily benefit from fiduciary obligations while preferred shares will only benefit in exceptional [circumstances]").

groups they are not a part of. When people give consent to data practices, they usually aren't motivated to reflect upon how their decision will affect vulnerable groups that they are not a part of.[50] This is similar to some people's indifference to public health when they "choose" not to wear a mask during a pandemic.

A reasonable user approach would also be consistent with the parallel duty of care and sensitive to the fact that tech companies deal in bulk and batched relationships. A reasonableness, context-sensitive approach would require loyalty obligations that are proportional to risk of abuse. The duty would be the most robust where the volume of data collected is highest and organization's power over people is the greatest. Because this duty of loyalty would be new and novel for privacy law and would need to be tailored to the unique characteristics of modern information relationships, lawmakers have the ability to craft a unique and fitting approach that borrows from how duties of loyalty operate in other contexts without being bound by it.

4. Limited to Trusting Parties' Exposure

In our previous work on trust, we defined the concept of trust as the willingness to make oneself vulnerable to the actions of others.[51] Our proposed general duty of loyalty would be limited to the extent of that vulnerability. Specifically, the "best interests" should be limited to the interests affected by the entrustment of data, labor, and attention, instead of an overall well-being standard. Organizations would be directed to ask what interests were implicated by the affordances of the data and design of user interfaces. So while it might be disloyal for a company to design a system that leveraged trusting parties' geolocation to allow pharmaceutical companies to target people when they are currently in the hospital (and thus vulnerable), it would probably not be disloyal for that company to generally allow pharmaceutical companies to place advertisements on their app or website. Systems that allow for such microtargeted advertising based on highly detailed profiles rather than isolated contexts make exploitation of vulnerable parties easier and compound incentives for companies to engineer exposure for financial gains.[52]

In conjunction with a duty of care, a duty of loyalty animates a number of different broad subsidiary duties, such as duties of candor,

---

50 *See, e.g.*, Richards & Hartzog, *Pathologies of Digital Consent*, *supra* note 5, at 1498; Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33, 44 (2020).

51 Richards & Hartzog, *Taking Trust Seriously*, *supra* note 5, at 448.

52 *See, e.g.*, JOSEPH JEROME & ARIEL FOX JOHNSON, ADTECH AND KIDS: BEHAVIORAL ADS NEED A TIME OUT (2021).

good faith, nondelegation of key services, and confidentiality.[53] But legislatures and courts often go further and create or delegate authority for the creation of a series of clearer subsidiary obligations that are more like rules than vague standards.[54]

This two-tiered approach allows lawmakers to tailor rules to specific relationships to avoid specific foreseeable conduct while maintaining flexibility for new and changed rules in the future.[55] As applied to privacy law, it would allow lawmakers to target large platforms or social media companies that presented specific problems of gatekeeping for third parties or self-dealing due to two-way markets without applying the same specific rules to traditional e-commerce or media streaming companies bound by a general duty of loyalty. Companies not bound by specific subsidiary rules would still be bound by a general duty of loyalty.

B. Second, Rules for Subsidiary Implementing Duties

Lawmakers can create specific subsidiary rules to help resolve objections that a duty of data loyalty is just too vague.[56] Enacting

---

53 *See* Whitt, *supra* note 3, at 94–95 ("Additional fiduciary obligations recognized by courts of equity over many centuries include the duty of candor, duty of good faith, duty not to delegate the services to others, and the duty of confidentiality. Typically they are subsumed as 'subsidiary' or 'implementing' obligations under either the duty of care or of loyalty. However, in some legal quarters the duty of confidentiality has been deemed an important supportive component of the 'primary' fiduciary duties. . . . [T]he duty of confidentiality deserves special status in the digital environment as an 'enabling' obligation that strengthens the more well-established fiduciary duties of care and of loyalty." (footnotes omitted)).

