

2022

Comments of the Cordell Institute on the Prevalence of Commercial Surveillance and Data Security Practices that Harm Consumers

Neil M. Richards


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

Woodrow Hartzog

Boston University School of Law

Jordan Francis

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

 Part of the [Legal Studies Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Repository Citation

Richards, Neil M.; Hartzog, Woodrow; and Francis, Jordan, "Comments of the Cordell Institute on the Prevalence of Commercial Surveillance and Data Security Practices that Harm Consumers" (2022). *Scholarship@WashULaw*. 498.
https://openscholarship.wustl.edu/law_scholarship/498

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

**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 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, 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, we²⁴ 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 Knows 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/metav-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 state⁷²—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, loses⁷⁶, and leaks⁷⁷ 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.cnn.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); *see 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/2009/03/090305rrscmp.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 data¹⁹⁸ 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.* 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 235 (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 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 advertisement²⁶⁷—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); *see 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 be 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%94people-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 our 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 274,274 (“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 318,318.

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 keystrokes³⁴⁰ 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, unavailability, 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 Nyrop & 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 a 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).