Stanford Law Review

Volume 77 June 2025

FEATURE

After Notice and Choice: Reinvigorating "Unfairness" to Rein In Data Abuses

Lina M. Khan, Samuel A.A. Levine & Stephanie T. Nguyen*

Abstract. The Federal Trade Commission (FTC) has long served as America's default privacy enforcer. Yet for much of its history, the agency relied on self-regulation through a "notice and choice" framework that left the public vulnerable in an era of rampant data collection and digital surveillance. Businesses overwhelmed users with dense privacy notices while amassing and exploiting vast troves of personal data. The agency's historical approach, rooted in outdated assumptions about self-correcting markets and an ideologically cramped view of the FTC's authorities and mandate, helped usher in a digital economy where data abuses became routine.

During the Biden Administration, the FTC charted a new course, rejecting disclosure-based frameworks in favor of substantive protections. Through major enforcement actions, new rulemaking initiatives, and internal capacity-building, the agency advanced significant measures to curb harmful data practices. These efforts included restricting excessive collection of data, establishing bright-line limits on the dissemination of sensitive data, targeting manipulative "dark patterns," expanding protections for children and teens, and crafting remedies to deter illegal data practices. By addressing upstream drivers of data abuses rather than just responding to downstream harms, the FTC spurred changes in how businesses collect, disseminate, and use Americans' personal data, while demonstrating that the agency's existing tools—especially its authority to prohibit "unfair" practices—can be deployed effectively to rein in digital abuses.

This Feature examines the paradigm shift underlying the FTC's new approach to consumer protection in the digital age. First, it situates this pivot by tracing the history, descriptive assumptions, and ideological tenets that shaped the agency's prior "notice and choice" framework. Second, it maps out the enforcement principles that animated the FTC's recent shift, examines the agency's revival of its "unfairness" authority, and explains

* Lina Khan served as Chair of the Federal Trade Commission from June 2021 through January 2025; she is presently an associate professor of law at Columbia Law School. Samuel Levine served as Director of the Bureau of Consumer Protection under Chair Khan, and Stephanie Nguyen served as the FTC's Chief Technologist. We are grateful to Daniel Zhao for his substantial assistance in drafting this Feature and to Ben Wiseman and Aaron Alva for insightful discussion and feedback. Many thanks also to the editors of the *Stanford Law Review* for their thoughtful engagement and excellent editorial assistance.

how recent agency actions across multiple domains illustrate this new approach. While the change in administration brings uncertainty about the agency's direction, the FTC's recent work has laid out a durable blueprint for substantive consumer protection in the digital age. Several of the reforms and programmatic advances have garnered rare bipartisan support at the FTC, in Congress, and in the states, building momentum toward a lasting shift away from disclosure-based regimes.

Table of Contents

Introduction

The United States is the only advanced economy in the world with no comprehensive law protecting people's online privacy.[1] This void has left Americans living under a regime often called "notice and consent"[2] or "notice and choice."[3] The concept is straightforward: Businesses and other providers of online services disclose what information they collect and how they intend to use it, and consumers can choose whether they want to use the service.[4]

While potentially appealing in theory, this model has failed in practice. A privacy regime that relies on notice falls short for several reasons. First, it places an outsized burden on individual users, forcing them to evaluate the fine print of lengthy privacy notices for their devices, applications, and digital services. These notices are often vague and ineffectively convey risk, even for careful readers—and they can be outright impenetrable to the average user.[5]

---

1. Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?*, N.Y. TIMES (Nov. 2, 2019), https://perma.cc/7MGY-UAE9. This absence stands in stark contrast with data protection regimes in peer nations, such as the European Union's General Data Protection Regulation. *See* Council Regulation 2016/679, 2016 O.J. (L 119) 1. Lacking a unified federal framework, individual states like California and Colorado have begun implementing their own privacy protection legislation. California Consumer Privacy Act, 2018 Cal. Stat. 1807 (codified at CAL. CIV. CODE §§ 1798.100-1798.199.100 (West 2023)); Colorado Privacy Act, 2021 Colo. Sess. Laws 3445 (codified at COLO. REV. STAT. §§ 6-1-1301 to 6-1-1314 (2024)).

2. *See, e.g.*, JOSEPH TUROW, YPHTACH LELKES, NORA A. DRAPER & ARI EZRA WALDMAN, AMERICANS CAN'T CONSENT TO COMPANIES' USE OF THEIR DATA 3 (2023), https://perma.cc/626H-KZLU ("In the European Union, consent must be explicit; a person must 'opt in' to allowing their data to be used. In the U.S., by contrast, FTC oversight and state laws allow consent to be implicit in most cases. That is, as long as privacy policies reveal what the company is doing with consumers' data, taking and using that data—and even selling it—is acceptable. Many privacy policies allow individuals to 'opt out' of these activities, often tying to an industrywide 'ad choices' framework that purports to facilitate this activity, but doing so is actually quite complex.").

3. Scott Jordan, *A Proposal for Notice and Choice Requirements of a New Consumer Privacy Law*, 74 FED. COMMC'NS L.J. 251, 254 (2022).

4. *See, e.g.*, TUROW ET AL., *supra* note 2, at 3 ("As a result, much privacy law still relies on industry self-regulation and individual privacy self-management: companies post privacy policies that detail the information they collect and individual consumers are tasked with reading and understanding these policies and making decisions about whether to use a website. This regime is known as 'notice-and-consent.'"); Andrew Perrin, *Half of Americans Have Decided Not to Use a Product or Service Because of Privacy Concerns*, PEW RSCH. CTR. (Apr. 14, 2020), https://perma.cc/8MM9-XJ48 (finding that approximately "half (52%) of U.S. adults said they decided recently not to use a product or service because they were worried about how much personal information would be collected about them").

5. *See, e.g.*, COLLEEN MCCLAIN, MICHELLE FAVERIO, MONICA ANDERSON & EUGENIE PARK, HOW AMERICANS VIEW DATA PRIVACY 27 (2023), https://perma.cc/QKZ9-DNJG

footnote continued on next page

Furthermore, it is unreasonable to expect users to grasp the intricacies of a corporation's algorithmic data practices and to anticipate how those practices could affect their lives today and in the future. Even in the rare cases when notices are relatively straightforward, the notices might simply inform people that the business is already collecting and using vast troves of their data however it pleases.[6] Businesses often change notices on a whim,[7] putting users in the untenable situation of having to constantly monitor their products and services for amended terms.

Another weakness of notice-based regimes is that many of the entities involved in the collection, aggregation, and monetization of personal data are not consumer-facing.[8] Individual users know very little about the practices of first-party platforms that share and sell data to data brokers and third-party companies who collect, aggregate, and buy their data, or who build consumer profiles based on inferences from this data.[9] Data brokers are the middlemen of the commercial surveillance ecosystem, and the notice-and-choice regime unreasonably burdens users with the Sisyphean task of scrutinizing a shadowy industry they may not even know exists.

Even if individuals could somehow overcome these obstacles, seldom can they do anything about them. For most users, the "choice" presented is whether to accept a company's terms of service or forego the service altogether. Yet digital products and services are increasingly essential for navigating day-to-day life. Daily tasks ranging from searching for a new doctor to paying rent now effectively require use of online services. The prevailing "notice-and-

(finding that "[r]oughly six-in-ten adults (61%) say privacy policies are not too or not at all effective for communicating how companies are using people's data").

6. Consumer sentiment reflects the limitations of the notice-and-consent regime. Pew found that "a majority say they're skeptical anything they do [to manage online privacy] will make much difference. And only about one-in-five are confident that those who have their personal information will treat it responsibly." *Id.* at 7.

7. In February 2024, responding to growing concerns around this practice, the FTC published a blog post noting that firms may risk violating the law when they revise privacy policies to retroactively change how consumer data is used. Off. of Tech. & Div. of Priv. & Identity Prot., *AI (and Other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive*, FTC: TECH. BLOG (Feb. 13, 2024), https://perma.cc/992U-VMB3.

8. *See* JUSTIN SHERMAN, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS: THREATS TO AMERICAN CIVIL RIGHTS, NATIONAL SECURITY, AND DEMOCRACY 2 (2021), https://perma.cc/55UE-2ETU; *see also Data Brokers*, ELEC. PRIV. INFO. CTR., https://perma.cc/7NT2-84AF (archived Apr. 29, 2025).

9. *See Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FTC: TECH. BLOG (Mar. 16, 2023), https://perma.cc/5MUP-FAMU.

consent" framework thus gives people a false choice: forego one's privacy or forego participating in modern life.[10]

Although the status quo may seem bleak, this Feature argues that we are now witnessing a new paradigm for consumer protection. The Feature focuses on the Federal Trade Commission (FTC), which has long acted as the de facto privacy enforcer in the United States.[11] For many years, the FTC embraced notice and choice, and in key moments even championed "self-regulation" by business over efforts by Congress to pass comprehensive legislation.[12] But during the Biden Administration, the agency set out on a new path—using its enforcement and rulemaking tools to secure baseline protections around the collection and use of people's data, combat harmful online interfaces, protect children and teenagers online, and ensure effective relief and accountability when data is abused. A throughline across these efforts is aligning law enforcement with the realities of how digital markets work and a focus on substantive protections over procedural ones.[13]

This Feature fills an important gap in the literature. The history of the FTC's privacy enforcement and the agency's key role in shaping data protection norms have been well-documented by leading scholars such as Daniel Solove, Woodrow Hartzog, and Chris Hoofnagle.[14] This Feature situates the FTC's approach to data privacy in a broader context, arguing that the agency's early embrace of online self-regulation was a direct consequence of the Reagan era, when FTC leadership adopted a hands-off approach to protecting Americans from illegal business practices. Only in recent years, the Feature argues, has the agency started to depart from this approach, revisiting flawed assumptions and harnessing the FTC's full set of tools to promote fair, honest, and competitive markets. While this reorientation has spanned the full breadth of the FTC's work, the agency's new approach to consumer protection in digital markets is at the forefront of the effort.

---

10. Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, NEW AM. (Mar. 23, 2020), https://perma.cc/7UKK-BGE3.

11. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014).

12. Chris Jay Hoofnagle, *Privacy Self-Regulation: A Decade of Disappointment*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 379, 380 (Jane K. Winn ed., 2006).

13. For an account of the distinction between substantive and procedural privacy protections, see Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1695 (2020) ("[Federal Information Processing Standards] regimes conceive of fair data processing as an eternally virtuous goal, which has the consequence of normalizing surveillance, processing, and procedural rules at the cost of more substantive protections.").

14. *See, e.g.*, Solove & Hartzog, *supra* note 11; CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016).

This Feature proceeds in three Parts. Part I recounts how the FTC has shaped U.S. data privacy practices since the mid-1990s. Drawing on primary sources as well as the work of leading scholars, the Feature lays out the agency's embrace of self-regulation in the 1990s, as well as its efforts to block privacy legislation in the early 2000s. The Feature also traces this hands-off approach to the ideological revolution that took place at the agency in the early 1980s. The Commission at that time adopted a radically diminished view of the government's role in policing markets, believing that markets were prone to self-correct and that consumer protection should be mostly limited to prohibiting outright fraud and lies. One practical effect of this shift was the Commission's retreat from using its authority to combat *unfair* practices—arguably its strongest tool to protect the public. The agency instead mostly turned its focus to policing *deceptive* practices. This approach, which has prevailed for the last several decades, focused on whether claims that businesses made were misleading, rather than whether their practices harmed people.

Part II details how the FTC has driven a significant paradigm shift during the Biden Administration. For the first time, the agency expressly disavowed notice and choice and is instead deploying its unfairness authority and other tools to prohibit harmful online practices, rather than simply require better disclosures. In particular, the agency has worked to limit overcollection and oversharing of people's data, challenge manipulative online interfaces, secure stronger online protections for children and teenagers, and ensure deterrence against data abuses.

Although this shift has been observed by lawyers and journalists,[15] it has largely gone unaddressed in academic scholarship. This Feature, whose authors held leadership roles at the agency from 2021 to 2025, aims to fill that gap by drawing a throughline across cases, rules, market studies, and other initiatives to explain how the FTC has advanced a new paradigm for consumer protection. While this Feature focuses on the FTC's work in digital markets, the paradigm shift extends across the agency's consumer protection work.[16]

Part III focuses on how this paradigm shift has been implemented and sustained in practice through institutional changes within the agency. In particular, this Part highlights the type of foundational infrastructure—including the mandate, organization, and staffing—that is critical to delivering durable benefits. A core priority has been bolstering one of the FTC's most valuable resources: staff with technical expertise who help the agency stay

15. *See, e.g.*, Singer, *infra* note 223; Weissman, *infra* note 623; Yuan & Swift, *infra* note 361.

16. *See* Luke Herrine, *Unfairness, Reconstructed*, 130 YALE J. ON REGUL. 95, 118-27 (2025) (observing the FTC's recent embrace of its unfairness authority across its consumer protection portfolio).

nimble as markets evolve. Looking forward, this Part aims to highlight a model for government agencies to ensure that enforcers can keep pace with rapidly developing technologies.[17]

I. The FTC's Historical Impact on U.S. Privacy Enforcement

The FTC is a small agency with a vast jurisdiction, charged by Congress to root out unfair or deceptive practices and unfair methods of competition across most sectors of the economy.[18] The FTC's enforcement portfolio is broad, spanning actions targeting illegal schemes to inflate the price of lifesaving drugs[19] to actions targeting scams that cheat people out of millions of dollars.[20] This Feature focuses on a specific aspect of the agency's work—its effort to protect online privacy in the face of expansive commercial surveillance practices.[21]

One might ask why privacy matters, especially when the FTC is tasked with addressing so many other pressing concerns. But protecting people's privacy is fundamentally about protecting their liberties. This is well understood in the context of government surveillance, with a constitutional amendment protecting against undue government intrusion.[22] But concerns

17. *Government Agencies Act to Elevate and Build Tech and Digital Capacity*, FTC: TECH. BLOG (Mar. 26, 2024), https://perma.cc/F8VQ-Z42W (including a report highlighting the FTC's Office of Technology as a case study for digital capacity building).

18. Memorandum from the FTC, A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority (updated May 2021), https://perma.cc/BR8K-ZC9L (explaining the FTC's primary enforcement authorities).

19. FTC v. Vyera Pharms., LLC, 479 F. Supp. 3d 31, 39 (S.D.N.Y. 2020). In *FTC v. Vyera Pharmaceuticals, LLC*, efforts to forestall generic competition to the market meant that consumers experienced price-gouging and often an inability to afford needed medications. *Id.*; *FTC Sues Prescription Drug Middlemen for Artificially Inflating Insulin Drug Prices*, FTC (Sept. 20, 2024), https://perma.cc/R427-QXKH.

20. Complaint for Permanent Injunction & Monetary Judgments for Civil Penalties & Consumer Redress, & Other Relief at 2-3, United States v. Burgerim Grp. USA, Inc., No. 22-CV-825 (C.D. Cal. Feb. 7, 2022).

21. We have explained that the term "surveillance" describes the pervasive and comprehensive tracking of consumers' movements and behaviors across virtually every aspect of our daily lives. This surveillance results in the collection and aggregation of sensitive and other personal data from disparate sources and contexts to create detailed consumer profiles that commercial entities monetize and use to make inferences and determinations about consumers, frequently without our knowledge or permission and, far too often, resulting in disparate impacts on racial minority groups or other protected classes. FTC, Cleveland-Marshall College of Law Cybersecurity and Privacy Protection Conference: Keynote Remarks of Samuel Levine, Dir., Bureau of Consumer Prot., FTC 1-4 (May 19, 2022), https://perma.cc/7J39-7GH4.

22. U.S. CONST. amend. IV; *see also* Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2513 (2021).

about *commercial* surveillance have historically been seen as distinct.[23] This has been especially true in the context of commercial transactions where consumers submit their personal information to gain access to a product—such as when consumers make their credit history available to secure a loan.[24]

But the economy has changed. The 1990s marked the dawn of the internet with the first generation of the World Wide Web, where businesses first began commercializing access to online information.[25] The 2010s saw the dramatic growth of digital platforms, where firms exploited network effects and data feedback loops to accelerate their growth—and where firms opted for business models premised on monetizing users through extensive data collection in exchange for "free" services.[26] About a decade later, firms are sprinting to train generative artificial intelligence (AI) models on troves of the public's data,[27] now offering generative AI-enabled products and services to tens of millions of users[28]—many of which are trained on massive amounts of the public's data.

In this environment, commercial surveillance has become so widespread and pervasive that it can no longer be thought of in terms of a discrete set of transactions to which consumers can knowingly consent.[29] Today, consumers are tracked constantly, often unknowingly and through multiple platforms.

---

23. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1958 (2013) ("One of the most significant changes that the age of surveillance has brought about is the increasing difficulty of separating surveillance by governments from that by commercial entities. Public- and private-sector surveillance are intertwined—they use the same technologies and techniques, they operate through a variety of public/private partnerships, and their digital fruits can easily cross the public/private divide. It is probably in this respect that our existing models for understanding surveillance—such as Big Brother and the Panopticon—are the most out of date. Even if we are primarily worried about state surveillance, perhaps because we fear the state's powers of criminal enforcement, our solutions to the problem of surveillance can no longer be confined to regulation of government actors. Any solutions to the problem of surveillance must thus take into account private surveillance as well as public.").

24. J. Howard Beales & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 116 (2008).

25. *See, e.g.*, MARGARET O'MARA, THE CODE: SILICON VALLEY AND THE REMAKING OF AMERICA 287-91 (2019).

26. Lina M. Khan, Opinion, *We Must Regulate A.I. Here's How*, N.Y. TIMES (May 3, 2023), https://perma.cc/VA3K-RHQ3.

27. *See* Sara Morrison, *The Tricky Truth About How Generative AI Uses Your Data*, VOX (July 27, 2023, 4:15 AM PDT), https://perma.cc/V9JS-63VR.

28. Krystal Hu, *ChatGPT Sets Record for Fastest-Growing User Base—Analyst Note*, REUTERS (Feb. 2, 2023, 7:33 AM PST), https://perma.cc/2BF9-GWK3.

29. TUROW ET AL., *supra* note 2, at 18 (noting that "downstream uses of consumer data are multiplying and diversifying" such that informed consumer consent is all but impossible).

Our phones,[30] fitness apps,[31] healthcare appointments,[32] smart devices,[33] and even cars[34] can track our information. These devices or platforms can expose our private actions, choices, and movements to employers,[35] bank lenders,[36] advertisers,[37] corporations,[38] or anyone willing to pay.[39] With commercial surveillance, the risk to people goes beyond the exposure of any single piece of personal information.

Although privacy is paramount for people's core liberties, the United States is among the only countries in the world without a comprehensive privacy law. The FTC has attempted to fill that void.[40] In a 2014 article, Solove and Hartzog trace how the FTC emerged as the country's de facto data protection authority.[41] They note that in the 1970s, Congress gave the FTC responsibility for one of the first-ever privacy laws: the Fair Credit Reporting Act.[42] In the decades since, Congress has given the FTC other formal privacy responsibilities, including enforcement of the Children's Online Privacy Protection Act and the Gramm-Leach Bliley (GLB) Act.[43]

30. Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, MARKUP (updated Sept. 30, 2021, 3:51 PM ET), https://perma.cc/K6CE-E62N.

31. Martin Giles, *Another Fitness App Reveals Data That Can Be Used to Identify Soldiers and Spies*, MIT TECH. REV. (July 9, 2018), https://perma.cc/W5K7-9JSU.

32. Donna M. Christensen, Jim Manley & Jason Resendez, *Medical Algorithms Are Failing Communities of Color*, HEALTH AFFS. (Sept. 9, 2021), https://perma.cc/CY8H-FQYL.

33. Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FTC: BUS. BLOG (July 11, 2022), https://perma.cc/JMP2-5U2F.

34. *Id.*

35. Ifeoma Ajunwa, *The "Black Box" at Work*, BIG DATA & SOC'Y, July 2020, at 2-3.

36. Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, MARKUP (Aug. 25, 2021, 6:50 AM ET), https://perma.cc/D3ZD-TKC6.

37. Alex P. Miller & Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias*, HARV. BUS. REV. (Nov. 8, 2019), https://perma.cc/MCD4-ZK7D.

38. *Your Data Is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE WHARTON (Oct. 28, 2019), https://perma.cc/4N2V-JCFU.

39. Alfred Ng & Maddy Varner, *The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress*, MARKUP (Apr. 21, 2021, 8:00 AM ET), https://perma.cc/7DTS-TV9E.

40. *Enforcement of Privacy Laws*, ELEC. PRIV. INFO. CTR., https://perma.cc/ST5B-4CZ4 (archived Apr. 18, 2025).

41. Solove & Hartzog, *supra* note 11, at 600-06.

42. *Id.* at 602. The Fair Credit Reporting Act (FCRA) of 1970 was the first consumer privacy statute in the United States; it seeks to limit the use of personal information by consumer reporting agencies. Pub. L. No. 91-508, 84 Stat. 1114 (codified at 15 U.S.C. §§ 1681-1681x).

43. The Children's Online Privacy Protection Act, passed in 1998, directed the FTC to promulgate rules to put parents in control of information collected online from children under thirteen. Pub. L. No. 105-277, 112 Stat. 2681 (codified in relevant part at

footnote continued on next page

But it was not only formal authority that rendered the FTC the country's de facto privacy enforcer. An equally significant way in which the FTC cemented its role, Solove and Hartzog explain, is by "lending credibility to the self-regulatory approach."[44] Under a self-regulatory regime, businesses have no affirmative obligation to protect people's privacy; they can simply volunteer to adopt privacy policies. In theory, the FTC can then give this regime teeth by bringing enforcement actions against firms that do not honor their self-adopted privacy policies.[45] The FTC's embrace of this self-regulatory approach, Solove and Hartzog argue, helped cement the agency's role as a key privacy enforcer.[46]

This Part situates the FTC's embrace of self-regulation in the context of a broader ideological shift that took place at the agency in the early 1980s. For the most part, the agency's approach to online privacy was rooted in a vision of markets as self-correcting and an extremely thin conception of the government's role. [47] This Part details the FTC's actions during the 1990s and explains how a core set of assumptions led the agency to promote a hands-off approach to protecting people's data across presidential administrations.

A. Late 1990s: Embracing Self-Regulation

The late 1990s saw the Commission repeatedly and presciently sounding the alarm about how businesses were using people's online data, yet nevertheless disavowing the need for comprehensive privacy legislation.

In June of 1998, for example, the FTC issued a report calling on websites to embrace so-called Fair Information Practice Principles.[48] These principles generally centered on creating procedural requirements for firms to follow, rather than any substantive limits on how firms could collect, use, or retain people's data.[49] For example, the access principle would require that consumers

15 U.S.C. §§ 6501-6506). The Gramm-Leach Bliley Act, passed in 1999, directed the FTC and other agencies to issue regulations ensuring that financial institutions protect the privacy of consumers' personal financial information. *See* Pub. L. No. 106-102, 113 Stat. 1338 (codified in relevant part at 15 U.S.C. §§ 6801-6809, 6821-27).

44. Solove & Hartzog, *supra* note 11, at 604.

45. *Id.*

46. *Id.*

47. *See infra* notes 172-92 and accompanying text.

48. FTC, PRIVACY ONLINE: A REPORT TO CONGRESS, at ii (1998), https://perma.cc/S5S8-YC56 [hereinafter 1998 FTC PRIVACY REPORT]; *see also* Press Release, FTC, FTC Releases Report on Consumers' Online Privacy (June 4, 1998), https://perma.cc/QWF3-LEZX.

49. *See* 1998 FTC PRIVACY REPORT, *supra* note 48; *see also* Jordan Francis, *Unpacking the Shift Toward Substantive Data Minimization Rules in Proposed Legislation*, Int'l Ass'n Priv. Pros.

footnote continued on next page

be given reasonable access to information collected about them and the ability to correct such information, similar to processes available under the Fair Credit Reporting Act.[50] The security principle would require firms to take reasonable steps to safeguard data from unauthorized use.[51] And the enforcement principle would ensure enforcers could seek sanctions for noncompliance and that harmed parties could seek redress through a private cause of action.[52]

The report also detailed FTC staff analysis examining the extent to which websites were complying with the most fundamental fair information principle—notice.[53] The analysis found that only 14% of websites provided any information about their personal information practices and that only 2% included a comprehensive privacy policy.[54] Given these results, the Commission concluded that industry self-regulatory efforts were falling short.[55]

Despite recognizing these self-regulatory failures, the Commission did not push for major reforms or call on Congress to act. Instead, the Commission argued that a well-designed self-regulatory regime would be desirable and "could afford consumers adequate privacy protection."[56]

(May 22, 2024), https://perma.cc/6MZ7-8WYG (discussing the distinction between procedural versus substantive data minimization requirements).