54 Robert Sitkoff explains that

> [t]he duties of loyalty and care, which we might call the *primary* fiduciary duties, are typically structured as broad, open-ended standards that speak generally. . . . By contrast, the *other* fiduciary duties, which we might call the *subsidiary* or *implementing* fiduciary duties, are typically structured as *rules* or at least as *more specific standards* that speak with greater specificity.

Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 36, at 419.

55 Sitkoff gives the prudent investor rule as an example of a how subsidiary rules develop in trust law. *Id.* at 421 ("Structurally the prudent investor rule is an elaborated standard that, by focusing on risk-and-return and diversification, gives specific content to the open-ended, primary duty of care, called prudence in trust parlance, as applied to the investment function of trusteeship . . . . [W]ithin the fiduciary fields that do include an investment function, the prudent investor rule encompasses the accumulated learning on what the duty of care requires in fiduciary investment. In consequence, rather than start from scratch in every fiduciary investment matter, fiduciaries, beneficiaries, and courts may look to the elaboration within the prudent investor rule to discern the application of the duty of care.").

56 In a hearing on the future of transatlantic data flows called by the U.S. Senate Committee on Commerce, Science, & Transportation, Senator Wicker asked of a panelist who advocated for a duty of loyalty in privacy law, "[w]here is there a working duty of loyalty

legislation should also either provide for subsidiary duties or delegate rulemaking authority for future subsidiary rules. These subsidiary data loyalty rules might take a page from and model information privacy versions of nonprivacy fiduciary duties such as disclosure, consent, accounting for property (access and portability rights), confidentiality, and the full suite of fair information practice principles. This would apply some of the most significant obligations compelled by the GDPR. A duty of loyalty, combined with a duty of care, could spur on specific rulemaking for concepts like data minimization and legitimate basis requirements that would be bound together by an antibetrayal ethos.

But lawmakers need not stop there. One of the most important subsidiary duties to stem opportunistic behavior would be a robust prohibition on abusive trade practices. As we detailed in prior work, companies leveraging people's own cognitive and resource limitations against them to wrongfully extract data and labor is an endemic problem online.

Subsidiary rules prohibiting abusive trade practices would prohibit entrustees from materially interfering with the ability of trusting parties to understand the terms of the relationship and the risk associated with exposure and engagement.[57] Rules against abuse would also prohibit entrustees from taking unreasonable advantage of trusting parties' lack of understanding about the material risks, costs, or conditions of the entrustees' service or the inability of trusting

---

in place in law somewhere that we can look to? When we're able to be specific in those instances, then we're getting somewhere. But beyond that, it's hard actually to define [a duty of loyalty]." *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2020) (statement of Sen. Roger Wicker, Chairman, S. Comm. on Com., Sci., & Transp.). Senator Wicker is the sponsor of one of the most prominent proposals for an omnibus federal privacy law in the United States. The Senator actually expressed tentative support for a duty of loyalty, even though such a duty does not explicitly appear in the bill he sponsored. And in full disclosure, the panelist was one of the authors of this Essay. Also, thank you for reading so deeply in our paper—and in its footnotes. *See also* James Grimmelmann, *When All You Have Is a Fiduciary*, LAW & POL. ECON. PROJECT (May 30, 2019), https://lpeproject.org/blog/when-all-you-have-is-a-fiduciary [https://perma.cc/V5PB-4D6B] (arguing that when applied to digital platforms "the rule against self-dealing is either absurdly under-inclusive, absurdly over-inclusive, or both").

57 We propose that lawmakers adapt language from the Consumer Financial Protection Bureau's authority to regulate abusive trade practices along these lines: "Abusive trade practice" means any conduct by a covered entity that 1) materially interferes with the ability of a trusting party to understand a term or condition of the agreement between covered entities and trusting party relating to the processing of personal data or effect or functionality of a system, tool, or user interface deployed by the covered entity; or 2) takes unreasonable advantage of: a) a lack of understanding on the part of the trusting party of the material risks, costs, or conditions of the covered entity's product or service; or b) the inability of the trusting parties to protect their interests in selecting or using a covered entity's product or service; or c) the reasonable reliance by the trusting party on a covered entity's representation to act in the interests of the trusting party.

parties to protect their interests within the relationship. Finally, anti-abuse rules would prohibit entrustees from taking unreasonable advantage of the reasonable reliance by trusting parties on entrustees' representations to act in the trusting parties' interests.