50. *Compare* 1998 FTC PRIVACY REPORT, *supra* note 48, at 9 (defining access as "an individual's ability both to access data about him or herself—*i.e.*, to view the data in an entity's files—and to contest that data's accuracy and completeness"), *with* Fair Credit Reporting Act § 609, 15 U.S.C. § 1681g (stipulating that consumer reporting agencies must "clearly and accurately disclose to the consumer . . . [a]ll information in the consumer's file at the time of the request"), *and* Fair Credit Reporting Act § 611, 15 U.S.C. § 1681i (setting forth procedures for consumers to dispute the accuracy of credit reports).

51. 1998 FTC PRIVACY REPORT, *supra* note 48, at 10. Certain sector-specific laws affirmatively require companies to safeguard data, including the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b), for financial institutions and the Children's Online Privacy Protection Act, 15 U.S.C. § 6502, for children's data.

52. 1998 FTC PRIVACY REPORT, *supra* note 48, at 10-11.

53. *Id.* at ii-iii (noting that "[t]he Commission's survey of over 1,400 Web sites reveals that industry's efforts to encourage voluntary adoption of the most basic fair information practice principle—notice—have fallen far short of what is needed to protect consumers").

54. *Id.* at iii.

55. *Id.* at iv. The Commission took a notably more aggressive approach to issues around children's data. An FTC analysis found that many websites were collecting information about children without obtaining consent from their parents or even notifying them. The Commission called on Congress to "develop legislation to require commercial Web sites that collect personal identifying information from children 12 and under to provide actual notice to the parent and obtain parental consent." *Id.* at 43.

56. *Id.* at 41.

This approach became the norm during this period. The agency argued to Congress that "self-regulation is preferred to a detailed legislative mandate because of the rapidly evolving nature of the Internet and computer technology."[57] Simultaneously, however, the Commission also told Congress that self-regulation had failed to adequately protect consumer privacy.[58]

This posture continued into 1999. That year, the Commission issued another report finding that only a small percentage of the busiest websites indicated they were implementing basic principles of notice, choice, access, and security.[59] Yet the Commission again opposed legislation.[60] Self-regulation, the Commission maintained, remained "the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[61]

Although all five Commissioners supported the Commission's 1999 report, fissures were emerging. On one side, Commissioner Sheila Anthony issued a statement dissenting against the Commission's recommendation against legislation: "Notice, while an essential first step, is not enough if the privacy practices themselves are toothless. I believe that the time may be right for federal legislation to establish at least baseline minimum standards."[62]

On the other side of the debate, Commissioner Orson Swindle opposed regulation under any circumstances. He called for a three-year moratorium on online privacy regulation, arguing that it takes time for self-regulation to work. He criticized supporters of privacy legislation for "statist" thinking and argued consumers should protect themselves by avoiding websites with unsatisfactory privacy policies:

> If a consumer is uncomfortable with a Web site's privacy policy or if the site has no privacy policy for the consumer to review, then that individual has the freedom—and should have the good sense—to go elsewhere on the Web. The market, not the government, should determine whether companies are to be rewarded or punished for their privacy policies (or lack thereof) through a growth or lessening of electronic commercial transactions.[63]

---

57. *Consumer Privacy on the World Wide Web Before the Subcomm. on Telecomms., Trade & Consumer Prot. of the H. Comm. on Com.*, 105th Cong. (1998) (statement of Robert Pitofsky, Chairman, FTC), https://perma.cc/UL9V-W2K5.

58. Chairman Pitofsky's testimony noted that "an effective self-regulatory system has yet to emerge and that additional incentives are required in order to ensure that self-regulation is effective and consumer privacy is protected." *Id.*

59. FTC, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 6 (1999), https://perma.cc/7SMF-ATHX.

60. *Id.* at 12.

61. *Id.* at 6.

62. *Id.* attach. (Sheila F. Anthony, Comm'r, concurring in part and dissenting in part).

63. Orson Swindle, *Regulation of Privacy on the Internet: Where Do You Want to Go Today?*, FTC (Apr. 8, 1999), https://perma.cc/4CSZ-59AT.

Had the Commission taken a different approach by calling on Congress to pass legislation, the state of online privacy today might look very different. Consider the agency's impact on minors' privacy. In its June 1998 report, the Commission warned of serious privacy harms facing children online and called on Congress to pass basic protections.[64] Just four months later, Congress passed the landmark Children's Online Privacy Protection Act (COPPA).[65]

Among other measures, that legislation required firms to obtain parental consent to collect personal information from children,[66] to maintain procedures to protect the security of children's data they collect,[67] and to not condition children's access to services on collecting more information than is reasonably necessary.[68] COPPA also authorized the FTC to issue implementing regulations pursuant to the Administrative Procedure Act[69] and to seek civil penalties against violators.[70] State attorneys general were also given enforcement powers.[71]

Although COPPA has gaps that Congress continues to try to fill today,[72] the law's data minimization requirements,[73] requirement to maintain data

64. *See* 1998 FTC PRIVACY REPORT, *supra* note 48, at 42.

65. *See, e.g.*, Press Release, FTC, Children's Online Privacy Proposed Rule Issued by FTC (Apr. 20, 1999), https://perma.cc/6RNB-URHC.

66. 15 U.S.C. § 6502(b)(1)(A)(ii) (requiring the operator of a child-directed website or online service to "obtain verifiable parental consent for the collection, use, or disclosure of personal information from children").

67. *Id.* § 6502(b)(1)(D) (requiring the operator of such a website or online service to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children").

68. *Id.* § 6502(b)(1)(C) (prohibiting such an operator from "conditioning a child's participation . . . on the child disclosing more personal information than is reasonably necessary to participate in such activity").

69. *Id.* § 6502(b)(1) (authorizing the Commission to promulgate rules under the Administrative Procedure Act to implement the provisions of 15 U.S.C. § 6502).

70. *Id.* § 6505(d) (authorizing the Commission to seek penalties for rule violations).

71. *Id.* § 6504(a)(1) (authorizing enforcement action by state attorneys general).

72. In the 118th Congress, Senators Ed Markey and Bill Cassidy reintroduced the Children and Teens' Online Privacy Protection Act, also known as COPPA 2.0, to update COPPA's protections for children under thirteen years old and extend online privacy protections to teens. *See, e.g.*, Press Release, U.S. Senator Ed Markey, Senators Markey and Cassidy Reintroduce COPPA 2.0, Bipartisan Legislation to Protect Online Privacy of Children and Teens (May 3, 2023), https://perma.cc/RDV8-SQ2B. In July 2024, the U.S. Senate passed a package of bills consisting of COPPA 2.0 and the Kids Online Safety Act, also known as KOSA. *See* Scott Wong, Frank Thorp V, Julie Tsirkin & Syedah Asghar, *Senate Passes the Most Significant Child Online Safety Bills in Decades*, NBC NEWS (July 30, 2024, 10:02 AM PDT), https://perma.cc/P6DK-N86S.

73. *See* 15 U.S.C. § 6502(b)(1)(C); *see also* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.10 (2024) (requiring an operator to "retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which

footnote continued on next page

securely,[74] and opt-in regime for targeted advertising[75] represented significant advances. Had such protections been extended market-wide, the data security requirement alone may have curbed catastrophic breaches,[76] while rulemaking authority would have allowed the Commission to update regulations to address new market realities.[77]

In any event, the Commission would change its approach at the dawn of the new millennium. But that change provoked backlash, and the FTC's more proactive posture proved short-lived.

B. 2000: Calling for Privacy Legislation

In 2000, the Commission's patience with the failures of self-regulation finally ran out. In a report issued that year, the agency for the first time called on Congress to pass comprehensive privacy legislation codifying the fair information principles of notice, choice, access, and security.[78] The Commission concluded that "the lack of broad-based implementation of . . . consumer protections online requires legislative action in order to fully protect consumers' personal information and build public confidence in electronic commerce."[79]

Calling for the codification of fair information principles was a significant step for the Commission. But notably, the agency omitted a key principle that others had long championed: baseline collection limitations. As early as the

---

the information was collected" and to "delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion").

74. *See* 15 U.S.C. § 6502(b)(1)(D) (requiring operators to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children").

75. *See* 16 C.F.R. § 312.5(a)(2) (2024) (requiring an operator to "give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties").

76. *See, e.g.*, Complaint for Permanent Injunction & Other Relief ¶ 23, FTC v. Equifax Inc., No. 19-mi-99999 (N.D. Ga. 2019) (alleging that Equifax "failed to provide reasonable security for the massive quantities of sensitive personal information stored within Defendant's computer network"). As noted above, COPPA explicitly requires firms to maintain reasonable procedures to protect consumer information. *See* 15 U.S.C. § 6502(b)(1)(D).

77. 15 U.S.C. § 6502(b)(1) (authorizing the Commission to promulgate rules under the Administrative Procedure Act to implement the provisions of 15 U.S.C. § 6502).

78. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS, at iii (2000) [hereinafter 2000 FTC PRIVACY REPORT], https://perma.cc/WNZ7-YNYS.

79. Press Release, FTC, FTC Recommends Congressional Action to Protect Consumer Privacy Online (May 22, 2000), https://perma.cc/438A-M6XQ.

1980s, the Organisation for Economic Co-operation and Development advocated "limits to the collection of personal data."[80] The Commission's report excluded this principle from its legislative recommendations and instead added its own principle: choice.[81] This decision sparked criticism that "the Commission's privacy vision" was "too limited."[82] Indeed, the emphasis on consumer choice over data collection limits was consistent with the Commission's post-1980 approach to consumer protection, which expected individuals to protect themselves from corporate misconduct and significantly limited the purview of the FTC's work.[83]

Even as the report faced external criticism for not going far enough, it faced internal blowback for going too far. Its legislative recommendation drew a fierce dissent from Commissioner Orson Swindle, who argued once more that self-regulation was succeeding, and that legislation "should be reserved for problems that the market cannot fix on its own."[84] He urged the agency to instead pursue an approach that relies on "market forces, industry efforts, and enforcement of existing laws."[85] While concurring with the report, Commissioner Thomas Leary also argued that it "does not explain why an adequately informed body of consumers cannot discipline the marketplace to provide an appropriate mix of substantive privacy provisions."[86]

Although the FTC's call for legislation was not unanimous, it was significant. As discussed above, Congress passed children's privacy legislation just four months after the Commission called on it to do so.[87] Two years later, there was hope that the agency could once again help advance legislation—this time market-wide.[88] But that hope proved short-lived, as the agency would reverse itself the following year.

---

80. Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183, 1201 n.84 (2003) (quoting Organisation for Economic Co-operation and Development, *Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 20 INT'L LEGAL MATERIALS 422, 424 (1980)).

81. 2000 FTC PRIVACY REPORT, *supra* note 78, at 36.

82. Gellman, *supra* note 80, at 1204-05.

83. *See infra* notes 172-92 and accompanying text.

84. Dissenting Statement of Commissioner Orson Swindle 4 (May 22, 2000), *in* 2000 FTC PRIVACY REPORT, *supra* note 78, at 4.

85. *Id.* at 2.

86. Statement of Commissioner Thomas B. Leary Concurring in Part and Dissenting in Part 4 (May 22, 2000), *in* 2000 FTC PRIVACY REPORT, *supra* note 78, at 4.

87. *See* Press Release, FTC, *supra* note 65.

88. *See, e.g.*, Patrick Thibodeau, *FTC, Senator Seek Online Privacy Rules*, COMPUTERWORLD (May 26, 2000), https://perma.cc/7MMU-JKFC.

C. Early 2000s: Returning to Self-Regulation Through a "Harms-Based" Approach

In 2001, George W. Bush was sworn in as President and designated Tim Muris to serve as Chair of the FTC.[89] The new Commission quickly signaled that it would take different view of privacy and self-regulation. Shortly after the election, Commissioner Thomas Leary addressed a conference of tech companies and assured them that there would be no new privacy regulations from the FTC, calling concerns around online privacy "a new hysteria."[90] He also predicted a highly competitive market, especially in e-commerce, saying: "I do not foresee any company getting insurmountable first-move advantage from e-commerce because the technology is so easy to duplicate."[91]

Newly-appointed Chairman Muris was also skeptical of privacy legislation, but he took a more subtle approach. Muris announced the agency's privacy agenda in a 2001 speech in Cleveland, Ohio.[92] Much of what Muris said was familiar. He expressed confidence that "industry will continue to make privacy a priority," and praised the fact that a growing number of websites were posting privacy policies.[93]

But Muris, unlike some of his colleagues, did not dismiss concerns around privacy or blame consumers. He instead professed a strong commitment to advancing consumer privacy, vowing "an ambitious, positive, pro-privacy agenda" backed with greater enforcement resources.[94] Notably, he defined the FTC's privacy work expansively. For example, his privacy agenda would include "offline information practices and the rapid convergence of online and offline information systems."[95] Such practices included the use of pre-acquired credit card numbers, identity theft, and unwanted telemarketing.[96]

As to online privacy legislation, Muris argued that it would be premature.[97] He also noted a number of challenges, including how to apply

89. Press Release, FTC, Timothy J. Muris Becomes FTC Chairman (June 5, 2001), https://perma.cc/5CQ9-EXFG.

90. Julia King, *FTC Says Privacy Concerns Becoming 'Hysteria'*, CNN (June 7, 2001), https://perma.cc/3DF3-E4HQ.

91. *Id.*

92. Timothy J. Muris, Chairman, FTC, Protecting Consumers' Privacy: 2002 and Beyond: Remarks at The Privacy 2001 Conference (Oct. 4, 2001), https://perma.cc/2DST-PANS.

93. *Id.*

94. *Id.*

95. *Id.* Muris's new focus was criticized by privacy advocates and former Commission officials frustrated with the pace of self-regulation, while earning praise from industry officials. *See* John Schwartz, *F.T.C. Plans to Abandon New Bills on Privacy*, N.Y. TIMES, Oct. 3, 2001, at C5, https://perma.cc/JZ2A-JNCU.

96. Muris, *supra* note 92.

97. *Id.*

data security requirements to firms of different sizes.[98] Observing that the growth of the internet was slowing, he highlighted the potential costs of privacy legislation.[99] He also argued that internet regulation would be *too narrow*, questioning why one avenue of commerce should be subject to different rules than another based merely on the medium in which it is delivered.[100] Muris concluded that "we need more law enforcement, not more laws."[101]

Muris was laying out what would later be called a "harms-based" approach to policing privacy.[102] Under this framework, policymakers did not view certain types of data collection, use, or dissemination as intrinsically risky or undermining of people's privacy.[103] Instead, policymakers would consider whether the dissemination of people's data resulted in specific types of concrete harm, particularly physical harm (e.g. stalking), economic harm (e.g. identity theft), or unwanted intrusion (e.g. robocalls).[104]

This harms-based approach defined harm narrowly. The FTC's unfairness authority, by contrast, can prohibit a wide range of practices that injure consumers.[105] But Muris declared that in the realm of privacy, "an unfairness analysis is particularly inappropriate."[106] He argued that common privacy intrusions—such as having one's online searches and browsing history impermissibly tracked or sold—were too "subjective" to warrant enforcement under the FTC's unfairness authority.[107] Rather than having government set baseline protections to guard people from privacy invasions, markets should be left to "match each consumer to the product or service that best satisfies his or her preferences."[108]

Muris's harms-based approach would come to define his work on privacy at the Commission. And the clearest illustration of this approach, according to

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 149 (2015).

103. Howard Beales & Timothy Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 118 (2008).

104. *Id.*

105. *See infra* Part II.

106. Howard Beales & Timothy Muris, *FTC Consumer Protection at 100: 1970s Redux or Protecting Markets to Protect Consumers?*, 83 GEO. WASH. L. REV. 2157, 2219 (2015).

107. *Id.* at 2217-19.

108. *Id.* at 2219.

his consumer chief and frequent co-author, J. Howard Beales, was the Do Not Call Registry.[109]

Their "Do Not Call" initiative allowed consumers to opt out of most telemarketing.[110] The initiative succeeded, Muris and Beales would later argue, because it focused on "the call, rather than the information sharing that led to the call."[111] After all, most phone numbers were already published, and no additional information was used to call consumers.[112] "The privacy problem arises not because information was shared," they concluded, "but because the call itself interrupted their right to be let alone."[113]

Other parts of Muris's privacy agenda included efforts to combat email spam,[114] an initiative to educate consumers about identity theft and facilitate recovery,[115] and actions against firms that made misleading privacy or data security claims.[116]

For years after they left office, Muris and Beales would tout the success of their approach to privacy.[117] But their efforts fell short, even as measured against their own goals. Their signature initiative, Do Not Call, aimed to reduce unwanted calls. But such calls have surged dramatically since their tenure,[118] leading to widespread public frustration.[119] Reports of identity theft rose even more dramatically, surging more than thirty-fold from 2000 to 2023.[120] The number of data breaches has

109. Howard Beales, The FTC and Consumer Privacy: An Accomplished Agenda, Remarks Before the IAPP 5 (June 2004), https://perma.cc/CZ5Z-PMKS.

110. *See* Beales & Muris, *supra* note 103, at 119.

111. *Id.* at 119-20.

112. *Id.* at 120.

113. *Id.*

114. *See* Beales, *supra* note 109, at 7.

115. *Id.* at 22-24.

116. *Id.* at 29-34.

117. *See, e.g.*, Beales & Muris, *supra* note 103, at 109; Beales & Muris, *supra* note 106, at 2157.

118. Between 2003 and 2009, the number of Do Not Call complaints reported to the FTC peaked at 1.8 million in 2009. FTC, NATIONAL DO NOT CALL REGISTRY DATA BOOK FOR FISCAL YEAR 2009, at 4 (2009), https://perma.cc/9G64-UHJ6. A decade later, the FTC received more than 5 million complaints. FTC, NATIONAL DO NOT CALL REGISTRY DATA BOOK FOR FISCAL YEAR 2019, at 6 (2019), https://perma.cc/U7V5-V67S.

119. *See* Simon van Zuylen-Wood, *How Robo-Callers Outwitted the Government and Completely Wrecked the Do Not Call List*, WASH. POST (Jan. 11, 2018), https://perma.cc/9SXK-F5Y7 (reporting on a surge in complaints of unwanted calls, and anger by many consumers).

120. *See* U.S. DEP'T OF JUST., PUBLIC ADVISORY: SPECIAL REPORT FOR CONSUMERS ON IDENTITY THEFT (2023), https://perma.cc/75R3-F8MK (reporting that the FTC received 31,117 reports of identity theft in 2000); FTC, CONSUMER SENTINEL NETWORK ANNUAL DATA BOOK 2023, at 8 (2024).

skyrocketed as well.[121] And there is no indication that firms stopped making misleading privacy commitments.[122]

Several factors may account for the failure of the Muris approach to deter these illegal practices. But one culprit is their narrow focus on downstream harms rather than upstream data practices.

Consider the problem of identity theft. In a prescient article, Daniel Solove explained that while identity theft should be prosecuted, policymakers can't ignore that "[t]he underlying cause of identity theft is an architecture that makes us vulnerable to such crimes and unable to adequately repair the damage."[123] Under this architecture, private sector firms build detailed dossiers on consumers that identity thieves can obtain and exploit.[124] Privacy regulation that actually limits firms' ability to build, maintain, and share these dossiers would combat an upstream driver of identity theft.[125] In contrast, Muris and Beales argued that, "at its root, identity theft is a criminal law enforcement problem."[126] Their agenda thus focused on consumer empowerment and criminal referral[127]—an approach that ignored the constellation of data practices that facilitate such widespread identity theft.

A similar dynamic can be seen around the problem of unwanted calls, where Muris and Beales not only refused to curb any of the upstream data practices that drive these calls, but instead argued these tactics were generally beneficial—a "multi-billion dollar industry" where "companies collect and collate different items of information about an individual from various sources and resell it."[128] To the extent that such resale leads to unwanted

121. *Data Breach Chronology Archive - PRC Historical Data 2005 - 2019*, PRIVACY RIGHTS CLEARINGHOUSE, https://perma.cc/7XXE-RNYT (last updated Nov. 13, 2023) (citing statistics showing that the number of records compromised surged from 55 million in 2005 to nearly 1.5 billion in 2018).

122. We are not aware of a way to precisely measure the prevalence of false claims, but a 2018 GAO study evaluating a decade of FTC privacy actions found that strong majority involved deceptive claims. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY, app. 2, at 44-51 (2019).

123. Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1251 (2003).

124. *Id.*

125. *See* DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 112-13, 156-57 (2022); *cf. id.* at 142-43 (arguing that "[p]oor privacy will undermine even the best data security," and that an organization concerned about data security should "curb its data appetite, collect only the data that is necessary and justified, [and] delete data when it is no longer needed").

126. *See* Beales & Muris, *Choice or Consequences*, *supra* note 103, at 127.

127. *See Beales, supra* note 109, at 26-27.

128. *See* Beales & Muris, *Choice or Consequences*, *supra* note 103, at 109-10.

telemarketing, they suggested that the solution was better targeting based on collecting *more* consumer information.[129]

In the decades since, it has become clear that these upstream data practices are key drivers of the robocall epidemic. One common example is so-called "consent farms"—operations that lure people to websites through manipulative marketing, harvest their personal information, solicit consent deceptively, and sell these leads (along with their purported consent) to telemarketers.[130] A person who inadvertently "consents" even once can then face calls from hundreds of telemarketers, even if the person is on the Do Not Call list.[131] And while Muris and Beales argued that more precise targeting could mitigate this concern, FTC enforcement has shown that it can actually leave people more exposed—such as when someone looking for a job unwittingly "consents" to calls from debt relief scammers.[132]

Indeed, the FTC's more recent work suggests that a focus on upstream drivers of robocalls rather than simply downstream harms is needed to address this epidemic. In 2023, the FTC launched its largest-ever crackdown on unwanted calls.[133] This crackdown targeted not only telemarketers directly but also the upstream firms that sold consumers' personal information to telemarketers. For example, the FTC took action against publicly traded firm Fluent, charging that it used "dark patterns" to manipulate consumers into sharing their data and then sold this information to hundreds of "marketing partners."[134] According to the FTC's complaint, the firm sold more than 600

129. *Id.* at 112 (arguing that targeted marketing allows "companies to offer consumers choices that better satisfy their preferences").

130. Lesley Fair, *E-I-E-I-NO: Operation Stop Scam Calls Targets Operators that Facilitate Illegal Robocalls, Including "Consent Farms"*, FTC BUS. BLOG (July 18, 2023), https://perma.cc/W4WL-CVL3; Alana Samuels, *The Government Finally Did Something About Robocalls*, TIME (Dec. 15, 2023), https://perma.cc/AAH9-AXQX.

131. *See, e.g.*, Complaint for Permanent Injunction, Civil Penalties, & Other Relief at 2, United States v. Yodel Tech., No. 23-cv-1575 (M.D. Fla. July 14, 2023) (alleging calls to consumers on the Do Not Call Registry using leads purchased from consent farms); Complaint ¶ 100, United States v. Fluent, No. 23-cv-81045 (S.D. Fla. July 17, 2023) (alleging a single consent can lead to calls from hundreds of third parties).

132. Complaint ¶¶ 138-50, United States v. Fluent, No. 23-cv-81045 (S.D. Fla. July 17, 2023) (describing consent funnel).

133. Press Release, FTC, Reports of Unwanted Telemarketing Calls Down More Than 50 Percent Since 2021 (Nov. 15, 2024), https://perma.cc/U2NF-TFLA [hereinafter Telemarketing Calls Down Since 2021] (noting that Operation Stop Scam Calls was the "largest crackdown on illegal telemarketing in the agency's history"); *see also* Press Release, FTC, Law Enforcers Nationwide Announce Enforcement Sweep to Stem the Tide of Illegal Telemarketing Calls to U.S. Consumers (July 18, 2023), https://perma.cc/29CC-JJU4 [hereinafter Telemarketing Enforcement Sweep].

134. Complaint ¶ 36, United States v. Fluent, No. 23-cv-81045 (S.D. Fla. July 17, 2023). *See generally infra* notes 332-37 and accompanying text (discussing dark patterns).

million leads over the course of less than two years.[135] To prevent further harm, the FTC secured an order sharply restricting the firm's collection and sharing of consumers' personal information and requiring Fluent to destroy data it already collected.[136] Other firms engaging in similar conduct faced similar relief.[137]

Focusing on upstream actors' information-sharing practices became a key focus during Lina M. Khan's tenure as Chair of the FTC, and it showed results. Operation Stop Scam Calls targeted firms responsible for billions of calls,[138] and the agency followed up with additional enforcement actions limiting what data firms could collect and share,[139] as well as new rules to protect small businesses from fraudulent calls.[140] By the end of Khan's tenure, reports of unwanted calls had plummeted by more than half—falling from 3.4 million complaints in 2021 to 1.1 million complaints in 2024.[141]

After Muris left the FTC, the agency expanded its work on privacy and data security, including through occasionally deploying its unfairness authority. Two areas stand out. In 2005, the agency brought its first of many cases alleging that the failure to maintain reasonable security practices was unfair.[142] Muris would later claim that this theory was generally "far-reaching

135. Complaint ¶ 32, United States v. Fluent, No. 23-cv-81045 (S.D. Fla. July 17, 2023). There exist many additional examples of upstream architecture contributing to downstream harm. It is well documented that data brokers are a key driver of fraud against older Americans. When these brokers experience breaches, highly sensitive information can be disclosed—including Social Security numbers that can used to commit fraud. *See* Brian Boynton, Principal Deputy Assistant Att'n Gen., U.S. Dep't of Just. Off. of Pub. Affs., Remarks at White House Roundtable on Protecting Americans from Harmful Data Broker Practices (Aug. 15, 2023), https://perma.cc/G8CP-X2HW; AARP, *Data Privacy*, *in* AARP POLICY BOOK 2023-2024 (2023), https://perma.cc/5SP9-LUP8.

136. Telemarketing Enforcement Sweep, *supra* note 133.

137. *Id.*; *see also* Stipulated Order at 11, United States v. Viceroy Media Solutions, No. 23-cv-03516 (N.D. Cal. July 17, 2023); Stipulated Order at 9-10, United States v. Vision Solar, No. 23-cv-01387 (D. Ariz. July 14, 2023); Stipulated Order at 5, United States v. Yodel Techs., No. 23-cv-01575 (M.D. Fla. Aug. 4, 2023).

138. Telemarketing Enforcement Sweep, *supra* note 133.

139. Press Release, FTC, California-based Lead Generator Agrees to Settlement Banning It from Making or Assisting Others in Making Telemarketing Calls, Including Robocalls (Jan. 2, 2024), https://perma.cc/KZ2P-AV7C.

140. Press Release, FTC, FTC Implements New Protections for Businesses Against Telemarketing Fraud and Affirms Protections Against AI-Enabled Scam Calls (Mar. 7, 2024), https://perma.cc/8MEZ-6AUN.

141. Telemarketing Calls Down Since 2021, *supra* note 133; *see also* FTC, NATIONAL DO NOT CALL REGISTRY DATA BOOK FOR FISCAL YEAR 2024 6 (2023); FTC, A Record of Results for American Consumers: Remarks of Samuel Levine at the National Advertising Division Annual Conference 3 (2024), https://perma.cc/3CRY-MVG8.

142. *See* HOOFNAGLE, *supra* note 14, at 227-28 ("[DSW] was the first of many security cases where a combination of practices explicitly justified the unfairness label.").

and subject to abuse" and should be reserved for cases involving "intentional breaches that are highly likely to lead to fraudulent use of the information," among other preconditions.[143] The agency would also use its unfairness authority to rein in the surreptitious installation of spyware on rent-to-own computers—software that could track customers' movements, monitor their keystrokes, and hijack their webcams.[144] Even this effort by the Commission drew criticism from Muris, who argued that surreptitious tracking could benefit consumers, and that it was "odd" to be concerned about location tracking given the prevalence of mobile phones.[145]

These examples would prove an aberration. On the whole, the Commission maintained the Muris approach, choosing generally not to enforce the law against unfair—rather than deceptive—data practices and neglecting the upstream drivers of illegal practices. A 2018 GAO report examining every privacy action the agency brought during the prior decade found that more than eighty percent involved deceptive privacy promises.[146] Fewer than a quarter—23 out of 101 cases—included an unfairness claim, and most unfairness actions involved the installation of software without consumers' consent.[147] This prompted Muris to boast that the agency's concern with rooting out harmful information-sharing practices involved "much rhetoric" but had "little impact on FTC enforcement."[148]

Although the FTC's enforcement approach largely remained the same, Commissioners would come to uniformly reject and reverse Muris's opposition to legislation. In 2012, for the first time since 2000, the Commission called on Congress to pass privacy legislation.[149] And the agency abandoned the cramped conception of harm that Muris championed, concluding that "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions."[150] This move drew a Muris-esque dissent from Commissioner Rosch, who argued that such an approach was

143. *Id.* at 132. Despite Muris's alarmism, the Commission continued charging that unreasonable security practices are unfair. *See* FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), https://perma.cc/HMC2-RRAF.

144. Press Release, FTC, FTC Halts Computer Spying (Sept. 25, 2012), https://perma.cc/F6KE-F5VX.

145. *See* Beales & Muris, *supra* note 106, at 2220-21.

146. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 122.

147. *Id.*

148. Beales & Muris, *supra* note 106, at 2162.

149. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at i (2012).

150. *Id.* at 8.

paternalistic.[151] But even Rosch would endorse targeted legislation,[152] as would future Commissioners from both political parties.[153]

Although Muris would lose that battle at the Commission, he likely succeeded in helping to forestall the passage of comprehensive privacy legislation.[154] In a 2004 speech on Muris's legacy, Commissioner Leary argued explicitly that the Chair's emphasis on Do Not Call sapped momentum from budding privacy efforts:

> People may not fully appreciate that the Do Not Call Rule was also an imaginative way for Muris to avoid a divisive pre-existing debate over "privacy" legislation and to re-channel the agency's energies in a way that could command unanimous support internally and externally. The previous debate had focused on one aspect of consumer privacy—the protection of personal information obtained in e-commerce transactions—and the subject was controversial both in the Commission and in the Congress. Muris shifted the focus to another aspect of consumer privacy—the reduction of unwanted commercial intrusions into the home—and the entire nation applauded.[155]

Congress's failure to pass privacy legislation, paired with the FTC's reluctance to use its unfairness authority, left notice and choice as the dominant framework, notwithstanding widespread criticism that it fails to protect consumers' privacy.[156]

Muris's success in effectively sidestepping the privacy debates of the late 1990s was only one example of the lasting impact he had on the FTC. In the early 1980s, while serving as Director of the Bureau of Consumer Protection, Muris helped reshape the agency's entire approach to consumer protection law—especially around its use of unfairness. [157] The FTC's subsequent work on online privacy can be traced back to the ideological shift he helped usher in several decades earlier.

---

151. *Id.* at c-5.

152. *Id.* at c-3.

153. *See, e.g.*, Alexis Collins & Alan B. Freedman, *FTC Chair, Commissioners Endorse Comprehensive Privacy Legislation at Senate Oversight Hearing*, CLEARY CYBERSECURITY & PRIV. WATCH (Dec. 10, 2018), https://perma.cc/5295-DECP.

154. Schwartz, *supra* note 95 ("Without the trade commission's support for legislation, several bills that are awaiting Congressional action are likely to lose momentum . . . .").

155. Thomas B. Leary, Comm'r, FTC, The Muris Legacy, Speech at the Annual Meeting of the A.B.A. (Aug. 7, 2004), *in* ANTITRUST SOURCE, Nov. 2004, at 3-4. Commissioner Orson Swindle similarly contrasted his strong opposition to privacy legislation with his strong support for Do Not Call. Orson Swindle, Former Comm'r, FTC, Remarks at the 2004 Administrative Law Conference: A Regulator's Perspective on Protecting Consumers and Competitive Marketplaces: Developments at the FTC (Nov. 7, 2003).

156. Richard Warner, *Notice and Choice Must Go: The Collective Control Alternative*, 23 SMU SCI. & TECH. L. REV. 173, 173-75 (2020).

157. *See infra* Part I.D.

D. The FTC's Approach to Privacy in Context

As the FTC celebrated its 100th birthday in 2014, Muris and Beales celebrated the impact of the agency's 1980 Unfairness Policy Statement.[158] That Policy Statement, they argued, foreclosed the agency from using its unfairness authority to target "subjective" harms—like the privacy invasion of having one's browser data impermissibly tracked.[159] It required instead that the agency center its work on maintaining consumer sovereignty "by attacking practices that impede consumers' ability to make informed choices."[160]

Muris and Beales were right that the 1980 Policy Statement shaped the agency's work for decades to come. This Subpart situates the FTC's approach to privacy in the broader context of its retreat from combatting unfair practices.

The FTC Act's prohibition against unfair acts or practices is one of the FTC's strongest tools to combat illegal business practices. For the first two decades of its existence, the FTC enforced the prohibition on unfair methods of competition, but encountered legal difficulties in using that tool to challenge deceptive advertising and other injurious business practices.[161] That changed in 1938, when the Wheeler-Lea amendments to the FTC Act prohibited acts or practices that were "unfair" or "deceptive."[162] This authority is commonly known as "UDAP." In the decades since, every state has adopted its own UDAP statute,[163] and numerous federal agencies—including the U.S. Department of Agriculture (USDA),[164] the Department of Transportation,[165] the Consumer Financial Protection Bureau (CFPB),[166] and prudential banking regulators—enforce UDAP authorities of their own.

158. *See* Beales & Muris, *supra* note 106, at 2217-19.

159. *Id.* at 2162.

160. *Id.* at 2172, 2219.

161. Maureen K. Ohlhausen, *Weigh the Label, Not the Tractor: What Goes on the Scale in an FTC Unfairness Cost-Benefit Analysis?*, 83 GEO. WASH. L. REV. 1999, 2002-03 (2004); *see also* FTC Act, ch. 49, sec. 45, § 3, 52 Stat. 111 (1938).

162. *Id.* at 2003.

163. CAROLYN L. CARTER, CONSUMER PROTECTION IN THE STATES: A 50-STATE REPORT ON UNFAIR AND DECEPTIVE ACTS AND PRACTICES STATUTES 3 (2009).

164. Existing statutes such as the Packers and Stockyards Act include language on unfairness and the USDA introduced a new rule in 2024 on unfairness in the livestock industry. Press Release, USDA, USDA Proposes New Rule to Clarify Unfair Practices in the Livestock, Meat, and Poultry Industries (June 25, 2024), https://perma.cc/L3N5-XV5X.

165. 14 C.F.R. § 399 (2022).

166. The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) in sections 1031 and 1036 grants the CFPB the ability to regulate unfairness in consumer financial firms and markets. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, 124 Stat. 1383 (codified as amended in scattered sections of the U.S. Code).

Although they involve some overlap, unfairness is distinct from deception. The FTC Act's deception prohibition bars acts or practices, such as false advertising, that are likely to mislead consumers acting reasonably under the circumstances.[167] It does not require a showing of injury.[168] Unfairness, in contrast, is focused on injury—specifically, whether an act or practice (i) causes or is likely to cause substantial injury (ii) that is not reasonably avoidable and (iii) is not outweighed by countervailing benefits to consumers or competition.[169]

This distinction becomes especially important in the context of data abuses and online privacy. When practices are deceptive, the typical remedy requires providing clear and accurate information to consumers.[170] But that approach leaves a gap, as businesses may stop making privacy commitments altogether. If their data practices are nevertheless harmful, though—for example, because they expose consumers to identity theft—the core problem has not been addressed. Enter unfairness. If the company's data collection or dissemination practices causes unavoidable injury that is not outweighed by countervailing benefits—the statutory test—then the FTC can seek remedies that go beyond better disclosure and instead actually restrict the offending practice.[171]

The 1980s saw new leadership at the Commission committed to a more hands-off approach to enforcing the law against illegal business practices.[172] Limiting the agency's use of unfairness was a prime target.[173] Amidst a wave of consumer advocacy in the 1970s, the Commission began using its unfairness authority in new ways and secured a major win in 1972 when the Supreme

167. James C. Miller III, Chairman, FTC, FTC Policy Statement on Deception (Oct. 14, 1983).

168. *Id.*

169. 15 U.S.C. § 45(n).

170. *See, e.g.*, Press Release, FTC, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network (Mar. 30, 2011), https://perma.cc/ZBH4-QPKR (alleging that Google engaged in deceptive privacy practices, and barring further misrepresentations); Press Release, FTC, Myspace Settles FTC Charges That It Misled Millions of Users About Sharing Personal Information with Advertisers (May 8, 2012), https://perma.cc/GL59-EX8F (alleging similar claims about MySpace with similar result).

171. *See, e.g.*, Press Release, FTC, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://perma.cc/XQ98-PJ2F (alleging it was unfair to share sensitive location data and banning the practice); Press Release, FTC, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (Jan. 18, 2024), https://perma.cc/W9WC-EU7X (same); *see also* 15 U.S.C. § 45(n).

172. *See, e.g.*, Eleanor M. Fox, *Chairman Miller, the Federal Trade Commission, Economics, and* Rashomon, 50 L. & CONTEMP. PROBS. 33, 40 (1987) ("[Chairman Miller] equates laissez faire, limited by no more than minimal antitrust intervention and virtually no regulatory intervention, with political freedom.").

173. *See* Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U. L. REV. 431, 522 (2021).

Court confirmed the reach of the authority in the landmark *Sperry* decision.[174] The Commission built on this legal win by issuing a set of new rules banning unfair or deceptive practices, including its Credit Practices Rule prohibiting predatory credit terms.[175] Perhaps the most famous rulemaking the Commission pursued during this period proposed to limit the advertising of sugary cereals to children.[176] Although this effort had strong support from both the public and Congress, a concerted special interest campaign eventually sparked significant backlash, with detractors accusing the FTC of using its unfairness authority too aggressively.[177]

In an effort to appease critics, the FTC responded with a letter to Senators Wendall Ford and John Danforth that set forth the agency's view of unfairness in a policy statement.[178] Through this letter, the Commission sought to both clarify the "framework for future application of [its] unfairness authority" and assure members of Congress that enforcement of unfairness claims would not unduly burden businesses.[179]

A key line from the statement illustrates the Commission's emerging skepticism toward government action: "Normally we expect the marketplace to be self-correcting, and we rely on consumer choice—the ability of individual consumers to make their own private purchasing decisions without regulatory intervention—to govern the market."[180]

The Commission's approach to unfairness was premised on a particular descriptive account of the economy, where "self-correcting" markets ensure that corporate abuse is disciplined by competition and where consumers are fully informed and perfectly rational actors. Based on this theoretical conception, the Commission undertook a radical departure from decades of FTC action, adopting a much thinner conception of the agency's mission and role. Under this approach, the focus of the Commission's work became

174. Yaniv Ron-El, Mobilizing Consumers: The American Consumer Movement in the 1960s-70s as a Social Movement 174-75 (Aug. 2022) (Ph.D. dissertation, University of Chicago) (on file at Open Access Repository, Knowledge@UChicago), https://perma.cc/KL72-JQ9X; FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 (1972).

175. *See* Herrine, *supra* note 173, at 483-84.

176. *Id.* at 484-86.

177. *Id.* at 490, 507.

178. Letter from Michael Pertschuk, Chairman, Paul Rand Dixon, Comm'r, David A. Clanton, Comm'r, Robert Pitofsky, Comm'r & Patricia P. Bailey, Comm'r, to Sen. Wendell H. Ford & Sen. John C. Danforth (Dec. 17, 1980), https://perma.cc/A9LE-CF6Z, *reprinted in* Int'l Harvester Co., 104 F.T.C. 949, app. at 1070-76 (1984) (Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction), https://perma.cc/ZZ6W-UZWY.

179. *Id.*

180. *Id.*

preserving consumers' ability to make rational purchasing decisions, primarily through ensuring they had access to accurate information and were not actively misled.[181] In this way, the Commission's focus more closely mapped on to its deception authority.[182]

The Unfairness Policy Statement also sought to limit the types of harms the FTC would aim to address. Most substantial injury, the Statement proclaimed, involved monetary losses.[183] "Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."[184] This statement, for which no legislative text or judicial decisions are cited, would profoundly shape how the Commission approached its work on data abuses two decades later.

In many ways, the policy statement was a success. It earned bipartisan support at the Commission and—after Congress codified its three-part test in 1994—continues to bind the Commission today.[185]

However, this success came with a heavy price: The Commission largely stopped bringing unfairness cases in the 1980s and all throughout the 1990s, even in the face of major corporate abuses.[186] This abandonment of a core Commission authority set the stage for the Commission's approach to market governance and enforcement in the early 2000s.[187]

For example, in the early 1990s, enforcers and public health advocates loudly sounded the alarm about tobacco companies like R.J. Reynolds using cartoons to entice children to smoke cigarettes.[188] But R.J. Reynolds—working with Howard Beales, Tim Muris's future consumer chief—pushed back, arguing that there was "no evidence to support the notion that advertising has

181. Herrine, *supra* note 173, at 441-42; *see also* J. Howard Beales, Dir., Bureau of Consumer Prot., *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (May 30, 2003), https://perma.cc/9GPX-L3FE.

182. *See* Beales, *supra* note 181 (arguing that deception should be viewed as a subset of unfairness where misleading claims "cause consumer injury because consumer choices are frustrated and their preferences are not satisfied").

183. Letter from Pertschuk et al., *supra* note 178.

184. *Id.*

185. *See* Beales, *supra* note 181; 15 U.S.C. § 45(n) ("In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence.").

186. *See* Rohit Chopra, Comm'r, FTC, Comment Letter on Department of Transportation Proposed Rule: Defining Unfair or Deceptive Practices 5 & n.25, https://perma.cc/GUL6-B3TY (archived Apr. 18, 2025) (noting that "between 1980 and 1993, there were only five adjudicated unfairness orders, three federal appellate reviews, and zero reviews by the Supreme Court").

187. *See infra* notes 206-10 and accompanying text.

188. John Harrington, *Up in Smoke: The FTC's Refusal to Apply the "Unfairness Doctrine" to Camel Cigarette Advertising*, 47 FED. COMMC'NS L.J. 593, 594 (1995).

an important or powerful effect on teenagers' decisions."[189] The Commission evidently credited this argument, and voted against challenging the practice as unfair.[190] Four years later, the Commission would reverse this decision,[191] but its action would soon be mooted by a multistate settlement.[192]

In the 2000s, the Commission's unwillingness to use its unfairness authority shaped its approach to subprime lending. In 2004, Beales—now leading the Bureau of Consumer Protection—provided testimony on "unfair and deceptive subprime lending."[193] The testimony stressed that while the Commission was committed to rooting out "dishonest and unscrupulous" lenders, "the agency ha[d] been careful to avoid discouraging honest subprime lenders from making credit available to consumers."[194] Such credit, Beales argued, was being made available based on finely calibrated risk-based pricing, and subprime lending "provided access to mortgage loans, and thus home purchases, in communities that have been underserved in the past."[195] The best defense against unscrupulous subprime lending, he concluded, was educated consumers.[196]

This rosy view of subprime lending as a force for good that the Commission should not disturb directly informed the Commission's hands-off approach to enforcement in this area.[197] And indeed, Chairman Muris was seen

189. Caroline E. Mayer, *FTC Choice Defended Tobacco Ad*, L.A. TIMES (May 31, 2001, 12:00 AM PT), https://perma.cc/6FFG-AU7U.

190. Joint Statement of Commissioners Mary L. Azcuenaga, Deborah K. Owen, and Roscoe B. Starek, III, R.J. Reynolds Tobacco Co., FTC File No. 932-3162 (June 6, 1994), https://perma.cc/HLL9-KNSR (explaining that the Commission voted not to issue a complaint against R.J. Reynolds because "the evidence to support [the] intuition" that its "Joe Camel advertising campaign would lead more children to smoke or lead children to smoke more" was "not there"); *see also* Harrington, *supra* note 188, at 594-95; Stuart Elliott, *The F.T.C. Explains Its Joe Camel Decision*, N.Y. TIMES (June 8, 1994), https://perma.cc/B26M-GC37.

191. Press Release, FTC, Joe Camel Advertising Campaign Violates Federal Law, FTC Says (May 28, 1997), https://perma.cc/83N7-9GD9.

192. *The Tobacco Master Settlement Agreement*, NAT'L ASS'N ATT'YS GEN, https://perma.cc/VDZ8-PLLE (archived Apr. 18, 2025).

193. J. Howard Beales, Dir., Bureau of Consumer Prot., Prepared Statement of the Federal Trade Commission on Efforts to Combat Unfair and Deceptive Subprime Lending Before the Senate Special Committee on Aging (Feb. 24, 2004), https://perma.cc/RJ7C-XFVW.

194. *Id.* at 1.

195. *Id.* at 3.

196. *Id.* at 8.

197. *See, e.g.*, Deborah Platt Majoras, Chair, FTC, Remarks before the Consumer Federation of America 2007 Consumer Assembly 4 (Feb. 2, 2007), https://perma.cc/YD5C-UGT8 (describing the Commission's recent work in consumer financial protection, and noting that for consumers considering financial products, "it is essential that they understand all the terms" of such products).

as having downplayed the catastrophic risks posed by subprime lending.[198] The Commission never challenged directly what many saw as the core problem in the subprime market: that lending without considering a consumer's ability to repay debt set up consumers to fail.[199]

In a stark example of the shift in the agency's priorities, the FTC did bring a lawsuit against one of the most notorious subprime lenders in 2007, but that lawsuit was for Do Not Call violations.[200] The company's lending practices, which even in 2006 were being challenged by other enforcers as predatory,[201] went unaddressed by the FTC.[202]

Once subprime mortgages began to collapse in 2007 and 2008, the FTC came under heavy criticism for failing to use its legal authority, especially its unfairness authority, to target improvident lending—with one U.S. Senator describing the FTC as "absent" on the issue.[203] On the defensive, FTC leadership specifically blamed the agency's post-1980 view of unfairness,

198. *See* Chris Jay Hoofnagle, *The Federal Trade Commission's Inner Privacy Struggle*, in THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 168, 172 n.19 (Evan Selinger et al. eds., 2018).

199. Other UDAP enforcers deployed unfairness more proactively, protecting their citizens from serious harm. In 2007, the Massachusetts Attorney General charged a mortgage lender, Fremont Investment and Loan, with engaging in "structurally unfair" lending, and won a landmark decision by the state's Supreme Judicial Court. Commonwealth v. Fremont Inv. & Loan, No. 07-4373-BLS1, 2008 WL 517279, at *7, *10 (Mass. Super. Feb. 26, 2008); Commonwealth v. Fremont Inv. & Loan, 452 Mass. 733 (2008).

200. The FTC only brought charges forward on "Violating the National Do Not Call Registry" and "Ignoring Entity-Specific Do Not Call Requests" in their complaint filed against Ameriquest Mortgage Company. Complaint for Civil Penalties, Permanent Injunction, & Other Relief ¶¶ 17-18, Ameriquest Mortg. Co., FTC File No. 042-3082, https://perma.cc/6MFK-TSKY (last updated Nov. 7, 2007).

201. Press Release, Office of California Attorney General Bill Lockyear, Attorney General Lockyer Announces $325 Million Settlement with Ameriquest to Resolve National Predatory Lending Case (Jan. 23, 2006), https://perma.cc/C3B5-QVL7.