Lawmakers might also consider rigid prohibitions on specific practices like the deployment of unreasonably dangerous automated tools or the use of personal data to train those automated systems. They could create subsidiary rules for inherently dangerous practices and technologies that, at the systemic level, are in fundamental conflict with the best interests of trusting parties, such as microtargeting, a practice that paves the path for third party abuse and imposes more externalities than benefits for trusting parties; and affect recognition, a fundamentally misguided, mistaken, and oppressive tool.[58] Lawmakers could craft even more rules designed for specific parties such as "social media platforms may not deploy affect recognition technologies on photos or videos submitted by trusting parties." There might also be disclosure mandates, process requirements, prohibitions on conduct, or obligated tasks. Each rule should target specific areas where trusted parties have an incentive to engage in self-dealing.[59]

Lawmakers could, of course, impose all these rules even without couching them within an umbrella duty of loyalty. We have proposed in previous research that trust-building and trust-enforcing rules irrespective of a relationship between the parties could be meaningful complements or the next best thing to broad and strong relational obligations.[60] Many of these rules, such as data protection obligations, should have sibling rules that apply regardless of whether data controllers are in an information relationship with a trusting party. But we believe that a duty of loyalty would act as an important animating force, interpretive guide, and catchall provision that would bring more coherence, flexibility, and accountability through enforcement than these rules would have as stand-alone laws.

Nonetheless, we propose specific subsidiary rules within information relationships to maximize the advantages of a relational approach to privacy. Scholars and lawmakers have identified different contexts where the incentives for self-dealing by the powerful party in

---

58 For an exploration on the dangers of affect recognition systems see, e.g., KATE CRAWFORD, ATLAS OF AI (2021); Kate Crawford, *Artificial Intelligence Is Misreading Human Emotion*, THE ATLANTIC (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/ [https://perma.cc/T6AV-J25T]; LUKE STARK & JESSE HOEY, THE ETHICS OF EMOTION IN ARTIFICIAL INTELLIGENCE SYSTEMS (2021).

59 *See* Andrew S. Gold, *The Fiduciary Duty of Loyalty*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 36, at 401 ("Different opportunism risks will then justify different loyalty content and approaches to legal decision-making.").

60 *See* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 5.

an information relationship are overwhelming, making these contexts ripe for subsidiary data loyalty rules.[61] We synthesize these contexts into five main areas: Entrustees should be loyal when *collecting* information, being sure to collect only information for purposes that do not conflict with a trusting party's best interests. Entrusees should be loyal when *personalizing*, i.e., treating people differently based upon personal information or characteristics. Entrustees should be loyal *gatekeepers*, avoiding conflicts when allowing government and other third-party access to trusting parties and their data. Entrustees should be loyal when trying to *influence* trusting parties, such as when they leverage personal data and digital tools to exert sway over people to achieve particular results. Finally, entrustees should be loyal in the ways they *mediate* interactions between users of their platform, specifically in the creation and administration of systems that govern how people are allowed to interact with each other. These contexts often overlap and involve issues like discriminatory microtargeting, harmful amplification of misinformation, failure of process for content moderation, and abusive dark patterns. We propose that lawmakers create subsidiary loyalty rules and standards to mitigate these kinds of disloyal behaviors.