202. Ameriquest Mortg. Co., *supra* note 200 (charging Ameriquest with Do Not Call rather than lending violations).

203. In 2008, Senator Byron Dorgan accused the FTC of being "absent" on subprime lending, while Senator Bill Nelson criticized the agency's failure to challenge unfair lending products. *See Improving Consumer Protections in Subprime Lending: Hearing Before the Subcomm. on Interstate Com., Trade, and Tourism, of the S. Comm. on Com., Science, & Transp.,* 110th Cong. 9, 21 (2008) (statements of Sen. Byron L. Dorgan, Chairman, Subcomm. on Interstate Com., Trade, and Tourism, & Sen. Bill Nelson, Member, Subcomm. on Interstate Com., Trade, and Tourism). Congress held another hearing addressing the FTC's enforcement track record the following year, where a witness described the Agency as being "completely passive" in using its unfairness authority. *See Consumer Credit and Debt: The Role of the FTC in Protecting the Public: Hearing Before the Subcomm. on Com., Trade, & Consumer Prot., of the H. Comm. on Energy & Com.,* 111th Cong., 100 (2009) (testimony of Ira Rheingold, Executive Dir., National Association of Consumer Advocates) [hereinafter *Consumer Credit and Debt*].

arguing that it left the Commission less prepared to bring cases.[204] Congress responded by creating a new agency to police financial abuses, the CFPB. Lawmakers reassigned some of the FTC's work to the CFPB and equipped the agency with unfairness authority as well as a new prohibition on abusive practices.[205]

The FTC's post-1980 approach to unfairness—and the ideological assumptions underlying it—ultimately laid the groundwork for the agency's hands-off approach to data privacy in the early 2000s.[206] Indeed, Muris would later celebrate how the Policy Statement on Unfairness purportedly foreclosed the agency from challenging practices like surreptitious tracking.[207] And there are parallels between the FTC's approach to subprime lending and its approach to online regulation. The FTC did not challenge predatory lending as such, instead focusing efforts on ensuring loan terms were adequately disclosed.[208] Similarly, the focus in the privacy arena was on ensuring that privacy policies were posted and followed, rather than seeking substantive protections for people's data.[209] In both areas, the agency took the position that consumers should be left to defend and protect themselves from corporate abuse, so long as they are not misled.[210]

Just as the subprime mortgage crisis triggered an avalanche of complaints around the FTC's failure to protect consumers in financial markets, the Cambridge Analytica scandal led to harsh criticism of the FTC's privacy

204. In 2009, the incoming Chairman of the FTC responded to a challenge on why the FTC had brought so few unfairness actions by acknowledging that the Agency's post-1980 definition had left it less prepared to bring cases. *See Consumer Credit and Debt*, *supra* note 203, at 69 (statement of Jon Leibowitz, Chairman, FTC) ("I would say certainly if we had a little more leverage in our unfairness standard, we might be able to bring unfairness cases more often. We had a much broader standard in the 1960s and 1970s, and through the late 1970s, and then Congress asked us to modify first of our own volition and then it put it in the statute, I think, in 1992, our unfairness authority."); *see also* Braden Cox, *Beyond Privacy Policies to Policy Prescription: The New Unfairness Doctrine at the FTC*, NETCHOICE (Jan. 12, 2010), https://perma.cc/9P32-KCGM.

205. 12 U.S.C. § 5531.

206. *See supra* note 92 and accompanying text.

207. Beales & Muris, *supra* note 106, at 2219-20.

208. Majoras, *supra* note 197, at 4 (noting that with respect to nontraditional mortgages, the FTC was focused on "instances of deceptive mortgage advertising").

209. 1998 FTC PRIVACY REPORT, *supra* note 48, at 7 (identifying "notice" as the most fundamental fair information practice); Solove & Hartzog, *supra* note 11, at 627-28 (2014).

210. *Cf.* Herrine, *supra* note 173, at 441-42 (describing the Commission's adoption of the consumer sovereignty framework, in which the FTC would be prevented from "acting recklessly or paternalistically" and would instead act narrowly to "attack[] practices that impede consumers' ability to make informed choices" (internal citations omitted)).

enforcement,[211] with some calling for the creation of a new privacy agency.[212] But in recent years, the FTC has reasserted itself as a vigorous, nimble, and forward-leaning enforcer aiming to not repeat the mistakes of the early 2000s and to instead architect a new approach to consumer protection in the digital age.[213]

II. A New Approach to Digital Consumer Protection

By the 2020s, the flaws in the Commission's early approach to online privacy were highly apparent. The Commission itself had acknowledged years earlier that self-regulation had failed.[214] Even the Commission's effort to push self-regulatory fixes like a "Do Not Track" signal had no meaningful market impact, with major firms largely ignoring the signal.[215] Notice and choice had fared no better, with firms inundating users with lengthy terms of service for products that people increasingly relied on to navigate daily life.

Although "notice and choice" was a policy failure, it did prompt most firms to post privacy policies.[216] In contrast, Muris's harms-based approach failed even on its own terms. Identity theft,[217] data breaches,[218] and unwanted calls[219] all surged following his tenure.

---

211. In 2018, reporting from the *New York Times* revealed that Cambridge Analytica, a British political consulting firm, had improperly obtained data on tens of millions of Facebook users. Nicholas Confessore & Cecilia Kang, *Facebook Data Scandals Stoke Criticism That a Privacy Watchdog Too Rarely Bites,* N.Y. TIMES (Dec. 30, 2018), https://perma.cc/NM8W-3JE7. For criticism of the FTC's response, see, for example, *id.*

212. *See, e.g.*, *The U.S. Urgently Needs a Data Protection Agency*, ELEC. PRIV. INFO. CTR. (2021), https://perma.cc/4MQZ-4VPW; Press Release, U.S. Senator Kirsten Gillibrand, Gillibrand Introduces New and Improved Consumer Watchdog Agency to Give Americans Control Over Their Data (June 17, 2021), https://perma.cc/U7YT-L5YJ.

213. FTC, Remarks of Chair Lina M. Khan: FTC Tech Summit 1, 5 (2024), https://perma.cc/L74T-NXN5.

214. *See supra* Part I.A (describing the FTC's confidence and eventual disappointment in self-regulatory efforts).

215. *Small Business Perspectives on a Federal Data Privacy Framework*: *Hearing Before the Subcomm. on Mfg., Trade, & Consumer Prot.* (statement of Justin Brookman, Director, Privacy and Technology Policy, Consumer Reports before the Senate Subcommittee on Manufacturing, Trade, and Consumer Protection on Small Business Perspectives on a Federal Data Privacy Framework) (Mar. 26, 2019), https://perma.cc/ZY5X-V3U6.

216. Solove & Hartzog, *supra* note 11, at 594.

217. *See* U.S. DEP'T OF JUST., *supra* note 120 (reporting that the FTC received 31,117 reports of identity theft in 2000); FTC, *supra* note 120.

218. *Supra* note 121.

219. Van Zuylen-Wood, *supra* note 119.

Recognizing these shortcomings, the Biden-era Commission set out to develop a new framework for consumer protection in the digital age. First, the Commission would examine and target the upstream drivers of data abuses, focusing on the underlying collection of data and the business models driving this unchecked surveillance. Second, the Commission would scrutinize how firms design online architecture, especially "dark patterns" that manipulate people and cost consumers money or time. Third, the Commission would recognize children and teens as a distinct category of consumers requiring strong protections. Finally, responding to the failures of self-regulation, the Commission would focus on deterrence, crafting remedies that disincentivize lawbreaking rather than encourage it.

The core ideas behind this approach are not novel. Targeting the far-reaching and excessive collection of data is well-established in privacy law.[220] Concerns about online abuses and manipulation go back at least a decade.[221] Leading regulators have warned for years that, too often, large firms and their executives view breaking the law as a profitable proposition.[222] What the FTC's new approach offered was a coherent framework for law enforcement in the digital economy. And during the period from 2021 to 2024, the FTC applied this framework across its cases, rulemakings, policy guidance, and market studies.

This Part will examine the four pillars of the FTC's new approach. Many of the FTC's recent activities received widespread public attention, both by journalists[223] and select scholars.[224] This Part ties together these distinct actions by describing the underlying vision and strategy.

This Part does not purport to declare victory over data abuses or suggest that this work is complete. Indeed, the FTC's new strategy remains nascent—and its institutional durability remains an open question. Yet for the first time since Muris laid out his harms-based approach to privacy, the FTC has laid out and implemented a coherent framework for advancing consumer protection in the digital age. And the early results are promising.

---

220. Jordan Francis, *Unpacking the Shift Toward Substantive Data Minimization Rules in Proposed Legislation*, Int'l Ass'n Priv. Pros. (May 22, 2024), https://perma.cc/6MZ7-8WYG.

221. Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE (Feb. 2012), https://perma.cc/Z3BC-G5Z7.

222. Memorandum 2018-01 on Repeat Offenders from Rohit Chopra, Comm'r, FTC (May 14, 2018), https://perma.cc/YL3V-F2TQ.

223. *See, e.g.*, Natasha Singer, *U.S. Regulators Propose New Online Privacy Safeguards for Children*, N.Y. TIMES (Dec. 20, 2023), https://perma.cc/8RCC-5975.

224. *See, e.g.*, Herrine, *supra* note 16, at 30-32.

The FTC's primary tools to pursue digital consumer protection are enforcement, rulemaking, and market guidance and inquiries.[225] From 2021 to 2024, the agency would reinvigorate each of these tools to reshape its approach to digital oversight and regulation.

The FTC's foremost tool is enforcement. The agency can bring cases administratively, litigate cases in its own name in federal court, or refer actions to the Department of Justice.[226] The FTC litigates cases, usually dozens at a time.[227] It also settles many actions through agreements known as "consent orders."[228] Businesses look to the agency's law enforcement work to gain insights on agency priorities and approaches.[229] This is especially true in the context of data abuses, where the absence of a standalone federal privacy law means that FTC enforcement actions can directly shape the rules governing the collection and use of people's data.[230] Scholars have noted that FTC consent orders settling charges related to online data abuses can serve as "the functional equivalent of privacy common law,"[231] seen as having "precedential weight" by privacy practitioners.[232]

The FTC can also issue guidance, such as through policy statements or business advisories.[233] FTC guidance is not binding, but it can identify

225. Memorandum from the FTC, A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority (updated May 2021), https://perma.cc/9MDJ-4NJ7.

226. *See id.*

227. *See Samuel Levine on the FTC and Man Controlling Trade*, CORP. CRIME REP. (Sept. 1, 2024), https://perma.cc/7FTT-MLRC (noting that the FTC is in litigation in "dozens of cases"); FTC, ANNUAL PERFORMANCE REPORT FOR FISCAL YEAR 2023 AND ANNUAL PERFORMANCE PLAN FOR FISCAL YEARS 2024-2025, at 10 (2025), https://perma.cc/T3EN-KKYU (noting the filing of more than fifty federal and administrative consumer protection complaints in fiscal year 2023).

228. Solove & Hartzog, *supra* note 11, at 610 (explaining how FTC matters can be resolved through consent orders).

229. *See, e.g.*, Anthony J. Dreyer, Margaret E. Krawiec, Paul M. Kerlin & Todd D. Kelly, *FTC Enforcement Trends in Consumer Protection Under the Biden Administration*, 2024 INSIGHTS (Dec. 13, 2023) https://perma.cc/M7AR-JQ87.

230. *See generally* Solove & Hartzog, *supra* note 11, at 585-86 ("[I]n practice, FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or any common law tort.").

231. *Id.* at 608. Privacy lawyers regularly use FTC settlements to advise companies how to avoid triggering FTC enforcement. *Id.* at 621. Firms that counsel clients on privacy matters routinely post and disseminate client alerts based off of FTC actions. *Id.*

232. *Id.* at 620.

233. The FTC maintains a public repository of all policy statements, as well as an active blog for consumers and private businesses alike. *Legal Library: Policy Statements*, FTC, https://perma.cc/PG8S-UKH5 (archived Apr. 18, 2025); *Business Blog*, FTC, https://perma.cc/SYC7-PM2H (archived Apr. 18, 2025).

enforcement priorities, synthesize relevant law, or put firms on notice.[234] Particularly as it confronts emerging areas like AI, the FTC can use policy statements to notify market participants as to how it intends to use its tools and authorities.

Finally, the Commission has the authority to promulgate rules.[235] This includes the authority to prohibit unfair or deceptive practices that are prevalent in the economy, to prohibit unfair methods of competition, and to implement congressional statutes like COPPA or GLB.[236] Rules can be applicable market wide, and the Commission can generally seek injunctions, refunds, and civil penalties for violations.[237]

The following Subparts illustrate how, during the Biden Administration, the agency has harnessed each of these tools to chart a new approach to digital consumer protection.

A. Limiting What Firms Can Collect, Retain, and Disseminate

In pursuing a new approach to the FTC's data privacy work, agency leaders started with the proposition that data that is not held cannot be abused.[238] Accordingly, the FTC has sought to place limits on the collection, use, storage, and dissemination of personal data. Potential limits on a navigation app, for example, could permit the collection of location data only while the app is being used and only if such data is deleted promptly.

Establishing substantive limits on what data can be collected and how it can be used represents a decisive break from the Muris-era approach. Those efforts (1) focused on a narrow subset of downstream harms, like identify theft and data breaches, while ignoring the upstream data-practices that can facilitate these harms, and (2) focused on imposing procedural steps like

234. *See, e.g.*, Press Release, Committee on Judicial Review, Administrative Conference of the United States, *Agency Guidance Through Interpretive Rules* (Aug. 8, 2019), https://perma.cc/7W63-8ZCS (explaining the operation of guidance and interpretive rules and recommending best practices).

235. Memorandum from the FTC, *supra* note 225.

236. 15 U.S.C. § 6502(b) (directing the Commission to promulgate rules under COPPA); *id.* § 6804 (authorizing the Commission to promulgate rules).

237. *See* Memorandum from the FTC, *supra* note 225.

238. Some call this concept "data minimization," though its exact contours are somewhat imprecise. *See* SOLOVE & HARTZOG, *supra* note 125, at 146. ("Data that doesn't exist can't be compromised. The central privacy principle of *data minimization*—to collect only data necessary for the purpose at hand and to avoid retaining unnecessary data—can play a key role at minimizing the harmful effects of breaches."); *see also* Helena Engfeldt & Elisabeth Dehareng, *Data Minimization: An Increasingly Global Concept*, Int'l Ass'n Priv. Pros. (May 7, 2024), https://perma.cc/YB8K-RV4X.

notifying users of sweeping data collection and use, rather than setting any substantive limits on the collection and use of data in the first instance.

By targeting the upstream practices that enable downstream lawbreaking, the FTC's revamped approach has sought to cut off data abuses before they occur.[239] This can help effectuate "structural changes in the data ecosystem" that are focused on addressing business incentives and preventing injury rather than redressing it after the fact.[240] The move from procedural rules to substantive restrictions has also shifted the FTC's work away from the "fair information practices" framework, which "conceive[s] of fair data processing as an eternally virtuous goal"[241] and can "normalize the kinds of data collection and surveillance harms that [procedural requirements] are supposed to mitigate."[242]

This Subpart lays out the FTC's recent approach in two parts. First, it details the FTC's efforts to secure baseline limits on how firms collect, use, and retain data. Next, it lays out the FTC's more tailored approach to sensitive data, where specific uses and dissemination are targeted as unfair under the FTC Act.

1. Baseline limits on the collection, use, and retention of data

The FTC has recommended for at least a decade that companies not collect or retain data longer than is reasonably necessary.[243] Additionally, many civil society advocates have recognized baseline limits as the most viable alternative to notice and consent, as it sets out clear restrictions regardless of what is stated in a terms of service or privacy policy.[244] Drawing on these insights, Commission leadership identified in 2022 the importance of establishing substantive limits, rather than procedural rules, for increasing the efficacy of its privacy enforcement.[245] Central to this approach is an appreciation for the

239. SOLOVE & HARTZOG, *supra* note 125, at 146.

240. *Id.* at 75.

241. *See* Hartzog & Richards, *supra* note 13, at 1695.

242. *Id.* at 1696.

243. *See, e.g.*, FTC, *supra* note 149, at23.

244. *See, e.g.*, Sara Geoghegan, *Data Minimization: Limiting the Scope of Permissible Data Uses to Protect Consumers*, ELEC. PRIV. INFO. CTR. (May 4, 2023), https://perma.cc/LG4G-ZNWE.

245. *See* Lina M. Khan, Chair, FTC, Remarks at IAPP Global Privacy Summit 6 (Apr. 11, 2022), https://perma.cc/2UV8-78DP ("Going forward, I believe we should approach data privacy and security protections by considering substantive limits rather than just procedural protections, which tend to create process requirements while sidestepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place. The central role that digital tools will only continue to play invites us to consider whether we want to live in a society where firms can condition access to critical technologies and opportunities on users surrendering to commercial surveillance.").

business models that can spur firms to endlessly monetize user data, creating an incentive for expansive collection—be it the sale of behavioral ads or the training of large language models.

One early model of this approach was the Commission's 2022 data security action against the online blogging platform CafePress.[246] The FTC charged CafePress with concealing multiple data breaches from its users and failing to implement reasonable security measures to protect sensitive information stored on its network, including Social Security numbers, passwords, and answers to password reset questions.[247] These were all standard components of the FTC's traditional data security work.[248] But the CafePress complaint went further, charging that the company "created unnecessary risks to Personal Information by storing it indefinitely on its network without a business need[,]" thus violating the FTC Act's prohibition on unfair practices.[249] The CafePress order similarly broke new ground by including a number of novel features—including a requirement for the company to adopt multifactor authentication methods that use a secure authentication protocol,[250] as well as to redress consumers who had been affected.[251] It also marked the Commission's first data security action to require the respondent to adopt "[p]olicies and procedures to minimize data collection, storage, and retention."[252]

Practitioners recognized the CafePress order's significance. An article published by the International Association of Privacy Professionals described the remedy as "arguably revolutionary."[253] Baseline limits on data collection, the article pointed out, are "too often overlooked in a world obsessed with notice and consent."[254] A major law firm, DLA Piper, advised clients that this

246. Complaint, Residual Pumpkin Entity, LLC, FTC File No. 1923209 (June 23, 2022), https://perma.cc/L5KG-242P.

247. *Id.* ¶ 11.

248. *Privacy and Security Enforcement*, FTC, https://perma.cc/E6D2-H3SS (archived Apr. 18, 2025).

249. Complaint, *supra* note 246, ¶ 11.

250. Decision and Order at 4, Residual Pumpkin Entity, LLC, FTC File No. 1923209 (June 23, 2022), https://perma.cc/GGN7-4FY6.

251. *Id.* at 9.

252. Decision and Order, *supra* note 250, at 4; Jim Dempsey, *Key Data Security Insights from FTC CafePress Settlement*, Int'l Ass'n Priv. Pros. (Mar. 22, 2022), https://perma.cc/2U7P-JAYC (noting that this "may be the first settlement to mandate data minimization at the collection phase and may signal growing Commission support for bringing data minimization into the center of FTC enforcement").

253. Dempsey, *supra* note 252.

254. *Id.*

action "may signal new attention from the FTC on data minimization and overcollection of unnecessary consumer data."[255]

DLA Piper's prediction proved accurate. Over the next three years, the Commission would bring more than sixteen additional actions requiring firms to substantively limit their collection, use, and retention of personal data.[256]

255. Andrew Serwin, Deborah Meshulam & Leila Javanshir, *CafePress to Pay $500,000 for FTC Violations*, DLA PIPER (Mar. 22, 2022), https://perma.cc/CZ2E-X3Y9.

256. These include proposed or final orders in actions the FTC has taken against Blackbaud, Avast, X-Mode Social, InMarket Media, RiteAid, Global Tel*Link, BetterHelp, Amazon Alexa, Easy Healthcare, Edmodo, GoodRx Holdings, Epic Games, Chegg, Drizly, CafePress, and Kurbo (Weight Watchers). *See* Press Release, FTC, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges Its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://perma.cc/8FGP-8SJS; Press Release, FTC, FTC Finalizes Order with Avast Banning It from Selling or Licensing Web Browsing Data for Advertising and Requiring It to Pay $16.5 Million (June 27, 2024), https://perma.cc/Q775-MS7G; Press Release, FTC, FTC Finalizes Order with X-Mode and Successor Outlogic Prohibiting It from Sharing or Selling Sensitive Location Data (Apr. 12, 2024), https://perma.cc/MGE6-9KL8; Press Release, FTC, FTC Finalizes Order with InMarket Prohibiting It from Selling or Sharing Precise Location Data (May 1, 2024), https://perma.cc/9ZHV-CX94 [hereinafter InMarket Order Press Release]; Press Release, FTC, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards (Dec. 19, 2023), https://perma.cc/V7YT-PVCM [hereinafter Rite Aid Proposed Order Press Release]; Press Release, FTC, FTC Takes Action Against Global Tel*Link Corp. for Failing to Adequately Secure Data, Notify Consumers After Their Personal Data Was Breached (Nov. 16, 2023), https://perma.cc/57JX-G8GE; Press Release, FTC, FTC Gives Final Approval to Order Banning BetterHelp from Sharing Sensitive Health Data for Advertising, Requiring It to Pay $7.8 Million (July 14, 2023), https://perma.cc/G7Z5-CNUD [hereinafter BetterHelp Order Press Release]; Press Release, FTC, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests (May 31, 2023), https://perma.cc/5KZ2-P2G5; Press Release, FTC, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), https://perma.cc/B52Y-5T7K [hereinafter Premom Proposed Order Press Release]; Press Release, FTC, FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts (May 22, 2023), https://perma.cc/G5TN-SZD4; Press Release, FTC, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023), https://perma.cc/4BEG-QXCW [hereinafter GoodRx Enforcement Action Press Release]; Press Release, FTC, Fortnite Video Game Maker Epic Games to Pay More than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges (Dec. 19, 2022), https://perma.cc/US2N-DXVP [hereinafter Epic Games Settlements Press Release]; Press Release, FTC, FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers (Oct. 31, 2022), https://perma.cc/Z7B4-VVFD; Press Release, FTC, 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://perma.cc/27A2-4GPJ; Press Release, FTC, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar. 15, 2022), https://perma.cc/79AF-3NS5; Press Release, FTC, FTC Takes Action Against Company Formerly Known as Weight

footnote continued on next page

The Commission crafted complaints and orders according to the specific facts in each matter and based on the Commission's evolving enforcement experience.[257] But collectively they reflected a sustained effort to make clear that over-collection and over-retention of data can be unfair under the FTC Act and must be remedied through a substantive obligation to limit collection, rather than through longer privacy disclosures.[258]

The Commission established that indefinite retention of data—even in the absence of other failures—can be an unfair practice under the FTC Act.[259] For example, the FTC's 2024 action against Blackbaud included a standalone count charging that the company's failure to implement appropriate data retention policies was unfair under the FTC Act.[260]

The FTC also addressed directly the question of whether retaining data indefinitely for the purpose of training machine learning models can override bans on indefinite retention. In the *Alexa* matter, the FTC charged that Amazon's practice of retaining children's data indefinitely in order to train its algorithms was both unfair and a violation of COPPA.[261] The order required the company to delete data from inactive accounts within 90 days and prohibited Amazon from using geolocation, voice information, and children's voice information subject to consumers' deletion requests for the creation or improvement of any data product.[262] In a statement accompanying the enforcement action, the Commission wrote:

Watchers for Illegally Collecting Kids' Sensitive Health Data (Mar. 4, 2022), https://perma.cc/7FDC-99Y7.

257. *See* Samuel Levine, Dir., Bureau of Consumer Protection, FTC, Remarks at Harvard Law School: Beyond the FTC: The Future of Privacy Enforcement (Apr. 1, 2023), https://perma.cc/AT3C-AU9R.

258. *Id.*

259. Susan Ross & David Kessler, *Two FTC Complaints that Over-Retention of Personal Data Violates Section 5*, NORTON ROSE FULBRIGHT (Feb. 13, 2024), https://perma.cc/PZ6M-PU8S.

260. Complaint ¶¶ 29-31, Blackbaud, Inc., FTC File No. 2023181 (May 17, 2024); Press Release, FTC, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://perma.cc/8FGP-8SJS.

261. Complaint ¶ 6, United States v. Amazon.com, Inc., No. 23-cv-00811 (W.D. Wash. May 31, 2023). Section 312.10 of COPPA allows for the collection and retention of children's data "for only as long as is reasonably necessary to fulfill the purpose for which the information was collected." Children's Online Privacy Protection Rule, 16 C.F.R. § 312.10 (2013); *see also* Jared Ho, *Under COPPA, Data Deletion Isn't Just a Good Idea. It's The Law*, FTC: BUS. BLOG (May 31, 2018), https://perma.cc/89S8-ZJGE.

262. This was defined as "any model, derived data, or other tool developed using Alexa App Geolocation Information, Voice Information, or a Child's Personal Information." Stipulated Order, United States v. Amazon.com, Inc., at 4, No. 23-cv-00811 (W.D. Wash. May 31, 2023), https://perma.cc/SRY5-JSDV.

> Machine learning is no excuse to break the law. Claims from businesses that data must be indefinitely retained to improve algorithms do not override legal bans on indefinite retention of data. The data you use to improve your algorithms must be lawfully collected and lawfully retained.[263]

The Commission's rulemaking, too, focused on establishing limits and prohibitions on data collection, including through addressing the monetization of data that fuels so much of the collection.[264] For example, the principles advanced in *Alexa* were codified in the FTC's proposed amendments to COPPA.[265] In December 2023, the agency proposed updates to its children's privacy rules to make clear that indefinite retention was unlawful and that firms should retain personal information only for as long as necessary to fulfill the specific purpose for which it was collected.[266] To ensure accountability, the rule also would require operators to make public a written data retention policy for children's personal information.[267] These COPPA updates were finalized in January 2025.[268]

Beyond enforcement and rulemaking, the Commission also advanced this work through public notices and policy statements. For example, the Commission issued a policy statement making clear that EdTech providers could not condition access to educational tools on collecting more information than is reasonably necessary.[269] It issued repeated warnings to industry noting that indefinite retention and over-collection can violate the law.[270] It issued a Policy Statement on Biometric Surveillance warning that "[c]ollecting or retaining biometric information without any legitimate business need or keeping that information indefinitely creates an increased risk of harm to

263. FTC, Statement of Commissioner Alvaro M. Bedoya Joined by Chair Lina M. Khan and Commissioner Rebecca Kelly Slaughter: In the Matter of Amazon Alexa (*United States v. Amazon.com, Inc.*) (May 31, 2023), https://perma.cc/RL8Y-PVK9.

264. *See, e.g.*, Press Release, FTC, FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data (Dec. 20, 2023), https://perma.cc/5TM8-EKBW; *Commercial Surveillance and Data Security Rulemaking*, FTC (Aug. 11, 2022), https://perma.cc/B2AP-2A2X.

265. *See* Press Release, *supra* note 264.

266. *Id.*

267. *Id.*

268. *See supra* notes 48-63 and accompanying text; *supra* notes 123-32 and accompanying text.

269. FTC, Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act (May 19, 2022), https://perma.cc/44AK-JJW2.

270. Lesley Fair, *Out of the Mouths of Babes? FTC Says Amazon Kept Kids' Alexa Voice Data Forever—Even After Parents Ordered Deletion*, FTC: BUS. BLOG (May 31, 2023), https://perma.cc/A96B-Z8ER; *see also* Elisa Jillson, *Hey, Alexa! What Are You Doing With My Data?*, FTC: BUS. BLOG (June 13, 2023), https://perma.cc/8C4C-THUU.

consumers."[271] The Commission also warned automakers that they "do not have the free license to monetize people's information beyond purposes needed to provide their requested product or service," raising particular concerns about their collection of sensitive geolocation data.[272]

As new AI tools soared in usage, the FTC issued timely notices explaining how its existing authorities could apply in these new contexts.[273] For example, following the release of ChatGPT in late 2022, the agency saw firms racing to horde data in order to train their models. In response, the FTC published guidance making clear that it may be unfair or deceptive for a company to start sharing consumers' data with third parties or using that data for AI training by making retroactive changes to its privacy policy.[274]

Much of this work culminated in a landmark 2024 report examining the data practices of social media and video streaming services.[275] For the first time in the Commission's history, the FTC called for baseline protections "against the over-collection, monetization, disclosure, or undue retention of personal data."[276] The recommendation signaled a break from the "notice-and-consent" approach.

By 2023 and 2024, securing substantive limitations on certain data practices formed the heart of the FTC's data privacy and security work.[277] This work also had spillover effects. Both major privacy bills advanced during this period—the American Data Privacy and Protection Act and American Privacy Rights Act—required that firms limit their data collection and made the FTC the primary enforcer and administrator.[278] States also enacted privacy laws

271. FTC, Policy Statement of the Federal Trade Commission on "Biometric Information and Section 5 of the Federal Trade Commission Act," at 9 n.45 (May 18, 2023), https://perma.cc/LAZ8-48TK.

272. Off. of Tech. & Div. of Priv. & Identity Prot., *Cars & Consumer Data: On Unlawful Collection & Use*, FTC: TECH. BLOG (May 14, 2024), https://perma.cc/Y9V8-MWSN.

273. *See, e.g.*, Press Release, FTC, FTC Launches New Office of Technology to Bolster Agency's Work (Feb. 17, 2023), https://perma.cc/K8M5-SDJ6.

274. Off. of Tech. & Div. of Priv. & Identity Prot., *supra* note 7; Eli Tan, *When the Terms of Service Change to Make Way for A.I. Training*, N.Y. TIMES (June 26, 2024), https://perma.cc/2E9X-BNH2.

275. FTC, A LOOK BEHIND THE SCREENS: EXAMINING THE DATA PRACTICES OF SOCIAL MEDIA AND VIDEO STREAMING SERVICES (2024), https://perma.cc/HS4P-J9YA. The report was issued by the Commission but was written by staff and reflected staff recommendations.

276. *Id.* at 80; *see also* Cecilia Kang, *F.T.C. Study Finds 'Vast Surveillance' of Social Media Users*, N.Y. TIMES (Sept. 23, 2024), https://perma.cc/3FYL-W5DU.

277. *See* FTC, A Record of Results for American Consumers: Remarks of Samuel Levine at the National Advertising Division Annual Conference 8 (2024), https://perma.cc/HVT8-2GAD.

278. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. §§ 101(a), 207(b)(1) (2022); American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. §§ 102(a), 115(b)(1).

similarly enshrining these principles.[279] Moving from procedural check-the-box disclosures to substantive limits was not a new concept, but these efforts collectively illustrate how the FTC's work helped translate the idea into an operative governing framework for policy and enforcement.

2. Bright-line limits on sensitive data uses

The FTC's recent efforts to secure baseline limits on collection and disclosure turned the page on the notice-and-consent regime. A parallel shift can be seen in the agency's efforts to secure bright-line limits on uses of sensitive data—the subject of this Subpart.

The Muris-era approach largely dismissed consumer injuries from privacy abuses that went beyond monetary harm, a decision that has been widely criticized for years. Chris Hoofnagle, for example, criticized the harms-based approach as "reducing the scope of privacy by denying recognition of norms, human rights, and consumer expectations as justifying privacy rights."[280] Other scholars have carefully documented how people can suffer an array of injuries from privacy invasions, including reputational harms;[281] emotional distress;[282] autonomy harms that restrict, undermine, inhibit, or unduly influence people's life choices;[283] discrimination;[284] and relationship harms.[285]

The Commission later retreated from Muris's cramped view of harms cognizable under the FTC Act.[286] In its 2012 privacy report, the agency expressed concern about the sharing of sensitive data—including data related to geolocation, minors, health, and finance—with third parties, suggesting that such data required greater safeguards.[287] The Commission also called for legislation establishing baseline privacy protections.[288]

279. Francis, *supra* note 220 (highlighting that thirteen of the seventeen comprehensive state privacy laws enacted at time of writing were grounded in data minimization principles).

280. HOOFNAGLE, *supra* note 14, at 78.

281. Daniel J. Solove & Danielle Citron Keats, *Privacy Harms*, 102 B.U. L. REV. 793, 837-41 (2021) (describing reputational harms).

282. *Id.* at 841.

283. *Id.* at 845.

284. *Id.* at 855.

285. *Id.* at 859.

286. *See* FTC, *supra* note 149, at 8 ("The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data.").

287. *Id.* at 59-60.

288. *Id.* at 12-13.

In the years since, Congress failed to pass any legislation limiting the collection or sale of sensitive consumer data. Meanwhile, the rise and expansion of mobile devices, coupled with the business models premised on endlessly monetizing people's personal data, made the collection of sensitive data ever more invasive, constant, and ubiquitous.[289]

Early in Chair Khan's tenure, agency leadership made clear that limiting abuses of sensitive data would be a priority. In a 2022 speech, Director Levine warned industry that "if your privacy and data security practices can cause harm to consumers, the FTC can take action—regardless of whether these practices are disclosed."[290] He zeroed in on the Commission's plan to use unfairness: "You can expect that the Commission's unfairness authority will be a key tool as we work to curb harmful commercial surveillance practices."[291] Chair Khan similarly previewed a shift away from a notice-and-consent-based regime.[292]

The centrality of unfairness in the agency's new approach to safeguarding sensitive data can be seen in how the FTC handled two cases with similar fact patterns: *Flo Health*, in 2021, and *Premom*, in 2023. Both Premom and Flo Health were fertility-tracking apps accused of sharing highly sensitive health data, including menstrual cycles, with Google and others.[293] But the differences in

289. *See generally* FTC, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 1-5 (2016), https://perma.cc/RXP4-DKJH (discussing the ways companies are collecting new behavioral and consumer data types, and how such data may be used); *id.* at 10 (noting how big data may be used to expose users' sensitive information by, for example, combining their Facebook "likes" with survey data to determine their ethnic origin, religious or political affiliations, or use of alcohol, drugs, or cigarettes).

290. Samuel Levine, Dir., Bureau of Consumer Prot., FTC, Keynote Remarks at Federal Trade Commission Cleveland-Marshall College of Law Cybersecurity and Privacy Protection Conference 9 (May 19, 2022), https://perma.cc/H3YK-AMPH.

291. *Id.*

292. Khan, *supra* note 245, at 6 ("[W]e need to reassess the frameworks we presently use to assess unlawful conduct. Specifically, I am concerned that present market realities may render the 'notice and consent' paradigm outdated and insufficient. Many have noted the ways that this framework seems to fall short, given both the overwhelming nature of privacy policies—and the fact that they may very well be beside the point. . . . Going forward, I believe we should approach data privacy and security protections by considering substantive limits rather than just procedural protections, which tend to create process requirements while sidestepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place.").

293. Complaint ¶¶ 2-4, Flo Health Inc., FTC File No. 1923133 (June 17, 2021) [hereinafter Flo Health Complaint]; Complaint for Permanent Injunction, Civil Penalty Judgment, & Other Relief ¶¶ 2-5, United States v. Easy Healthcare Corp., No. 23-cv-3107 (N.D. Ill. May 17, 2023), ECF No. 1 [hereinafter Easy Healthcare Complaint]; *see also* Press Release, FTC, Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of Their Health Data (Jan. 13, 2021), https://perma.cc/BJQ9-XQ4H.

these cases reveal the sea change that transpired in the Commission's approach between 2021 and 2023.

The first change relates to how the Commission pled the illegality of the underlying conduct. The *Flo Health* complaint charged the company with misrepresenting its data uses.[294] In particular, Flo was accused of deceptively sharing the health information of users with outside data analytics providers after promising that such information would be kept private.[295] In *Premom*, the firm's data sharing was charged as unfair in addition to being deceptive—implying that disclosure alone would not cured the illegality of sharing sensitive health data.[296] As Alicia Solow Niederman would later observe, "this theory of harm differs tremendously from past theories that focus on impediments to consumer choice or transparency" and "may have moved the Overton Window of Enforcement Possibility."[297]

A second change involved the relief. Under the FTC's settlement with Flo, the company was required to obtain users' consent before sharing consumers' sensitive health information.[298] Premom faced a much more stringent requirement: an outright ban on the sharing of personal health data for advertising purposes.[299]

The differences between the two matters illustrate the paradigm shift underlying the FTC's data privacy work.[300] While Flo signaled to the market that firms must provide notice and obtain consent before disclosing health information,[301] it did not actually limit the company's ability to share that data—nor its incentive to collect it.[302] By directly limiting the firm's use of

294. Flo Health Complaint, *supra* note 293, ¶¶ 51-65.

295. *Id.* ¶¶ 51-52.

296. *See* Easy Healthcare Complaint, *supra* note 293, ¶¶ 64-88.

297. Alicia Solow-Niederman, *The Overton Window and Privacy Enforcement*, 37 HARV. J. L. & TECH. 1007, 1036 (2023).

298. Press Release, *supra* note 293; Press Release, FTC, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021), https://perma.cc/9DN9-YWCF [hereinafter FTC Finalizes Order with Flo Health]; *see also* Agreement Containing Consent Order, attach. Decision and Order 4, Flo Health Inc., FTC File No. 1923133 (June 17, 2021), https://perma.cc/7HFX-FKGG (proposed consent agreement).

299. Premom Proposed Order Press Release, *supra* note 256; Stipulated Order for Permanent Injunction, Civil Penalty Judgment & Other Relief at 8, United States v. Easy Healthcare Corp., No. 23-cv-3107 (N.D. Ill. May 17, 2023), ECF No. 3-1.

300. A third key difference between these cases is the use of the Health Breach Notification Rule, discussed below. *See infra* notes 460, 464 and accompanying text.

301. Fran Faircloth & Kevin Frazier, *Recent FTC Settlement with Flo Health Focuses on Notice and Consent for Companies Sharing Sensitive Data*, ROPES & GRAY: ROPESDATAPHILES (Aug. 2, 2021), https://perma.cc/LA7Y-BFBF.

302. *See* FTC Finalizes Order with Flo Health, *supra* note 298.

sensitive data, the *Premom* remedy secured a substantive restriction in lieu of a procedural one.[303]

The approach the Commission took in *Premom*—prioritizing bright-line limits over disclosures—became the norm during Chair Khan's tenure. Over the course of that period, the Commission would bring twelve actions challenging the unfair use or sharing of sensitive data.[304] And in each of these cases that reached final judgment, the resulting order placed bright-line limits on future uses of such data.[305] These actions, paired with consistent market alerts, helped establish a new baseline standard around the protection of consumers' sensitive data.[306]

One major area of this work centered on the impermissible disclosure of sensitive geolocation data. Surveillance of geolocation data has long been

303. *See* Stipulated Order for Permanent Injunction, Civil Penalty Judgment & Other Relief, *supra* note 299, at 1, 10.

304. *See* Press Release, FTC, FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent (Jan. 16, 2025), https://perma.cc/72Z6-UGC8; Press Release, FTC, FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data (Jan. 14, 2025), https://perma.cc/GD8J-NHKH; Press Release, FTC, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites (Dec. 3, 2024), https://perma.cc/5AQG-UZGH [hereinafter Gravy Analytics Proposed Order Press Release]; Press Release, FTC, FTC Finalizes Order with Avast Banning It from Selling or Licensing Web Browsing Data for Advertising and Requiring It to Pay $16.5 Million (June 27, 2024), https://perma.cc/YMW3-LU7E; InMarket Order Press Release, *supra* note 256; Press Release, FTC, Proposed FTC Order will Prohibit Telehealth Firm Cerebral from Using or Disclosing Sensitive Data for Advertising Purposes, and Require It to Pay $7 Million (Apr. 15, 2024), https://perma.cc/WJ2V-AQRH [hereinafter Cerebral Proposed Order Press Release]; Press Release, FTC, FTC Finalizes Order with X-Mode and Successor Outlogic Prohibiting It from Sharing or Selling Sensitive Location Data (Apr. 12, 2024), https://perma.cc/3DEY-75UT; Press Release, FTC, Alcohol Addiction Treatment Firm Will Be Banned from Disclosing Health Data for Advertising to Settle FTC Charges that It Shared Data Without Consent (Apr. 11, 2024), https://perma.cc/A6WK-P4R4 [hereinafter Monument Settlement Press Release]; Rite Aid Proposed Order Press Release, *supra* note 256; BetterHelp Order Press Release, *supra* note 256; Premom Proposed Order Press Release, *supra* note 256; GoodRx Enforcement Action Press Release, *supra* note 256.

305. For example, in cases against GoodRx, Premom, Monument, Cerebral, and others, the FTC secured orders prohibiting the sharing of sensitive health data for advertising purposes. *See, e.g.*, GoodRx Enforcement Action Press Release, *supra* note 256; Premom Proposed Order Press Release, *supra* note 256; Monument Settlement Press Release, *supra* note 304; Cerebral Proposed Order Press Release, *supra* note 304.

306. *See, e.g.*, Glenn A. Brown, Kristin Bryan, Kyle Dull & Alan Friel, *Sensitive Data Processing Is in the FTC's Crosshairs*, SQUIRE PATTON BOGGS: PRIV. WORLD (Feb. 9, 2024), https://perma.cc/ZMR7-UQK8; Kate Lucente, Lea Lurquin, Madison Bucci & Matt Dhaiti, *US: The FTC Cracks Down on Sensitive Personal Information Disclosures,* DLA PIPER: PRIVACY MATTERS (Apr. 26, 2024), https://perma.cc/Y96Y-NJW6 ("The Federal Trade Commission . . . is taking bold actions to challenge business's collection and monetization of consumers' personal data—particularly sensitive personal data.").

recognized as a particular invasion of privacy, given the ways that this data can reveal the "privacies of life."[307] The Supreme Court's decision in *Dobbs* gave fresh urgency to these concerns, with some fearing that the unregulated sale of people's location data would heighten the risk that Americans seeking reproductive care would be tracked and prosecuted.[308]

In August 2022, the Commission sued Kochava, a major data broker, for indiscriminately selling precise geolocation data in a manner that could reveal individuals' visits to abortion clinics, churches, drug treatment centers, and other sensitive locations.[309] The complaint was predicated on unfairness alone, an unusual move for the agency.[310] Kochava made clear that it was fighting back.[311]

The FTC's *Kochava* action remains in active litigation, and the final outcome is uncertain. But the case has already delivered a major doctrinal advance. Denying Kochava's motion to dismiss in February 2024, the court found that the invasion of privacy alone can constitute "injury" under the FTC Act, without the need to show secondary negative effects, such as stalking or identity theft.[312] The ruling is a watershed development for privacy enforcement at the FTC—and a direct rejection of the Muris framework, which treated invasions of privacy as cognizable injuries only if they resulted in some separate downstream harm.

This decision not only allowed the Commission to proceed with its action against Kochava but also broke new ground in the agency's use of its unfairness authority.[313] But by the time the decision was issued, the Commission had

307. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2217, 2221-23 (2018) (holding that the government must generally obtain a warrant in order to collect historical cell-site location information) (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

308. Corin Faife, Russell Brandom, Nicole Westman & Mary Beth Griggs, *The Biggest Privacy Risks in Post-Roe America: Our Best Advice for Staying Safe While You're Seeking Abortion Care*, THE VERGE (June 27, 2022, 12:47 PM PDT), https://perma.cc/4W28-GNPZ; Jay Edelson, *Post-Dobbs, Your Private Data Will Be Used Against You,* BLOOMBERG LAW (Sept. 22, 2022, 1:00 AM PDT), https://perma.cc/YAU5-N3M2; Nico Grant, *Google Says It Will Delete Location Data When Users Visit Abortion Clinics*, N.Y. TIMES (July 1, 2022), https://perma.cc/6JTR-7XXV.

309. Press Release, FTC, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://perma.cc/G5P8-RCBX.

310. Complaint for Permanent Injunction & Other Relief ¶¶ 36-38, FTC v. Kochava Inc., 715 F. Supp. 3d 1319 (D. Idaho 2024) (No. 22-cv-00377); Brown et al., *supra* note 306 (noting the absence of a deception allegation).

311. Charles Manning, *Open Letter from Kochava CEO*, KOCHAVA (Sept. 20, 2022), https://perma.cc/GX7W-CH38.

312. *Kochava*, 715 F. Supp. 3d at 1324.

313. *See, e.g.*, Brown et al, *supra* note 306 ("By choosing to litigate Kochava solely based on an unfairness claim (and not deception) the FTC has the potential for establishing judicial

footnote continued on next page

already achieved significant wins in the battle against unlawful sharing of sensitive geolocation data. In the first two months of 2024, the Commission announced two landmark settlements with major data brokers—InMarket and X-Mode.[314] Each included novel and forward-leaning relief.

In *X-Mode*, the FTC charged the data broker with unlawfully selling precise location data that could be used to track people's visits to sensitive locations such as medical and reproductive health clinics, places of religious worship, and domestic abuse shelters.[315] Notably, the Commission secured an order *banning* the sale of sensitive geolocation data altogether—a continued break from the "notice-and-consent" remedies that simply required that the firm better disclose how the data could be collected and used. The order also required the firm to delete data it had already collected, introduced screening requirements around data suppliers, and directed that algorithms trained on unlawfully collected data be destroyed.[316]

Around the same time, the Commission announced an action against InMarket.[317] The complaint charged the data broker with unlawfully handling sensitive geolocation data, including by building profiles of consumers based on criteria such as "Christian church goers" and "wealthy and not healthy."[318] As in *X-Mode*, the FTC's order banned the company from selling or licensing precise geolocation data. It also banned InMarket from selling any profiles of consumers based on sensitive data and required the deletion of both geolocation data and models trained on such data.[319]

The Commission's enforcement actions taking on the indiscriminate disclosure of geolocation data have led industry players to change course. In early 2024, the Network Advertising Initiative (NAI)—a major self-regulatory organization[320]—announced it would be developing new guidance on location

precedent that privacy harms are cognizable and significant and can outweigh any benefits to competition or consumers, greatly expanding the FTC's authority to regulate privacy matters.").

314. InMarket Order Press Release, *supra* note 256; Press Release, FTC, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://perma.cc/7E6V-Y3GD.

315. Complaint ¶¶ 5, 17, X-Mode Social, Inc., FTC File No. 212-3038 (Apr. 11, 2024), https://perma.cc/QH6N-QRSU.

316. Press Release, *supra* note 314.

317. *See* Complaint, InMarket Media, LLC, FTC File No. 202-3088 (Apr. 29, 2024), https://perma.cc/M8PC-KCCJ.

318. *Id.* ¶¶ 8, 31-32.

319. Press Release, FTC, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (Jan. 18, 2024), https://perma.cc/W9WC-EU7X.

320. The Network Advertising Initiative is an industry trade group founded in 2000 that develops self-regulatory standards for online advertising. *About the NAI*, NETWORK ADVERT. INITIATIVE, https://perma.cc/XNB6-NGZE (archived Apr. 18, 2025).

data in response to the Commission's work in addition to changing state law.[321] And in late 2024, NAI released the guidance and announced that five major brokers had voluntarily adopted it.[322]

The Commission took a similar approach to the protection of other forms of sensitive data. The agency brought five major actions banning the disclosure of sensitive health data, including mental health data, for advertising purposes,[323] and collaborated with the Department of Health and Human Services to put other market participants on notice.[324] The FTC deployed its Penalty Offense Authority to warn against the misuse of sensitive financial information.[325] And the Commission accused a software provider of selling browsing data that could reveal religious beliefs, health concerns, political leanings, location, financial status, and other sensitive personal details, securing a ban on such sales and $16.5 million in redress.[326]

The FTC's shift in how it approaches sensitive data is a departure from the recent past and represents an even greater break from the Muris era. Prior Commissions championed self-regulation as adequate to protect consumer privacy, focused on securing better disclosures rather than issuing substantive bans, and sought to address downstream conduct like fraud and robocalls while ignoring the upstream data abuses driving the illegal conduct. The Commission's framework for data privacy enforcement has turned the page from the prior approach, focusing on key drivers of illegal conduct and reinvigorating its unfairness authority to prohibit abusive practices.[327] This shift is evident in the Commission's recent actions around the misuse of sensitive data, where the agency targeted the upstream privacy invasions *before*

321. *NAI Working with Members to Develop New Industry Guidelines for Sensitive Location Data,* NETWORK ADVERT. INITIATIVE (Jan. 24, 2024), https://perma.cc/F6ZR-VP6F.

322. *NAI Updates Location Data Privacy Standards Providing Additional Clarity for Identification of Sensitive Points of Interest*, NAI (Oct. 18, 2024), https://perma.cc/4EQE-F5ZJ.

323. *See* GoodRx Enforcement Action Press Release, *supra* note 256; Premom Proposed Order Press Release, *supra* note 256; Monument Settlement Press Release, *supra* note 304; BetterHelp Order Press Release, *supra* note 256; Proposed FTC Order Will Prohibit Cerebal, *supra* note 304.

324. Press Release, FTC, FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies (July 20, 2023), https://perma.cc/R98M-W6AF.

325. Press Release, FTC, FTC Warns Tax Preparation Companies About Misuse of Consumer Data (Sept. 18, 2023), https://perma.cc/G2V7-KKZ8.

326. Press Release, FTC, FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay $16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking (Feb. 22, 2024), https://perma.cc/R98M-W6AF.