1. Loyal Collection

A duty of loyalty should attach the moment a trusted party invites disclosure and makes the decision to collect personal information. In this way, data loyalty could embolden the fair information principle of data minimization. This principle holds that data collectors should only identify the minimum amount of personal information needed to fulfill a legitimate purpose and collection and hold that much information and no more.[62] Combined with the storage limitation principle, which holds that organizations should not keep data longer than they need it for their stated purpose, data minimization is a central pillar in data protection regimes around the world, but it too often fails to find traction.[63]

61 *See, e.g.*, Balkin, *The Fiduciary Model*, *supra* note 3; Scholz, *supra* note 3, at 197; Dobkin, *supra* note 3, at 17 (identifying four major ways of breaching an information fiduciary duty: "manipulation, discrimination, third-party sharing, and violating a company's own privacy policy"); Barrett, *supra* note 3, at 1100 ("[A]n information fiduciary framework should also address manipulation and discrimination in order to ensure that people are protected from the full array of modern digital threats that they face.").

62 *See Principle (c): Data Minimisation*, INFO. COMM'RS OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/#data_minimisation [https://perma.cc/6TTU-BJ8H].

63 *See id.*; Council Regulation 2016/679, art. 5(e) 2016 O.J. (L 119) 1 (EU) (providing the GDPR's storage limitation principle).

Data loyalty could provide a normative vision for when companies have exceeded their duty to minimize collection and retention—when it conflicts with a trusting party's (or collective trusting parties') best interests. Under general data protection frameworks that impose data minimization requirements, organizations must typically ensure that the data they are processing is adequate (sufficient to fulfil the stated purpose), relevant (has a relevant link to that purpose), and limited to what is necessary (collecting and holding only that which is needed for that purpose).[64] A duty of loyalty could provide a value-laden baseline that requires an examination of not just the purpose of the collection but also elevates the interests of those affected by the collection. While parties at an arm's length might act opportunistically in collecting as much data as possible, trusted parties remain loyal by leaving all data that, if collected, would conflict with the trusting parties' best interests on the table.

2. Loyal Personalization

The modern Internet routinely and systemically treats people differently based upon personal information or characteristics. Targeted and behavioral advertising is the most prominent example of this, but first-party product and streaming recommendations, news feeds, default settings, layouts, and more are all designed automatically to look and act differently based on people's personal characteristics. Some of this personalization, such as targeted recommendations for networked connections based upon intentionally revealed data such as where you work or attended high school, would probably be loyal. Other personalization systems, however, such as those that wrongfully discriminate or have a disparate impact on protected, marginalized, or vulnerable groups of people, would likely conflict with that trusting collective's best interests. Subsidiary rules built around the concept of loyal personalization could firmly and clearly address a systemic problem in a way that traditional data protection frameworks have been unable to mitigate.

3. Loyal Gatekeeping

Entrustees have a remarkable ability to facilitate third party access to trusting parties and their data. They can do so through their APIs, advertiser portals, fusion centers, and government backdoors. This access is the source of most major platforms' power. And everyone wants a piece of the users. Advertisers clamor for their attention. Data brokers and companies training AI models lust for their data. And

64 Council Regulation 2016/679, art. 5(c) 2016 O.J. (L 119) 1 (EU) (providing the GDPR's data minimization principle).

governments demand evidence. Entrustees have financial incentives to build portals and facilitate access for third parties. Some access granted by trustees to third parties is not in conflict with trusting parties' best interests. For example, contextual advertising usually doesn't significantly leverage people's own data or limitations against them, nor does it usually expose trusting parties to significant privacy harms. Protocols for interoperability to help people transfer data from one place to another also serve the interests (and wishes) of trusting parties.

However, certain lax gatekeeping practices would be disloyal because of how they endanger trusting parties by obscuring risk and breaking promises while facilitating access to third parties for organizational gains or to avoid costs. The three most resonant privacy scandals in the past decade, the government surveillance revelations by Edward Snowden, the FBI's request that Apple help it bypass encryption protections, and Cambridge Analytica's massive Facebook data exfiltration, all involved gatekeeping issues. Subsidiary rules built around the concept of loyal gatekeeping would help resolve longstanding debates around what obligations trusted organizations have regarding third-party access through portals, APIs, interfaces, and the automated scraping of websites. And in combination with a duty of confidentiality, subsidiary rules could also help clarify when sharing a trusting party's data with third parties is disloyal.