327. *See* FTC, The National Advertising Division Annual Conference: A Progress Report on Key Priorities, and a Warning on AI Self-Regulation 8-9 (2023), https://perma.cc/Z7RK-QTHA (remarks of Samuel Levine, Dir., Bureau of Consumer Prot.).

they manifested in fraud, identity theft, or other abuses, preventing the secondary harm rather than seeking to rectify it after the fact.[328]

B. Combatting Manipulative Digital Design

The extensive harvesting of Americans' personal data also fuels firms' growing ability to manipulate consumer behavior through data-driven design interfaces.[329] In some cases this can be innocuous and even beneficial for consumers—such as, for example when firms conduct A/B testing on different web designs to enhance usability.[330] Yet this same testing can also be used to steer user behavior in troubling ways, such as to coerce consumers into disclosing information they would prefer to withhold, or to keep them enrolled in a subscription they want to cancel.[331] These manipulative design techniques have been described as "dark patterns," and they can be turbocharged through massive data extraction.[332]

The term "dark patterns" was coined by Harry Brignull in 2010,[333] spurring a wider body of scholarship.[334] Jennifer King and Adriana Stephan have examined dark patterns in the broader context of "persuasive technology"—the use of digital devices to shape behavior—or "choice architecture[]," the context in which people make decisions.[335] Richard Thaler and Cass Sunstein have written extensively on choice architecture, warning against "[w]ily but malevolent nudgers" who can manipulate consumers into

328. For example, it was reported in 2025 that Gravy Analytics—a major broker—suffered a breach, revealing at least 30 million location data points and endangering both privacy and national security. Zack Whittaker, *A Breach of Gravy Analytics' Huge Trove of Location Data Threatens the Privacy of Millions,* TECHCRUNCH (Jan. 13, 2025, 4:35 AM PST), https://perma.cc/4EVC-ULZ5. Weeks earlier, the FTC had proposed an order limiting Gravy's collection and sale of sensitive consumer information. Gravy Analytics Proposed Order Press Release, *supra* note 304.

329. *See* FTC, BRINGING DARK PATTERNS TO LIGHT 2 (2022), https://perma.cc/A6HY-6RMM ("Moreover, companies that market online can experiment with digital dark patterns more easily, frequently, and at a much larger scale than traditional brick-and-mortar retailers, to determine which design features most effectively influence consumer behavior.").

330. Jennifer King & Adriana Stephan, *Regulating Privacy Dark Patterns in Practice—Drawing Inspiration from California Privacy Rights Act,* 5 GEO. L. TECH. REV. 250, 254-55 (2021).

331. *Id.* at 254-58.

332. *See* FTC, *supra* note 329 at 2 ("The pervasive nature of data collection techniques, which allow companies to gather massive amounts of information about consumers' identities and online behavior, enables businesses to adapt and leverage advertisements to target a particular demographic or even a particular consumer's interests.").

333. King & Stephan, *supra* note 330, at 254-58.

334. *See, e.g., id.* at 254-57; Katri Nousiainen & Catalina Perdomo Ortega, *Dark Patterns in Law and Economics Framework*, 36 LOY. CONSUMER L. REV. 90, 90-98 (2023).

335. King & Stephan, *supra* note 330, at 257.

taking actions that go against their own interests.[336] Other scholars have attempted to apply a law and economics lens to the concept of dark patterns, viewing it as a market distortion that exploits cognitive biases.[337]

Scholars have also warned that it may be challenging for government to confront these patterns absent new authority. For example, King and Stephan examined whether the FTC could combat dark patterns through existing authorities,[338] noting that design elements do not always involve actionable deceptive claims,[339] and that the FTC has historically been reluctant to use its unfairness authority.[340] Drawing on several other scholars, they suggest the agency may need to be granted authority to combat "abusive" practices—akin to an authority given to the Consumer Financial Protection Bureau—to address manipulative practices.[341]

Perhaps for these reasons, the FTC did not explicitly address the use of dark patterns until 2020. That year, the Commission brought a case challenging, *inter alia*, a firm's use of design interfaces that impeded consumers' ability to cancel their subscription to its service.[342] While the complaint did not refer to "dark patterns,"[343] then-Commissioner Rohit Chopra issued an associated statement urging the Commission to "methodically use all of our tools to shine a light on unlawful digital dark patterns" and "contain the spread of this popular, profitable, and problematic business practice."[344]

The following year, under the leadership of Acting Chair Rebecca Kelly Slaughter, the Commission held its first-ever workshop on dark patterns in April 2021.[345] The momentum continued once Chair Khan took office, with

336. Richard H. Thaler, Cass R. Sunstein & John P. Balz, *Choice Architecture*, *in* THE BEHAVIORAL FOUNDATIONS OF PUBLIC POLICY 428, 430 (Eldar Shafir ed., 2013).

337. Nousiainen & Ortega, *supra* note 334, at 99.

338. King & Stephan, *supra* note 330, at 262-63.

339. *Id.* at 262.

340. *Id.* at 262 & n.36 (citing J. Howard Beales III, *The Federal Trade Commission's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J. PUB. POL'Y & MKTG. 192, 193 (2003)).

341. *Id.* at 258.

342. Complaint for Permanent Injunction & Other Equitable Relief at 1-3, FTC v. Age of Learning, Inc., No. 20-cv-7996 (C.D. Cal. Sept. 1, 2020), ECF No. 1.

343. *See id.*

344. FTC, Statement of Commissioner Rohit Chopra: Regarding Dark Patterns in the Matter of Age of Learning, Inc. 3 (2020), https://perma.cc/8K62-9XF9.

345. *See, e.g.*, *Bringing Dark Patterns to Light: An FTC Workshop*, FTC (Apr. 29, 2021), https://perma.cc/S2DM-3PSS.

the Commission publicly announcing that it would be prioritizing scrutiny of dark patterns and ramping up enforcement.[346]

In 2022, the Bureau of Consumer Protection issued a major report—*Bringing Dark Patterns to Light*[347]—that provided a taxonomy of the types of dark patterns the agency was seeing across markets. The report identified a range of potentially unlawful practices, including dark patterns that induce false beliefs about urgency or scarcity, that hide or delay disclosure of material information, or that enable unauthorized charges.[348] The report concluded by warning firms that they could face FTC lawsuits for the harmful use of deceptive design interfaces.[349]

Over the next three years, tackling dark patterns was a key priority for the Commission. The agency reinvigorated its unfairness authority and strategically targeted some of the most egregious dark patterns—especially those that cause financial harm—to help establish the viability of using unfairness to combat harmful design practices.

Several early cases illustrate this strategy. In a major action against internet phone service provider Vonage, the FTC in 2022 charged the company with using a host of dark patterns to thwart people who tried to cancel their services.[350] These included eliminating cancellation options, making the cancellation process difficult, surprising customers with expensive junk fees when they tried to cancel, continuing to charge customers even after they cancelled to make cancellation more difficult, and racking up charges against consumers without consent.[351] The complaint details a number of these design practices, including (1) allowing online enrollment but not cancellation, (2) thwarting customers' ability to connect to a live agent through circuitous transfers and dropped calls, and (3) inserting small print disclosures about early termination without mention of fees—thus ultimately creating an "endless

346. *See, e.g.*, Press Release, FTC, FTC to Ramp up Enforcement Against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions (Oct. 28, 2021), https://perma.cc/UK2Q-8QQY; David Ingram, *'Dark Patterns': Regulators Eye Tech Tricks That Hurt Consumers*, NBC NEWS (Nov. 6, 2021, 6:27 AM PDT), https://perma.cc/W7LC-QF8X.

347. *See* FTC, *supra* note 329.

348. *Id.* app. A at 21-24.

349. Press Release, FTC, FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers (Sept. 15, 2022), https://perma.cc/83ZN-ZR43.

350. Complaint for Permanent Injunction, Monetary Relief & Other Relief at 7-17, FTC v. Vonage Holdings Corp., No. 22-cv-6435 (D.N.J. Nov. 3, 2022), ECF No. 1.

351. Press Release, FTC, FTC Sends Nearly $100 Million in Refunds to Vonage Consumers Who Were Trapped in Subscriptions by Dark Patterns and Junk Fees (Oct. 30, 2023), https://perma.cc/XFD7-M53Y.

loop" of hurdles.[352] The Commission's complaint alleged that Vonage engaged in an unfair practice by charging consumers without their consent.[353]

The complaint details why this conduct meets the three-part test for unfairness: Consumers suffered injury in the form of unauthorized charges; the injury was not avoidable given the manipulative practices; and unauthorized charges offer no benefits to consumers or competition. [354]

The next year the FTC sued Amazon and three executives for deploying a host of dark patterns to enroll consumers into its Prime program without their consent while knowingly making it difficult for consumers to cancel their subscriptions to Prime.[355] The complaint notes that Amazon used a variety of dark patterns, such as requiring consumers to either accept or decline a subscription before they could continue shopping, not disclosing the price of the monthly auto-renewal feature of Prime, and enabling visual elements that could mislead consumers into enrolling without understanding the reoccurring payment default.[356] Amazon referred to its cancellation process as "Iliad," a reference to the epic tale about a legendary war. [357]

Unlike *Vonage*, which settled, the FTC's case against Amazon proceeded into litigation, and it remains in litigation as of this writing. The agency's ability to combat dark patterns became a key battle line, with Amazon claiming the FTC's dark patterns theory was "unconstitutionally vague" and violated Amazon's due process rights because the FTC did not provide "fair notice" of this theory.[358] Filing an amicus brief in support of Amazon, the Chamber of Commerce urged the court to reject the FTC's effort to regulate "so-called 'dark patterns'" through enforcement.[359]

The court wholly rejected the efforts by Amazon and allied amici to dismiss the complaint.[360] Legal observers saw this victory as strengthening the

352. Complaint for Permanent Injunction, Monetary Relief, & Other Relief, *supra* note 350, at 7-17.

353. *Id.* at 1-2.

354. *Id.* at 17-18.

355. Press Release, FTC, FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel (June 21, 2023), https://perma.cc/8J7B-MW5L.

356. Complaint for Permanent Injunction, Civil Penalties, Monetary Relief, & Other Equitable Relief at 6-8, 24, 35, FTC v. Amazon.com, Inc., No. 23-cv-0932 (W.D. Wash. June 21, 2023), ECF No. 1.

357. *Id.* at 3.

358. FTC v. Amazon.com, Inc., 735 F. Supp. 3d 1297, 1314 (W.D. Wash. 2023).

359. Brief of Amicus Curiae the Chamber of Commerce of the United States of America in Support of Defendants' Motion to Dismiss at 2-3, FTC v. Amazon.com, Inc., 735 F. Supp. 3d 1297 (No. 23-cv-0932).

360. *Amazon.com*, 735 F. Supp. 3d at 1334.

FTC's hand as it challenged dark patterns elsewhere,[361] with one law firm noting the FTC's win advancing its "groundbreaking case."[362]

The agency's enforcement strategy began with a focus on dark patterns that cost consumers money and then expanded to those manipulative design techniques that undermine people's privacy. For example, in 2023 the Commission took action against BetterHelp, a mental health platform providing counseling and therapy online. The FTC charged the company with unfairly sharing consumers' sensitive health data with Facebook and others for targeted advertising.[363] The agency specifically took aim at BetterHelp's deceptive design techniques, where the firm prominently promised users that their sensitive data would be protected and then buried inadequate disclosures in lengthy terms of service.[364]

The FTC order resolving the charges points to a new paradigm for privacy protection—one that limits both the use of manipulative dark patterns as well as the indiscriminate sharing of sensitive health data. First, as with *GoodRx* and other recent health privacy cases, the order bans BetterHelp from sharing sensitive health data for advertising purposes and requires the company to retain covered information only as long as necessary to fulfill the purpose for which it was collected.[365] Notably, the order also targets manipulative design techniques directly by prohibiting firms from using dark patterns to obtain user consent. If BetterHelp seeks to disclose sensitive data for purposes not prohibited under the order, it must obtain a user's affirmative express permission and is barred from doing so "through a user interface that has the effect of subverting or impairing user autonomy, decision-making, or choice."[366]

The FTC also harnessed its rulemaking authority to crack down on harmful dark patterns. Building on its work against Vonage and other cases involving subscription traps, the FTC in 2024 finalized a rule requiring that

361. *See, e.g.*, Xu Yuan & Mike Swift, *Comment: Amazon's Latest Defeat in 'Dark Patterns' Action by US FTC Sets Potentially Important Precedent for Future Litigation,* MLEX (June 3, 2024, 10:30 PM GMT), https://perma.cc/WMD5-RNDU; Edward D. Rogers, Erin L. Fischer & Edmund Nyarko, *The Iliad Flows: Federal Judge Allows FTC "Dark Patterns" Suit Against Amazon to Proceed*, BALLARD SPAHR (May 30, 2024), https://perma.cc/NJT6-G9HM.

362. Rogers et al., *supra* note 361, at 1.

363. BetterHelp Order Press Release, *supra* note 256.

364. Complaint ¶¶ 4, 23-37, 75, BetterHelp Inc., FTC File No. 2023169 (Mar. 2, 2023), https://perma.cc/CTD4-PKWB.

365. BetterHelp Inc., No. C-4796, slip op. at 6, 10 (FTC July 7, 2023), FTC File No. 2023169 (decision and order).

366. *Id.* at 7.

businesses make subscriptions as easy to cancel as they are to enroll in.[367] This "Click to Cancel" effort was notable for several reasons.

First, it represented a new strategy for the agency. The Commission had spent years urging sellers to make subscriptions easier to cancel,[368] but unlawful practices continued and—by some measures—actually worsened.[369] Deploying its rulemaking authority, a step the FTC had been deeply reluctant to take since the 1980s,[370] represented a significant shift.

Second, the FTC's final rule requires substantive rights for consumers, rather than merely requiring disclosures. For example, rather than requiring that firms disclose how consumers can cancel, the rule requires businesses to make their cancellation process simple.[371] The rule also requires symmetry between enrollment and cancellation, so that if consumers can sign up for a service online, they must be able to cancel it online too.[372]

Third, the agency explicitly situated this effort within a broader initiative to eliminate manipulative dark patterns. The final rule notes that the rule's provisions are "consistent with longstanding Commission precedent that consent can be subverted, including by so-called 'dark patterns,'"[373] and prohibits firms from obtaining consumer consent through the use of dark patterns, defined as "any information that interferes with, detracts from, contradicts, or otherwise undermines the ability of consumers to provide their express informed consent to the Negative Option Feature."[374]

---

367. Press Release, FTC, Federal Trade Commission Announces Final "Click-to-Cancel" Rule Making It Easier for Consumers to End Recurring Subscriptions and Memberships (Oct. 16, 2024), https://perma.cc/D2VZ-CMHT.

368. *See, e.g.*, Andrew Smith, *$10 Million ABCmouse Settlement: Avoiding Auto-Renewal Traps,* FTC: BUS. BLOG (Sept. 2, 2020), https://perma.cc/BH7B-ZFAX; Lisa Weintraub Schifferle, *Negative Options—Make Them a Positive*, FTC: BUS. BLOG (Sept. 22, 2016), https://perma.cc/HWR8-GL7X.

369. Public comments on the Commission's advance notice of proposed rulemaking illustrate that complaint volume about free trial offers was rising by multiple measures. *See* Negative Option Rule, 88 Fed. Reg. 24716, 24720-21 (proposed Apr. 24, 2023) (discussing the rising consumer complaints concerning negative option practices).

370. *See, e.g.*, Jon Leibowitz, Chairman, Association of National Advertisers Advertising Law and Public Policy Conference, FTC 2 (Mar. 18, 2010), https://perma.cc/GYZ4-LCWN ("The requirements to promulgate a rule under these procedures are so onerous that the agency has not proposed a new Mag-Moss rule in 32 years.").

371. Press Release, *supra* note 367.

372. *Id.* (noting that under the rule, sellers must "make it as easy for consumers to cancel their enrollment as it was to sign up").

373. Negative Option Rule, 89 Fed. Reg. 90476, 90499 (Nov. 15, 2024) (to be codified at 16 C.F.R. pt. 425).

374. *Id.* at 90538.

The FTC's aggressive approach to policing dark patterns was not without corporate pushback. In addition to objections from defendants in FTC actions, a major trade association warned that the agency was trying to "criminalize design elements such as size and color."[375] The rulemaking process, too, generated opposition as well as enormous support, with more than 16,000 public comments submitted.[376]

The FTC's work here was a critical complement to its efforts to limit expansive tracking and unauthorized use of Americans' personal data. Dark patterns are both a cause and effect of unchecked surveillance—they become increasingly effective as firms amass more user data,[377] and they can be deployed to harvest more data still.[378] The overwhelmingly positive reaction to the FTC's Click-to-Cancel rule suggests widespread consumer frustration with these design tricks.[379]

The Commission's work on dark patterns also marks a firm rejection of the neoclassical approached embraced by Muris and Beales. A core assumption underlying their agenda was that markets will generally self-correct and that consumers can protect themselves so long as they are given accurate information.[380] But dark patterns belie this notion. As scholars have noted, dark patterns prey on cognitive frailties—when "human actions systematically diverge from the *homo economicus*, and thus the economic model."[381] Policymakers may assume that consumers are "discerning and rational in the face of the market's blandishments," but in fact "the new powers in the digital

375. *FTC "Dark Patterns" Theory Crosses Dangerous Constitutional Line, IAB Argues in Amicus Brief to Federal Court*, INTERACTIVE ADVERT. BUREAU (Oct. 27, 2023), https://perma.cc/WS98-FZD4.

376. *See Informal Hearing on Proposed Amendments to the Negative Option Rule,* FTC (Jan. 16, 2024), https://perma.cc/8ZLM-SZNU; Press Release, *supra* note 367 ("Agency acts after receiving more than 16,000 comments from the public.").

377. *See* Arvind Narayanan, Arunesh Mathur, Marshini Chetty & Mihir Kshirsagar, *Dark Patterns: Past, Present, and Future*, 18 ACM QUEUE 67, 76 (2020).

378. *Id.* at 77 ("A less obvious, yet equally pervasive, goal of dark patterns is to invade privacy. For example, cookie consent dialogs almost universally employ manipulative design to increase the likelihood of users consenting to tracking."); *cf.* King & Stephan, *supra* note 330, at 260-61 (noting broad concern with dark patterns designed to induce information disclosure).

379. *See, e.g.*, Kevin T. Dugan, *New Rule Making It Easy to Cancel Subscriptions Is in Danger*, N.Y. MAG.: INTELLIGENCER (Oct. 23, 2024), https://perma.cc/M44W-63KA (describing the FTC's rule as "an enormously popular triumph" over firms that trap consumers in subscriptions).

380. *See* Letter from Pertschuk et al., *supra* note 178 ("Normally we expect the marketplace to be self-correcting, and we rely on consumer choice—the ability of individual consumers to make their own private purchasing decisions without regulatory intervention—to govern the market.").

381. Nousiainen & Ortega, *supra* note 334, at 98.

age have built their business models on strategies—enabled and turbocharged by self-improving algorithms—that actively undermine the principles that make capitalism a good deal for most people."[382]

By focusing on the realities of today's markets—and how practices like "dark patterns" can upend prior assumptions—the Commission's work in this area has already delivered historic wins, with courts recognizing the unfairness and deception of dark patterns as cognizable injuries.

C. Challenging Exploitative and Unfair Practices Targeting Youth Online

The first two pillars of the FTC's revamped approach to consumer protection enforcement in digital markets—prioritizing baseline limits on data collection and tackling manipulative design tactics like dark patterns—benefit all users. But recognizing that younger people are facing unique threats online, the agency has also harnessed its tools to take on exploitative and unfair practices targeting minors.[383]

Parents, teachers, medical professionals, and young people have warned for more than a decade that social media use may pose significant risks to young people.[384] The chorus of voices sounding the alarm on how social media and other online apps and services affect children and teens has grown louder in recent years—triggering policy responses. For example, in 2023 the Surgeon General issued an advisory about the effects of social media on youth mental health.[385] The White House formed a Kids Online Health and Safety Task

382. King & Stephan, *supra* note 330, at 260 (quoting Maya MacGuineas, *Capitalism's Addiction Problem*, ATLANTIC (Apr. 2020), at 10, https://perma.cc/PYM3-8NWM).

383. *See* FTC, Statement of Commissioner Alvaro M. Bedoya: On the 6(b) Report Examining the Data Practices of Social Media and Video Streaming Services 1 (Sept. 19, 2024), https://perma.cc/EFF2-ELN6 (noting "unique risks to kids and teens"); *see also* DEP'T OF HEALTH & HUM. SERVS., ONLINE HEALTH AND SAFETY FOR CHILDREN AND YOUTH: BEST PRACTICES FOR FAMILIES AND GUIDANCE FOR INDUSTRY 10-17 (2024), https://perma.cc/JM8Q-TA2D.

384. *See, e.g.*, Alison V. King, *Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech*, 63 VAND. L. REV. 845, 849-52 (2010) (discussing negative effects of online harassment); Ana Radovic, Theresa Gmelin, Bradley D. Stein & Elizabeth Miller, *Depressed Adolescents' Positive and Negative Use of Social Media*, 55 J. ADOLESCENCE, Feb. 2017, at 5, 5-12 (describing negative effects of social media including, among others, risky behaviors and cyberbullying); Gwenn Schurgin O'Keeffe, Kathleen Clarke-Pearson & Council on Communications and Media, *The Impact of Social Media on Children, Adolescents, and Families*, 127 PEDIATRICS 800, 801-02 (2011) (warning of potential negative effects associated with social media such as cyberbullying and privacy concerns, among others).

385. Press Release, Dep't. Health & Hum. Servs., Surgeon General Issues New Advisory About Effects Social Media Use Has on Youth Mental Health (May 23, 2023), https://perma.cc/DL95-8ZTA.

Force and published a report on the risks that social media poses for youth.[386] Congress extensively discussed and debated specific legislation, including the Kids Online Safety Act (KOSA) and the Children and Teens' Online Privacy Protection Act (COPPA 2.0),[387] to better protect children online. States like New York and California also advanced their own bills to safeguard minors online.[388] At the FTC, Commissioner Alvaro Bedoya warned of a "youth mental health emergency," noting that "suicide is now the second-leading cause of death for children ten to fourteen years of age."[389] He pushed the Commission to hire in-house psychologists, better equipping the agency to assess the potential dangers online services pose to children and teens.[390]

Despite this growing drumbeat of concern, federal legislation ultimately stalled. Neither KOSA nor COPPA 2.0 passed, and the original COPPA covers only children under thirteen.[391] As a result, the law offers teenagers no greater protection than adults, even as teenagers suffer more acute harms.[392]

386. *Kids Online Health and Safety Task Force*, SUBSTANCE ABUSE & MENTAL HEALTH SERVS. ADMIN., https://perma.cc/UL2Z-X6R8 (last updated Dec. 5, 2023).

387. Sarah Jeong, *Congress Moves Forward on the Kids Online Safety Act*, THE VERGE (Sept. 18, 2024), https://perma.cc/5DTX-Q38Y.

388. Press Release, N.Y. State Governor's Press Off., Governor Hochul Joins Attorney General James and Bill Sponsors to Sign Nation-Leading Legislation to Restrict Addictive Social Media Feeds and Protect Kids Online (June 20, 2024), https://perma.cc/6S8D-A3T9; California Age-Appropriate Design Code Act, Assemb. Bill 2273, 2022 Assemb., Reg. Sess. (Cal. 2022) (enacted). The Northern District of California blocked enforcement of the law, but as of writing, the California Attorney General has appealed the decision. Press Release, State of Cal. Dep't of Just. Off. of the Att'y Gen., Attorney General Bonta Appeals Age-Appropriate Design Code Act Decision (Apr. 11, 2025), https://perma.cc/QV2U-BMWM.

389. Alvaro M. Bedoya, Comm'r, FTC, Prepared Remarks for the National Academies of Sciences, Engineering & Medicine Meeting of the Committee on the Impact of Social Media on the Health and Wellbeing of Children & Adolescents 1 (Feb. 7, 2023), https://perma.cc/3ZHL-NXEJ; *see also* Andrea Vittorio, *FTC's Bedoya Wants Study of Social Media's Impact on Kids*, BLOOMBERG L. NEWS (Aug. 9, 2022), https://perma.cc/4HG3-M4GK.

390. Bedoya, *supra* note 389, at 7-8.

391. Press Release, Sen. Ed Markey, Senators Markey and Cassidy Reintroduce COPPA 2.0, Bipartisan Legislation to Protect Online Privacy of Children and Teens (May 3, 2023), https://perma.cc/9FC2-KMGV. As of writing, Senators Markey and Cassidy have continued to push for revisions to COPPA. Press Release, Sen. Ed Markey, Senators Markey and Cassidy Reintroduce Children and Teen's Online Privacy Protection Legislation (Mar. 4, 2025), https://perma.cc/Z7YH-G3Y4.

392. *Id.*; *see also* Bedoya, *supra* note 389, at 3-4 (summarizing literature on the effect of social media on teenagers).

As a more general statute, the FTC Act can reach harms to teens.[393] But harnessing unfairness to these ends surfaces a series of questions, especially given the FTC's post-1980 pronouncements on unfairness.[394]

First, what kind of injury is actionable by the FTC? The agency's 1980 policy statement states explicitly that unfair practices generally involve monetary harm.[395] But the harms teens generally experience online are not strictly monetary, especially when social media services monetize people's data rather than charging a fee.[396] Researchers instead have pointed to harms to mental health[397]—precisely the sort of injury that the 1980 Statement discounts.[398]

Second, can the business practice at issue "cause[]" or be "likely to cause" such injury, as required by the statutory standard?[399] Although there is mounting evidence that social media usage correlates with serious mental health harms,[400] whether that evidence is sufficient for purposes of establishing causality under the unfairness standard remains an open question.

Finally, unfairness requires an analysis of countervailing benefits to consumers and competition.[401] Whereas other practices targeted as unfair—like marketing tobacco to teens[402]—have limited upside, social media can confer certain benefits.[403] Accordingly, the cost-benefit analysis of certain social media practices is not a straightforward exercise.

While these challenges are nontrivial, the agency crafted an investigative strategy to uncover whether certain online business practices expose young

393. *See* 15 U.S.C. § 45(n) (prohibiting practices that cause or are likely to cause unavoidable net harm to consumers, which can of course include teenaged consumers).

394. *See* Letter from Pertschuk et al., *supra* note 178 ("Emotional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair.").

395. *Id.*

396. Mary Clare Peate, *Why Are Some Social Media Sites Free to Use?*, FED. RSRV. BANK ST. LOUIS: ONE PAGE ECON. (May 1, 2023), https://perma.cc/CWY6-QQVE.

397. Kathy Katella, *How Social Media Affects Your Teen's Mental Health: A Parent's Guide*, YALE MED. NEWS (June 17, 2024), https://perma.cc/FBZ6-H2KH.

398. *See* Letter from Pertschuk et al., *supra* note 178.

399. 15 U.S.C. § 45(n).

400. Ujala Zubair, Muhammad K. Khan & Muna Albashari, *Link Between Excessive Social Media Use and Psychiatric Disorders*, 85 ANNALS MED. & SURGERY 875, 875-78 (2023); OFF. SURGEON GEN., SOCIAL MEDIA AND YOUTH MENTAL HEALTH: THE U.S. SURGEON GENERAL'S ADVISORY 4-10 (2023), https://perma.cc/V7ZP-XUS2.

401. 15 U.S.C. § 45(n).

402. *See supra* notes 188-91 and accompanying text.

403. Kirsten Weir, *Protecting Teens on Social Media: New Psychological Research Exposes Harms and Benefits*, 54 MONITOR ON PSYCH. 46, 50 (2023).

people to injury. The Commission mapped out a case-by-case approach that was grounded in specific evidence of harms.

Two cases best illustrate this approach, with both involving novel uses of the FTC's unfairness authority. The first was filed against Epic Games, the maker of the popular video game Fortnite.[404] Epic would pay a record-setting penalty—$275 million—for knowingly collecting personal information from children in violation of COPPA.[405] The Commission also closely examined the other ways the platform was exposing young people to harm.[406] First, the Commission found that Epic was using dark patterns to trick people into making unwanted charges[407] and secured a second order recovering a record-setting $245 million for harmed consumers.[408] Second—and more relevant here—the agency alleged that Epic engaged in an unfair practice when it enabled real-time voice chat communications for children and teens by default.[409]

The Commission's complaint details extensively how this practice caused significant harm to children and teens:

> Children and teens have been bullied, threatened, and harassed within Fortnite, including sexually. Children and teens have also been exposed to dangerous and psychologically traumatizing issues, such as suicide and self-harm, through Fortnite. And the few relevant privacy and parental controls Epic has introduced over time have not meaningfully alleviated these harms or empowered players to avoid them.[410]

On this basis, the Commission alleged that Epic engaged in an unfair practice under the FTC Act.[411] Teens suffered grievous injury, including bullying and harassment.[412] This injury was directly enabled by Epic's default settings, which allowed strangers to communicate with young people through real-time voice chats—a risk that Epic was aware of and declined to address.[413]

---

404. Epic Games Settlements Press Release, *supra* note 256.

405. *Id.*

406. *Id.*

407. Stipulated Order for Permanent Injunction & Civil Penalty Judgment at 2, United States v. Epic Games, Inc., No. 22-cv-00518 (E.D.N.C. Feb. 7, 2023), ECF No. 15 (alleging violations of COPPA).

408. Epic Games, Inc., No. C-4790, slip op. at 4 (FTC Mar. 13, 2023), FTC File No. 192-3203 (alleging unfair billing practices).

409. Complaint for Permanent Injunction, Civil Penalties, Monetary Relief, & Other Relief ¶¶ 68-79, United States v. Epic Games, Inc., No. 22-cv-00518 (E.D.N.C. Dec. 19, 2022), https://perma.cc/8FUR-AVZP.

410. *Id.* ¶ 3.

411. *Id.* ¶¶ 67-70.

412. *Id.* ¶ 40.

413. *See id.* ¶ 37.

This injury was not outweighed by countervailing benefits, especially since the benefits of playing Fortnite could have been realized without exposing young people to bullying and harassment.[414]

Epic demonstrated that unfairness can reach injuries stemming from privacy violations and online harassment.[415] In contrast to the Muris approach—which did not treat online data abuses as meaningful harms—*Epic* illustrated how exposing people online could cause substantial injury.[416]

The following year, the FTC built on this work through its action against NGL, a highly popular social media platform.[417] NGL was an anonymous messaging app that targeted high school teens.[418] As the FTC's complaint describes, NGL executives urged employees to get "kids who are popular to post and get their friends to post" and noted that the "best way is to reach out on [Instagram] by finding popular girls on high school cheer [Instagram] pages."[419]

Users who downloaded the app were encouraged to post questions to their social media followers, such as "If you could change anything about me, what would it be?"[420] Their followers could then respond to such questions anonymously.[421] To generate engagement, NGL also sent individuals fake computer-generated messages that appeared to be from real people.[422] These

414. *Cf.* FTC v. Amazon.com, Inc., No. C14-1038, 2016 WL 10654030, at *10 (W.D. Wash. 2016) (noting that the purported benefits—"a seamless, efficient mobile experience"—could still be achieved even if the injurious practice were fixed, so the benefits were not countervailing); Ohlhausen, *supra* note 161, at 2001 ("[O]nly the practice's effects should be considered under the third prong of the unfairness test and it is inappropriate to weigh other benefits, such as the total benefits of the product or platform itself or benefits of the company's entire line of products.").

415. Epic Games Settlements Press Release, *supra* note 256. This approach secured bipartisan support. *See* FTC, *Concurring Statement of Commissioner Christine S. Wilson Regarding Epic Games, Inc.* (Dec. 19, 2022), https://perma.cc/LZ4A-9PLS.

416. Complaint for Permanent Injunction, Civil Penalties, Monetary Relief, & Other Relief, *supra* note 409, ¶¶ 40-41.

417. Complaint ¶ 25, FTC v. NGL Labs, LLC, No. 24-cv-5753 (C.D. Cal. July 9, 2024), https://perma.cc/AD23-HX9T.

418. *Id.* ¶ 51.

419. *Id.* ¶ 52.

420. *Id.* ¶ 14.

421. *Id.* ¶ 15.

422. *Id.* ¶ 23.

messages included "are you straight?" and "I know what you did."[423] These practices contributed to rampant cyberbullying and threats on the platform.[424]

Faced with these facts, the FTC brought a novel claim: that the company's marketing of anonymous messaging apps to teens was unfair.[425] And the agency's order was equally novel—banning the company from marketing or offering its app to teens.[426]

This action raised thornier questions than those surfaced in *Epic*. Anonymous messaging apps may have some benefits, providing teens with an environment where they can more openly express themselves.[427] And teens could, in theory, avoid the harm—say, by not using the app. Yet, strikingly, the settlement was approved unanimously.[428]

The Commission's full support for the NGL action marked a significant departure from FTC's 1980 statement that financial injury should be the primary basis for unfairness and that emotional impact was too speculative.[429] The harms in this case were emotional.[430] Commissioner Ferguson issued a statement, joined by Commissioner Holyoak, stressing that teenagers are uniquely exposed to these harms—describing the "vulnerable teenage psyche"

423. *Id.*

424. Press Release, FTC, FTC Order Will Ban NGL Labs and Its Founders from Offering Anonymous Messaging Apps to Kids Under 18 and Halt Deceptive Claims Around AI Content Moderation (July 9, 2024), https://perma.cc/4LX5-4ZK5.

425. *See, e.g.*, *In re* NGL Labs, LLC, FTC File No. 2223144 (July 9, 2024) (Ferguson, Comm'r, concurring), https://perma.cc/8JVT-Z48J (describing the unfairness count as "novel").

426. *See, e.g.*, Cecilia Kang, *F.T.C. Bars Anonymous Messaging App From Serving Users Under Age 18*, N.Y. TIMES (July 9, 2024), https://perma.cc/XZM4-9T4G; Emily Litka, *FTC Introduces Novel Ban in Its Settlement with NGL Labs and Scrutinizes AI Representations*, HINTZE LAW (Aug. 19, 2024), https://perma.cc/7GCW-Z5DH; Noah Katz, Rushil Mehta & Stacey Brandenburg, *We're "Not Gonna Lie," FTC's Settlement Contains Novel Requirement for Neutral Age-Gate for U18*, ZWILLGEN BLOG (July 17, 2024), https://perma.cc/A8KR-HHCW.

427. Shelley L. Craig, Andrew D. Eaton, Lauren B. McInroy, Vivian W. Y. Leung & Sreedevi Krishnan, *Can Social Media Participation Enhance LGBTQ+ Youth Well-Being? Development of the Social Media Benefits Scale*, SOC. MEDIA + SOC'Y., Jan.-Mar. 2021, at 2, 8; Matthew N. Berger, Melody Taba, Jennifer L. Marino, Megan S. C. Lim & S. Rachel Skinner, *Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, J. MED. INTERNET RSCH., 2022, at 1.

428. *In re* NGL Labs, LLC, FTC File No. 2223144 (July 9, 2024) (Ferguson, Comm'r, concurring), https://perma.cc/SA6Z-G5EB; Press Release, *supra* note 424.

429. Letter from Pertschuk et al., *supra* note 178 ("Emotional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair.").

430. *See* Complaint, *supra* note 417, ¶¶ 56-57.

and noting that their "brains and ability to assess risk are still developing . . . ."[431]

This case points to a more capacious conception of unfairness, one that can keep pace with the nature of consumer injuries suffered online. As enforcers grapple with the myriad risks associated with young people's use of online apps and services—from addiction and abuse to fraud and bullying—the FTC's unfairness authority—which can account for the vulnerabilities of injured consumers—can be a key tool. The bipartisan support for this application of unfairness, moreover, suggests this forward-leaning work will continue regardless of who leads the FTC.[432]

D. Crafting Effective Relief and Promoting Deterrence

As detailed in Part I, at the dawn of the internet the FTC steadfastly endorsed self-regulation as the best way to protect the public online.[433] But measured against the Commission's own goals, this confidence proved misplaced.[434] In fact, the same year that Tim Muris expressed confidence in industry efforts to promote privacy,[435] Google began monetizing its users' search queries, laying the groundwork for a behavioral ad-based business model that would normalize surveillance as the price of using swaths of digital services.[436]

Recognizing the serious costs of this approach, the Biden-era Commission focused on vigorous law enforcement in lieu of misplacing confidence in industry self-regulation.[437]

---

431. Concurring Statement of Commissioner Andrew N. Ferguson Joined by Commissioner Melissa Holyoak 4, NGL Labs, LLC, FTC File No. 2223144 (July 9, 2024), https://perma.cc/WP32-HRQH.

432. *See* Cristiano Lima-Strong, *In a First, Federal Regulators Ban Messaging App From Hosting Minors*, WASH. POST (July 9, 2024, 4:06 PM EDT), https://perma.cc/8K8Z-7Q27 (nothing that the action is "emblematic of the bipartisan concern over children's online safety in Washington.").

433. *See supra* Part I.A.

434. *See, e.g.*, *supra* notes 118-22 and accompanying text (discussing the failure of Muris's approach toward reducing unwanted calls).

435. Timothy J. Muris, Chairman, FTC, Protecting Consumers' Privacy: 2002 and Beyond, Remarks at The Privacy 2001 Conference (Oct. 4, 2001).

436. Jennifer 8. Lee, *Postcards from Planet Google*, N.Y. TIMES (Nov. 28, 2002), https://perma.cc/5WKU-5FRF.

437. *Testimony of Chair Lina M. Khan Before the House Appropriations Subcomm. on Fin. Servs. & Gen. Gov't*, 117TH CONG., at 15 (2022) (statement of Lina M. Khan, Chair, FTC) ("The Commission is taking a comprehensive approach to curbing and deterring unlawful data practices, including conduct that harms user privacy or data security."); *see also* FTC, The National Advertising Division Annual Conference: A Progress Report on

footnote continued on next page

A key dimension of effective law enforcement is deterrence. Two factors that can increase deterrence are monetary relief and individual liability.[438] In the context of online privacy and security, though, the FTC has historically struggled to secure either form of relief. Among the 101 privacy cases the agency brought between 2008 and 2018, fewer than a quarter included any monetary relief.[439] Holding individuals personally accountable is also rare.[440]

Despite these challenges, the Commission in recent years made a concerted effort to ramp up accountability for data abuses and promote deterrence.

1. Relief for monetary harms

In addition to handicapping the FTC from vigorously addressing illegal practices online, Muris and Beales also took steps to limit what remedies the FTC could obtain to address law violations. During the Reagan Administration, the FTC adopted the view that section 13(b) of the FTC Act authorized it to seek redress and disgorgement from lawbreakers.[441] This view of section 13(b) led agency leadership to rely heavily on this provision for securing monetary relief and neglect other statutory authorities that also unlocked monetary relief, such as section 19, section 5(m)(1)(B), and section 18.

In 2021, AMG Capital took the FTC to the Supreme Court to challenge its use of section 13(b). Although Muris and Beales had previously adopted the Reagan-era view that section 13(b) authorized monetary equitable relief, they

---

Key Priorities, and a Warning on AI Self-Regulation 8-9 (2023), https://perma.cc/Z7RK-QTHA (remarks of Samuel Levine, Dir., Bureau of Consumer Prot.).

438. *See* Rohit Chopra, Comm'r, FTC, Prepared Remarks at Truth in Advertising Event on the FTC's Remedial Authority (Jan. 11, 2021), https://perma.cc/M29T-XMXJ (stressing importance of monetary relief); Rebecca Kelly Slaughter, Comm'r, FTC, Statement Regarding section 13(b) of the FTC Act (Apr. 28, 2022), https://perma.cc/RW3S-GDKZ (same); Rohit Chopra, Director, Consumer Fin. Prot. Bureau, 2022 Distinguished Lecture on Regulation at the University of Pennsylvania: Reining in Repeat Offenders (Mar. 28, 2022), https://perma.cc/2WXX-WJVL (stressing importance of individual liability); Rebecca Kelly Slaughter, Comm'r, FTC, Statement Regarding United States v. Williams-Sonoma, Inc. (Apr. 26, 2024), https://perma.cc/NBR4-ATPK (same).

439. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY, app. 2 at 44-51 (2019).

440. Natasha G. Kohne, Erica E. Holland, Michael Stanley & Joseph Hold, *FTC Takes Rare Step in Bringing an Enforcement Action Against Drizly and Its CEO*, AKIN DATA DRIVE (Jan. 10, 2023), https://perma.cc/GKT7-XMZQ (noting the rarity of the FTC naming an individual respondent).

441. *See* J. Howard Beales III & Timothy J. Muris, *Striking the Proper Balance: Redress Under Section 13(b) of the FTC Act*, 79 ANTITRUST L.J. 1, 4-5 (2013) (arguing that the Commission should use section 13(b) only in fraud cases).

later argued that the FTC should limit its use of section 13(b) to fraud cases[442]—an entirely atextual reading of the FTC Act. In *AMG*, a unanimous Supreme Court rejected this view of section 13(b), holding that the provision did not provide *any* authority to seek restitution, compensation for money lost, or disgorgement, recovery of unjust gains.[443] Overnight, the FTC lost what had become its mainstay tool for securing redress and disgorgement in federal court.

AMG also significantly impacted the agency's privacy program. While other statutory provisions create alternative pathways for the FTC to obtain redress for money lost, many privacy cases involve unjust profits rather than direct monetary loss, and *AMG* cut off the FTC's only route to securing disgorgement in federal court.[444] Without the prospect of needing to pay out unjust gains, corporate actors could illegally violate people's privacy with impunity.[445]

While commentators predicted that *AMG* would severely handicap the FTC's ability to secure monetary relief,[446] the agency activated other statutory tools to ensure lawbreakers would still be on the hook for monetary harm suffered by consumers.[447]

A key early example was in *CafePress*,[448] where the agency successfully recovered redress for small businesses whose data was compromised by the

442. J. Howard Beales III, Benjamin M. Mundel & Timothy J. Muris, *Section 13(b) of the FTC Act at the Supreme Court: The Middle Ground*, ANTITRUST SOURCE, Dec. 2020, at 1, 1-2.

443. AMG Cap. Mgmt. LLC v. FTC, 141 S. Ct. 1341, 1344 (2021) (limiting the ability of the agency to obtain monetary remedies such as disgorgement or restitution).

444. *See, e.g.*, In re Facebook, Inc., FTC File No. 1823109, at 16 (July 24, 2019) (Chopra, Comm'r, dissenting), https://perma.cc/C7FW-FAL5 (arguing that privacy violations justify disgorgement of ill-gotten gains).

445. See *id.*; FTC, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 5 (Sept. 13, 2021), https://perma.cc/H8SD-3Z8J (describing the impact of *AMG* on the agency's privacy program).

446. *See, e.g.*, *AMG v. FTC: US Supreme Court Severely Limits FTC's Ability to Seek Monetary Relief*, COOLEY (Apr. 29, 2021), https://perma.cc/J24A-ZVFJ ("The Supreme Court's decision, which reversed the Ninth Circuit's ruling, strips the FTC of one of its most powerful enforcement tools and severely limits the FTC's ability to seek monetary relief.").

447. *Testimony of Chair Lina M. Khan Before the H. Comm. on Appropriations Subcomm. on Fin. Servs. & Gen. Gov't*, 118TH CONG., at 3 (2024) (statement of Lina M. Khan, Chair, FTC) (noting "remarkable" success in returning money to consumers).

448. *See* Dempsey, *supra* note 252 ("CafePress may be the first settlement to mandate data minimization at the collection phase and may signal growing Commission support for bringing data minimization into the center of FTC enforcement."); *see also* Decision and Order, Residual Pumpkin Entity, LLC, FTC File No. C-4768 (June 23, 2022), https://perma.cc/D33D-LUZU.

companies' unlawful data security practices.[449] The approach generated interest, with the defense bar describing this relief as novel and indicative that *AMG* would not deter the FTC from using other authorities. [450] The agency would soon follow up by using section 19 to seek redress in privacy cases like *BetterHelp,* where the FTC secured $7.8 million for consumers in what was described as "the agency's first apparent foray into using its Section 19 authority post-*AMG*,"[451] and later *Avast*, where the Commission secured $16.5 million in redress.[452]

In addition to seeking redress for consumers, the Commission increasingly began seeking civil penalties for privacy violations. Civil penalties are distinct from restitution or disgorgement. Rather than aiming to make consumers whole, civil penalties are intended to deter lawbreaking and vindicate agency interests.[453] Civil penalties are available to the Commission only in select instances—namely, when conduct violates a preexisting order, an agency rule, or a statute that specifically provides for civil penalties.[454] But since 2021, the Commission has prioritized obtaining civil penalties where available.[455]

449. Press Release, FTC, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar. 15, 2022), https://perma.cc/58JM-ZANB.

450. *See, e.g.*, K. Dailey Wilson, *Breaking Down the FTC's Hard-Press Against CafePress: Five Takeaways from the Recent FTC Action*, HUDSON COOK, LLP (Apr. 29, 2022), https://perma.cc/FNA2-PCA4; *cf.* Andrew Serwin, Deborah Meshulam & Leila Javanshir, *CafePress to Pay $500,000 for FTC Violations*, DLA PIPER US (Mar. 22, 2022), https://perma.cc/74S6-QEKK (highlighting the novelty of including redress in a data security action).

451. Tracy Shapiro, Haley N. Bavasi, Eddie Holman, Hale Melnick, Yeji Kim & Stacy Okoro, *FTC Announces Settlement with BetterHelp for Disclosing Consumers' Health Information to Third-Party Advertisers,* WILSON SONSINI GOODRICH & ROSATI (Mar. 8, 2023), https://perma.cc/96W3-QB6X.

452. Press Release, FTC, FTC Finalizes Order with Avast Banning It from Selling or Licensing Web Browsing Data for Advertising and Requiring It to Pay $16.5 Million (June 27, 2024), https://perma.cc/X8BC-7RAB.

453. Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC's Penalty Offense Authority*, 170 U. PENN. L. REV. 71, 81-82; *see* 15 U.S.C. § 45(m).

454. Justin Brookman & Maureen Mahoney, *Consumer Reports Praises House for Advancing Bill to Provide New Funds, Authority for FTC Privacy Protections; Urges Senate to Take Action*, CONSUMER REPORTS (Nov. 19, 2021), https://perma.cc/7DDF-S44D (noting that "when companies are caught deceiving or defrauding consumers, the FTC usually does not have the ability to obtain penalties from a court or in settling a case . . . .").

455. For recent actions where the Commission sought civil penalties for privacy violations, see, for example, Press Release, FTC, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests (May 31, 2023), https://perma.cc/L2LF-A5PA, and Press Release, FTC, FTC and CFPB Settlement to Require Trans Union to Pay $15 Million over Charges It Failed to Ensure Accuracy of Tenant Screening Reports (Oct. 12, 2023), https://perma.cc/98VM-BWDK.

One key area has been children's privacy. Given marketers' strong interest in reaching children, surveilling kids can be highly lucrative.[456] The agency's COPPA enforcement made clear that breaking the law would cost more than following it. In *Epic*, the FTC secured the largest COPPA penalty in the agency's history—$275 million, on top of $245 million in redress.[457] The Commission then secured eight-figure penalties against both Amazon and Microsoft for improper retention and collection of children's data.[458] In late 2024 the Commission worked with the Department of Justice to seek both monetary and injunctive relief against TikTok for serious violations of children's privacy and of a previous FTC order.[459]

Beyond children's privacy, the Commission also began seeking civil penalties for health privacy violations. These cases primarily involve violations of the Commission's Health Breach Notification Rule (HBNR), which requires businesses to notify consumers when unsecured personal information is breached.[460] While HBNR was finalized in 2009, the Commission did not bring an action under it until 2023, which resulted in a $1.5 million payment from GoodRx and a prohibition on continuing the infringing actions.[461] Defense-side law firms described the case as "breathing new life into [a] decade old regulation"[462] and a sign of federal regulators looking for "novel ways to protect consumers' sensitive health information through enforcement."[463] Shortly after, the Commission brought its second HBNR enforcement action against Premom, securing a civil penalty judgment against the firm for unlawfully disseminating sensitive fertility data.[464]

---

456. *Kids' Ad Revenue for Social Media*, CTR. FOR HEALTH DECISION SCI., HARVARD T.H. CHAN SCH. PUB. HEALTH (Feb. 28, 2024), https://perma.cc/E5S4-NPPY.

457. Epic Games Settlements Press Release, *supra* note 256.

458. Press Release, FTC, FTC Will Require Microsoft to Pay $20 Million over Charges It Illegally Collected Personal Information from Children Without Their Parents' Consent (June 5, 2023), https://perma.cc/G3V7-RQ48; Press Release, Dep't of Justice, Amazon Agrees to Injunctive Relief and $25 Million Civil Penalty for Alleged Violations of Children's Privacy Law Relating to Alexa (July 19, 2023), https://perma.cc/AR8L-DV3G.

459. Press Release, FTC, FTC Investigation Leads to Lawsuit Against TikTok and ByteDance for Flagrantly Violating Children's Privacy Law (Aug. 2, 2024), https://perma.cc/9WJF-EVBU.