4. Loyal Influencing

Technologies are artifacts built to act upon the world. Every single design decision made in the creation of a website or app is meant to facilitate a particular kind of behavior.[65] The structure of digital technologies will affect people's choices even if the effect is not intended by designers. When designers create a drop-down menu, privacy settings, "I agree" buttons, and any other feature that implicates people's privacy, they are influencing them. They can't avoid it.[66] Given their power, they should be loyal in exercising their influence.

The most prominent example of disloyal influence involves organizations leveraging "dark patterns" or "malicious interfaces"

65 *See, e.g.*, LANGDON WINNER, THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY 94 (1986).

66 *See* Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. ON REGUL. 413, 421 (2015) ("Human beings . . . cannot wish [choice architecture] away. Any store has a design; some products are seen first, and others are not. Any menu places options at various locations. Television stations come with different numbers, and strikingly, numbers matter, even when the costs of switching are vanishingly low; people tend to choose the station at the lower number, so that channel 3 will obtain more viewers than channel 53.").

which are user interface elements meant to influence a person's behavior against their intentions or best interests.[67] Companies deploy effort traps to make deleting an account confusing and difficult. They make "cancel" buttons hard to see and press, they obscure important details in tiny fonts or walls of boilerplate, and they leverage our deeply entrenched and empirically validated overconfidence regarding risk, deference for conformity, endowment effects, status quo bias, and other biases and mental shortcuts to manipulate us to their ends. Jamie Luguri and Lior Strahilevitz have observed that "dark patterns are strikingly effective in getting consumers to do what they would not do when confronted with more neutral user interfaces."[68]

---

67 *See, e.g.*, HARTZOG, *supra* note 22, at 148, 162; Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43 (2021); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Gregory Conti & Edward Sobiesk, *Malcious Interfaces and Personalization's Uninviting Future*, IEEE PRIV. & SEC., May/June 2009, at 72, 73; JOHANNA GUNAWAN, DAVID CHOFFNES, WOODROW HARTZOG & CHRISTO WILSON, TOWARDS AN UNDERSTANDING OF DARK PATTERN PRIVACY HARMS (2021); Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, A LIST APART (Nov. 1, 2011), https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/ [https://perma.cc/4VBK-HEEG]; COLIN M. GRAY, YUBO KOU, BRYAN BATTLES, JOSEPH HOGGATT & AUSTIN L. TOOMBS, THE DARK (PATTERNS) SIDE OF UX DESIGN (2018); Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROCEEDINGS ACM HUM.-COMPUT. INTERACTION 81 (2019); ARUNESH MATHUR, JONATHAN MAYER & MIHIR KSHIRSAGAR, WHAT MAKES A DARK PATTERN. . . DARK? (2021); Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp & Stefan Pfattheicher, *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, 4 PROC. ON PRIV. ENHANCING TECHS. 237, 248 (2016); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OP. PSYCH. 105, 105, 107–09 (2020).

68 Luguri & Strahilevitz, *supra* note 67, at 46 (emphasis omitted). Luguri and Strahilevitz found that

> [r]elatively mild dark patterns more than doubled the percentage of consumers who signed up for a dubious identity theft protection service, which we told our subjects we were selling, and aggressive dark patterns nearly quadrupled the percentage of consumers signing up. In social science terms, the magnitudes of these treatment effects are enormous.

Id. They further found that

> the most effective dark pattern strategies were hidden information (smaller print in a less visually prominent location), obstruction (making users jump through unnecessary hoops to reject a service), trick questions (intentionally confusing prompts), and social proof (efforts to generate a bandwagon effect). Other effective strategies included loaded questions and making acceptance the default. . . . In many cases, consumers exposed to dark patterns did not understand that they had signed up for a costly service. These results confirm the problematic nature of dark patterns and can help regulators and other watchdogs establish enforcement priorities.

Id. at 47.

Lawmakers have struggled for years to articulate when attempts at persuasion become harmful.[69] But trusting parties do not need to be injured for entrustees to violate a duty of loyalty. Subsidiary rules around disloyal attempts to influence would address the most pernicious and dangerous dark patterns head-on.[70] Lawmakers should focus on how the design is meant to take advantage of a person's limitations or vulnerabilities to benefit the designer in a way that is against the best interests of the trusting party.[71]

5. Loyal Mediation

Certain kinds of organizations design their platforms so that their users interact not just with the organization itself, but with each other. In other words, they mediate people's social and market experiences with other people using their service. Sometimes this is a great experience for people who use these services. But things can go off the rails quickly as companies feel pressured to achieve continual and endless growth. They create systems that reward virality and the most outrageous or venomous hot takes instead of the ostensible purpose of meaningful social interaction and social, emotional, and intellectual nourishment. They optimize their algorithms and interfaces to reward our most impulsive and petty reactions. Amplification of certain kinds of information combined with strategically reduced or increased transaction costs to speak, report harmful and dangerous speech, and hide from other users leads to acute individual harms like harassment[72]

69 *See id.* at 104; *see also* Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in A Digital World*, 4 GEO. L. TECH. REV. 1, 3 (2019) ("[A]t its core, manipulation is hidden influence—the covert subversion of another person's decision-making power. In contrast with persuasion, which is the forthright appeal to another person's decision-making power, or coercion, which is the restriction of acceptable options from which another person might choose, manipulation functions by exploiting the manipulee's cognitive (or affective) weaknesses and vulnerabilities in order to steer his or her decision-making process towards the manipulator's ends.").

70 Luguri and Strahilevitz recommend a multi-factor test to help determine when dark patterns cross the line

> that looks to considerations such as (i) evidence of a defendant's malicious intent or knowledge of detrimental aspects of the user interface's design, (ii) whether vulnerable populations—like less educated consumers, the elderly, or people suffering from chronic medical conditions—are particularly susceptible to the dark pattern, and (iii) the magnitude of the costs and benefits produced by the dark pattern.

Luguri & Strahilevitz, *supra* note 67, at 99.

71 Balkin has proposed looking to "techniques of persuasion and influence that (1) prey on another person's emotional vulnerabilities and lack of knowledge (2) to benefit oneself or one's allies and (3) reduce the welfare of the other person." JACK M. BALKIN, HOOVER INST., FIXING SOCIAL MEDIA'S GRAND BARGAIN 4 (2018).

72 *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014).

as well as systemic harms like polarization, reduced ability to engage in self-governance, negative public health outcomes, and chilling effects for large groups of vulnerable users.

A duty of loyalty cannot solve all of the complex problems of content moderation or harassment. As we have maintained, a duty of loyalty is merely one important tool in a larger toolkit. But companies do have remarkable power to influence how people using their systems interact with each other.[73] When they use this power in a way that conflicts with the best interests of their users in order to optimize growth, they are being disloyal. Subsidiary rules for loyal mediation are, of course, complicated because of the potentially conflicting interests amongst actors and those potentially adversely affected by the act. One trusting party wants to speak while the other(s) is made worse because of it. This is where our proposed systemic focus and the traditional fiduciary law method of developing a hierarchy of loyalties would help clarify lawmakers' actions.

CONCLUSION

Duties of data loyalty will take time and effort to meaningfully implement as a part of U.S. privacy law. Data loyalty is a significant and necessary departure from privacy law's ineffective notice and consent approach. But lawmakers can confidently embrace loyalty and other relational duties as part of a holistic approach to mitigating the power and abuses of data collectors. If done clearly, carefully, and with commitment, lawmakers can chart a bold new vision for our privacy rules that is capable of nurturing a sustainable and flourishing future for those who share their personal information as well as those entrusted with it.

73 *Id.* at 25; *see also* Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 5, at 1695.