460. Health Breach Notification Rule, 16 C.F.R. pt. 318 (2009).

461. GoodRx Enforcement Action Press Release, *supra* note 256.

462. Jordan T. Cohen, *FTC's Enforcement Action Against GoodRx Breathes New Life into Decade Old Regulation,* AKERMAN (Feb. 27, 2023) (capitalization altered), https://perma.cc/68UB-E7EF.

463. Deborah L. Gersh, Jennifer L. Romig, Christine Moundas & Winnie Uluocha, *FTC Enforces Health Breach Notification Rule Against GoodRx in First of Its Kind Enforcement Action*, ROPES & GRAY (Feb. 8, 2023), https://perma.cc/WNJ9-HU59.

464. Premom Proposed Order Press Release, *supra* note 256.

Nor was this relief secured solely through settlements. In 2024, the FTC conducted its first ever jury trial against a cash advance lender, Richmond Capital Group (RCG), for making false statements to obtain consumers' bank information.[465] Following the trial, the court imposed a $20 million judgment—including both redress and civil penalties—against the operation's ringleader.[466] Although *RCG* was not a privacy action per se, it helped open the door to securing monetary relief when consumers' data is obtained unlawfully.[467]

Across the board, the Commission—in spite of *AMG*—prioritized returning money to consumers and taxpayers whenever it had the tools to do so. Requiring lawbreaking firms to pay for lax data security and egregious privacy abuses helps internalize the costs of this misconduct and deters other firms from engaging in similar practices.[468]

2. Relief for nonmonetary harms

Just as the Commission has recognized that illegal practices online can cause injury that extends beyond monetary harm, the agency has crafted remedies that similarly account for this broader purview. Two forms of nonmonetary harms are particularly salient.

First, the Commission has recognized that firms can profit from unlawfully obtained data in a host of ways—including through training models and algorithms. Indeed, the explosion of large language models has spurred a race among firms to mass harvest users' data to train models, including in ways that may be illegal.[469] To ensure that firms are not profiting from illegally

465. Press Release, FTC, Court Enters $20.3 Million Judgment in FTC Case Against Merchant Cash Advance Operator Jonathan Braun for Deceiving Small Businesses and Unlawfully Seizing Assets (Feb. 14, 2024), https://perma.cc/7PPE-TNJF; FTC v. RCG Advances, LLC, 695 F. Supp. 3d 368, 379, 381 (S.D.N.Y. Sept. 27, 2023).

466. *See* FTC, *supra* note 465.

467. *See* Ioana Gorecki, *Federal Court Upholds FTC's Expanded Interpretation of Gramm-Leach-Bliley Act Pretexting*, 141 BANKING L.J. 78, 83 (2024) (noting that "[i]n its expanded and now court-vetted interpretation of [the Gramm-Leach-Bliley Act] pretexting, the FTC has gained an important avenue for monetary relief against first-time Section 5 violators"); Nikhil Singhvi, *The FTC May Be Expanding Its Monetary Relief Toolbox*, LAW360 (Aug. 10, 2023, 4:34 PM EDT), https://perma.cc/U6X8-BKXP.

468. *See* Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, 102 B.U. L. REV. 793, 820-21, 829 (2021) (describing the importance and difficulty of recovering monetary relief and achieving deterrence in privacy and data security actions).

469. Eli Tan, *When the Terms of Service Change to Make Way for A.I. Training*, N.Y. TIMES (June 26, 2024), https://perma.cc/2E9X-BNH2.

obtained data, the FTC orders firms to delete such data.[470] But this remedy leaves a key gap—if a firm trained its models on this data, it can still realize the benefit of its illegal collection even after the data is deleted.

To close this loophole, the Commission has deployed a new remedy—data product deletion—that requires firms destroy not only data they collected illegally but also any models trained on ill-gotten data.[471] Between 2021 and 2024, the Commission brought nearly a dozen actions requiring firms to destroy algorithms trained on illegally obtained data.[472]

Second, the Commission has recognized that dark patterns and other manipulative tactics online can waste people's time as well as their money. For example, in 2022, the Commission alleged that CreditKarma deceived consumers by advertising they were "pre-approved" for credit, and recovered $2.5 million to compensate them for wasted time.[473] Since then, the agency

470. Press Release, FTC, FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data (Sept. 1, 2021), https://perma.cc/YNR4-P4YM.

471. *See* Tonya Riley, *The FTC's Biggest AI Enforcement Tool? Forcing Companies to Delete Their Algorithms*, CYBERSCOOP (July 5, 2023), https://perma.cc/RU6H-SMFC.

472. *See, e.g.*, Stipulated Order for Permanent Injunction & Other Relief, attach. A at 6, FTC v. Rite Aid Corp., No. 23-cv-5023 (E.D. Pa. Dec. 19, 2023), https://perma.cc/8EEN-JMJN; Proposed Stipulated Order for Injunction & Monetary Relief at 7, FTC v. Ring LLC, No. 23-cv-1549 (D.D.C. May 31, 2023), https://perma.cc/Z35T-FX48; Stipulated Order for Injunction & Civil Penalty Judgment at 13, United States v. Edmodo, LLC, No. 23-cv-2495 (N.D. Cal. June 27, 2023), https://perma.cc/26ZU-V22L; *In re* X-Mode Social, Inc., FTC Matter No. 2123038, at 10 (Jan. 9, 2024) (decision and order), https://perma.cc/29Q8-S8QJ; InMarket Media, LLC, FTC Docket No. C-4803, at 8 (Apr. 29, 2024) (decision and order), https://perma.cc/7R98-9H8T; Stipulated Order for Permanent Injunction, Civil Penalty Judgment, & Other Relief at 8, United States v. Kurbo Inc., No. 22-cv-00946 (N.D. Cal. Mar. 3, 2022), https://perma.cc/6B5P-ZQNQ; Decision at 6, *In re* Avast Ltd., FTC Docket No. C-4805 (June 26, 2024), https://perma.cc/F5TL-HE6H; Proposed Stipulated Order for Permanent Injunction, Monetary Judgment for Civil Penalty, & Other Relief at 14, FTC v. CRI Genetics, LLC, No. 23-cv-9824 (C.D. Cal. Nov. 20, 2023), https://perma.cc/PFS2-AB38; *In re* Everalbum, Inc., FTC Docket No. 1923172, at 4 (May 7, 2021) (decision and order), https://perma.cc/C9MP-THRY; Stipulated Order for Permanent Injunction, Civil Penalty Judgment, & Other Relief at 12-13, U.S. v. Monument, Inc., No. 24-cv-01034-BAH (D.D.C. June 7, 2024), https://perma.cc/8QJD-JZZ7. The FTC's success in obtaining this remedy across so many cases has generated widespread interest. *See, e.g.*, Riley, *supra* note 471. Some have argued that the agency may be overreaching. *See* Jeremy Straub, *Algorithmic Disgorgement is Bad for Science and Society,* LAWFARE BLOG (June 12, 2023, 3:00 AM), https://perma.cc/DT7E-WMRZ; *see also* Joshua A. Goland, *Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as the FTC's Newest Enforcement Tool for Bad Data*, RICH. J.L. & TECH., 2023, at 43-47 (summarizing arguments against disgorgement).

473. Press Release, FTC, FTC Takes Action to Stop Credit Karma from Tricking Consumers with Allegedly False "Pre-Approved" Credit Offers (Sept. 1, 2022), https://perma.cc/5XJG-BZV9; *see also* Alexandra Megaris & Leonard Gordon, *FTC Action Against Credit Karma Underscores That Conversion Cannot Trump Compliance*, VENABLE (Sept. 6, 2022), https://perma.cc/W4DL-6Z7J (describing the agency's lost

footnote continued on next page

expanded this approach and recovered nearly $80 million for small businesses,[474] older Americans,[475] and eyecare customers[476] who were alleged to have lost time, rather than money, as a result of unlawful practices. Most recently, in late 2024, the Commission secured $7 million from H&R Block to compensate taxpayers whose time was wasted through deceptive advertising and poor customer service.[477] This action—which also required H&R Block to overhaul its customer service practices—earned unanimous support at the Commission, signaling durable support for holding firms accountable for wasting consumers' time.[478]

3. Individual accountability

Enforcers widely recognize that individual accountability is key to deterring lawbreaking.[479] For example, in 2015 Deputy Attorney General Yates circulated a memo explaining that bringing charges against individuals, when appropriate, can be a key mechanism for achieving deterrence.[480] Upon joining the FTC, Commissioner Rohit Chopra expanded on the need for individual accountability in cases of serious wrongdoing by serial offenders.[481] Both statements underscore the importance of ensuring that business leaders who flagrantly violate laws are held to account.

At their most effective, enforcers will apply an evenhanded approach to charging decisions—not hesitating to hold accountable senior executives and large corporations, just as they would smalltime fraudsters and scammers.[482] In

time recovery as "concerning" and warning firms that the agency may seek this remedy elsewhere to combat dark patterns).

474. Press Release, FTC, FTC Actions Against Companies Making Deceptive Pandemic Loan Promises Lead to Record $59 Million in Damages (Mar. 18, 2024), https://perma.cc/Y2VJ-9ZGS.

475. Press Release, FTC, FTC Takes Action Against Publishers Clearing House for Misleading Consumers About Sweepstakes Entries (June 27, 2023), https://perma.cc/2XMP-XBJG.

476. Press Release, FTC, FTC Order Requires LasikPlus to Pay for Its Bait-and-Switch Eye Surgery Ads (Jan. 19, 2023), https://perma.cc/M6UZ-YS6U.

477. *See* Press Release, FTC, FTC Action Stops H&R Block's Unfair Downgrading Practices and Deceptive Promises of 'Free' Filing (Nov. 12, 2024), https://perma.cc/UE7Y-RHZN.

478. *See id.*

479. *See, e.g.*, JOHN COFFEE, CORPORATE CRIME AND PUNISHMENT: THE CRISIS OF UNDERENFORCEMENT (2020).

480. Deputy Attorney General Sally Q. Yates, Memorandum on Individual Accountability for Corporate Wrongdoing at 1, 4 (Sept. 9, 2015).

481. FTC Commissioner Rohit Chopra, Memorandum on Repeat Offenders at 4 (May 14, 2018).

482. Rohit Chopra, Distinguished Lecture on Regulation at the University of Pennsylvania Carey Law School: Reining in Repeat Offenders (Mar. 28, 2022), https://perma.cc

footnote continued on next page

other instances, however, firms are allowed to pay large fines, while their executives who called the shots escape accountability.[483]

For FTC leadership these past few years, the country's recent experience with the financial crisis represented a clear failure by enforcers to hold executives accountable. While most large banks paid out fines to settle charges that they violated the law, few if any individual executives were prosecuted either civilly or criminally.[484] They thus reaped the rewards of years of lawbreaking, without facing meaningful consequences.

Accordingly, a key priority for agency leadership in the Biden Administration was holding individual executives accountable when they were found to have violated the law.[485] In the privacy context, this first occurred in September 2021, when the FTC took action against a stalkerware app called SpyFone, which allegedly sold products and services that surreptitiously collected data on people's movements, phone use, and online activities—yet failed to take reasonable measures to keep that data secure from hackers.[486] The FTC banned SpyFone and its CEO from re-entering the surveillance business, in addition to requiring the company to delete the illegally harvested information.[487]

The following January, the FTC took action against ITMedia and multiple executives for manipulating consumers into turning over sensitive financial information, and then selling that data to marketers.[488] The order required the defendants to pay a monetary judgment, halt their deceptive practices, and significantly restrict their data sales.[489] Since individuals were named, they

/XC3L-TAVT ("When small businesses get in trouble, regulators and enforcers are quick to target the top brass. It is inappropriate and unfair to not have the same approach to big financial institutions when the facts and circumstances of the role of individuals is the same.").

483. *See id.* (citing actions against Facebook, Wells Fargo, Citigroup, and others).

484. Rita Oliveira, Ruth Walters & Raihan Zamil, *How to Hold Bank Executives Accountable for Misconduct*, CLS BLUE SKY BLOG (June 13, 2023), https://perma.cc/A4KD-Y7FF.

485. *See, e.g.*, Lina M. Khan, Chairperson, FTC, Prepared Statement on Issuance of the Commission Statement Regarding the Criminal Referral and Partnership Process (Nov. 18, 2021), https://perma.cc/36LR-2NWK ("Pursuing individual liability in instances where top executives are responsible for or direct unlawful conduct is critical.").

486. Complaint ¶¶ 4, 13-17, Support King, LLC, FTC File No. 192 3003 (Dec. 20, 2021) https://perma.cc/5XP3-ELD7; FTC, *supra* note 470.

487. Lauren Feiner, *FTC Bars Alleged 'Stalkerware' Company and its CEO from the Surveillance Business*, CNBC (Sept. 1, 2021), https://perma.cc/5YVW-EKAP.

488. Press Release, FTC, Lead Generator that Deceptively Solicited Loan Applications from Millions of Consumers and Indiscriminately Shared Sensitive Info Agrees to Pay $1.5 Million FTC Penalty (Jan. 7, 2022), https://perma.cc/YX8L-JNZK.

489. Stipulated Order for Permanent Injunction and Judgment at 6-7, 12, FTC v. IT Media Solutions, No. 22-cv-00073 (C.D. Cal. Jan. 10, 2022), https://perma.cc/NE92-Y3U5.

will be bound by this order even if they form a new company.[490] This case led to warnings by the defense bar that the FTC was ramping up its focus on individual liability.[491]

Prioritizing individual accountability expanded beyond privacy enforcement actions. In 2022, the Commission brought a major data security action against alcohol delivery firm Drizly for a security breach that impacted millions of customers.[492] As part of this action, the CEO was held personally responsible, with the order crafted so that its obligations will follow the executive to future employment.[493] That a CEO of a major firm was named personally in a data security action was widely noticed,[494] and the FTC was not subtle about its aims, with the Bureau Director issuing a statement that "CEOs who take shortcuts on security should take note."[495]

The FTC during this period would also hold individuals accountable for violating children's privacy. In the agency's 2024 action against NGL, two of the company's founders were charged personally with violating kids' privacy, putting teens at risk, and making baseless claims around AI safety.[496] As with monetary relief, the FTC was prepared to take individuals to court when necessary, including a major lawsuit against the CEO of Cerebral, a telehealth firm alleged to have mishandled sensitive consumer data.[497]

By 2024, the market was well on notice that individual executives—even at large tech companies—could be held personally accountable for serious data

490. *Id.*

491. *See, e.g.*, Daniel Kaufman, *I'm a Lawyer . . . What Do You Mean I'm Being Named in an FTC Complaint? The FTC Act and Individual Liability*, BAKER HOSTETLER BLOG (Jan. 13, 2022), https://perma.cc/5B2H-2QFA; William Roppolo, Ashley Eickhof & Annasofia Roig, *Beware FTC's Expanded Focus on Private Equity, Individuals*, BAKER MCKENZIE (Nov. 21, 2022), https://perma.cc/PM97-N2PX; Kristin Bryan, Christina Lamoureaux & Kyle Dull, *Consumer Loan Data Seller Receives $1.5 Million FTC Penalty, with Accompanying Executive Liability*, PRIVACY WORLD (Jan. 10, 2022), https://perma.cc/JB2R-GG3D.

492. Press Release, FTC, 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://perma.cc/27A2-4GPJ.

493. *See* Decision & Order at 10, Drizly, LLC, FTC File No. 2023185 (Jan. 9, 2023), https://perma.cc/F94L-BBX7.

494. *E.g.*, Cat Zakrzewski, *FTC Brings Action Against CEO of Alcohol Delivery Company over Data Breach*, WASH. POST (Oct. 24, 2022), https://perma.cc/H4CS-PPVX; Alisa Chestler, Greta Messer & Baker Donelson, *Sobering Reality: Drizly Order Indicates Officers May Face Personal Liability for Data Breaches*, CORP. COMPLIANCE INSIGHTS (Feb. 1, 2023), https://perma.cc/B4BZ-N723; Lauren Feiner, *FTC Seeks to Hold Drizly CEO Accountable for Alleged Security Failures, Even if He Moves to Another Company*, CNBC (Oct. 24, 2022, 3:53 PM EDT), https://perma.cc/8UXV-YS4S.

495. Press Release, *supra* note 492.

496. Press Release, *supra* note 424.

497. Cerebral Proposed Order Press Release, *supra* note 304.

abuses. That year, following *Cerebral*, a major privacy firm in D.C. warned clients that "[c]ompany executives should take note that the FTC may seek to hold them accountable for maintaining a privacy and security program reasonable for the size, resources, and information activities of their companies."[498] A blog post by another firm described the Drizly action's finding of individual executive liability as one that could be a "new norm" for consent orders.[499] Yet another firm warned that the agency's "new focus on management's role in privacy and information security is unprecedented."[500]

Although the defense bar has sounded the alarm, it is too early to tell whether the FTC's stepped-up efforts to hold individuals accountable will meaningfully disincentivize illegal data abuses and other lawbreaking online. What is clear, however, is that the era of relying on self-regulation or forswearing individual accountability has ended. In time, this should meaningfully increase deterrence against data abuses.

III. Institutional Reform and Further Positioning the Agency to Respond to Emerging Challenges

The FTC's revamped approach to tackling consumer protection violations in the digital age has focused on several key areas. This Part focuses on the institutional upgrades the FTC has made as part of its work to implement this paradigm shift. First, this Part highlights the establishment of the Federal Trade Commission's Office of Technology in 2023, which built upon the agency's tradition of adapting to keep pace with new market realities. It lays out the mandate, structure, and staff of this new office, explaining how these factors have expanded the agency's institutional capacities and positioned it to be an effective enforcer in the digital age. This Part also highlights a body of work that the Office—in collaboration with attorneys, economists, investigators, analysts, and other staff—has produced in the past few years, showcasing a nimbleness that the agency's new capacity affords. Finally, this Part lays out the path ahead for cementing these institutional advances and upgrades.

498. Tracy Shapiro, Hale Melnick & Stacy Okoro, *FTC Announces Proposed Settlement Agreements with Two Digital Health Companies for Disclosing Consumers' Health Information to Third-Party Advertisers, Among Other Violations*, WILSON SONSINI (May 1, 2024), https://perma.cc/T9P6-T8DJ.

499. Kohne et al., *supra* note 440.

500. Alisa L. Chestler, *Privacy in 2023: Management and Officer Liability for Privacy and Data Security Programs*, BAKER DONELSON (Jan. 24, 2023), https://perma.cc/9JWZ-TJGX.

A. Establishing Internal Technological Capacity

Increasing the sophistication and rigor of the FTC's work in digital markets has required creating the institutional capacity needed to support these efforts. This Subpart details how investing in in-house tech expertise has equipped the agency to grasp and address emerging technologies, such as AI.

A Brief History.—Since its creation in 1914, the Federal Trade Commission has regularly expanded its in-house expertise to adapt to rapid changes brought about by new technologies.[501] For example, in 1929 the agency established the "Special Board of Investigation," consisting of "three Commission attorneys designated to represent the Commission at preliminary hearings and specialize" in cases relating to "[f]alse and misleading advertising matter," including by studying massive volumes of newspapers, magazines, and eventually, radio transcript data.[502]

The agency has upgraded its skills to better grasp and address technological developments and new mechanisms for lawbreaking. In 2006, the FTC established the Division of Privacy and Identity Protection, a new group comprised of over thirty staff with expertise in privacy, data security, and identity theft.[503] And amid the growing adoption of mobile smartphone devices,[504] the FTC in 2012 established a forensic mobile lab to enable staff to conduct research and investigations to detect fraud, scams, and other illegal practices pursued through mobile phones.[505]

In terms of staffing, the agency also hired in-house expertise to support its enforcement work. In 2011, the Commission appointed its first Chief Technology Officer.[506] In 2015, the Commission's Chief Technologist pushed to hire more technologists in a single office, which led to the creation of the Office of Technology Research and Investigations, housed within the Bureau of Consumer Protection.[507] In total, there have been eight Chief Technologists,

501. Stephanie T. Nguyen, *A Century of Technological Evolution at the Federal Trade Commission,* FTC: TECH. BLOG (Feb. 17, 2023), https://perma.cc/3FL7-XVSL.

502. FTC, ANNUAL REPORT OF THE FEDERAL TRADE COMMISSION FOR THE FISCAL YEAR ENDED JUNE 30 1935, at 101-04 (1935), https://perma.cc/YSD8-W8AC.

503. FTC, THE FTC IN 2006: COMMITTED TO CONSUMERS AND COMPETITION 24 (2006), https://perma.cc/2GA6-V62J.

504. Dan Butcher, *Smartphone Sales Grew 72pc in 2010: Gartner*, RETAILDIVE, https://perma.cc/X3PM-7SKX (archived Apr. 19, 2025).

505. Edith Ramirez, Chairperson, FTC, Opening Remarks at the Mobile Security Forum (June 4, 2013), https://perma.cc/CCF4-J2EQ.

506. *See FTC Chief Technologists*, FTC, https://perma.cc/QY9U-FA5E (archived Apr. 19, 2025).

507. This office also announced several new positions including "a two-year Technology Policy Fellowship program, a research coordinator, and a technical internship
footnote continued on next page

each with various priorities and approaches to strengthening and supporting the agency.[508]

Establishing the Office of Technology.—In February 2023, the Commission voted unanimously to establish the Office of Technology (OT) to expand the agency's in-house technical expertise.[509] The Office was created with three core mandates: (1) to strengthen and support law enforcement investigations and actions, (2) to advise and engage with staff and the Commission on policy and research initiatives, and (3) to engage the public and relevant experts to understand trends and advance the Commission's work.[510] Since launching, OT has grown the FTC's ranks of technologists, formalized the efficient deployment of these expert resources across the agency, and promoted collaboration and coordination among technologists working across the agency.

The Office of Technology's team structure was informed by similar efforts pursued by other enforcement and policy bodies both internationally and domestically. In the 2010s, the rise of "digital service technologist" teams across the federal government created an initial template for how to bring technologists into public service. [511] Competition and consumer law enforcement agencies in other jurisdictions have also intentionally dedicated or increased tech capacity within their agencies, including the United Kingdom,[512] Australia,[513] Canada,[514] France,[515] Japan,[516] Korea,[517]

program." *FTC Seeks Technologists for New Research, Investigations Office*, FTC (Mar. 23, 2015), https://perma.cc/GG5A-SQM8.

508. *See* FTC, *supra* note 506.

509. Press Release, FTC Launches New Office of Technology to Bolster Agency's Work, FTC (Feb. 17, 2023), https://perma.cc/K8M5-SDJ6.

510. *Id.*

511. FTC, BUILDING TECH CAPACITY IN LAW ENFORCEMENT AGENCIES: ON STRENGTHENING FOUNDATIONS AND PATHWAYS FOR PUBLIC INTEREST TECHNOLOGISTS IN GOVERNMENT 6 (2024), https://perma.cc/855J-KGXP.

512. *See* Stefan Hunt, *The CMA DaTA Unit—We're Growing!*, COMPETITION & MKTS. AUTH. BLOG (May 28, 2019), https://perma.cc/3Q7A-LEY6; COMPETITION AND MARKETS AUTHORITY, *Digital Markets Unit and the Digital Markets Competition Regime*, GOV.UK, https://perma.cc/H64K-893G (last updated Dec. 19, 2024).

513. *See Organisation Structure*, AUSTRALIAN COMPETITION & CONSUMER COMM'N, https://perma.cc/ACM4-LYV4 (archived Apr. 20, 2025).

514. *Competition Bureau Organizational Structure*, GOV'T OF CAN., https://perma.cc/ZBK6-W2CH (archived Apr. 20, 2025).

515. *See Organisation Chart*, AUTORITÉ DE LA CONCURRENCE, https://perma.cc/87HY-VQDA (archived Apr. 19, 2025).

516. *See Organization Chart*, JAPAN FAIR TRADE COMM'N (Apr. 2025), https://perma.cc/2B9C-EC7M.

517. *See About KFTC: Organization*, FAIR TRADE COMM'N, https://perma.cc/86WS-XXQJ (archived Apr. 20, 2025).

Germany,[518] the Netherlands,[519] Singapore,[520] Mexico,[521] India,[522] and the European Commission.[523] In the United States, a number of federal agencies have also been building out their technical capacity to ensure they can regulate present and emerging technologies, including the Consumer Financial Protection Bureau, the Department of Justice, and the Federal Communications Commission.[524]

Staffing, Structure, and Process.—OT prioritized onboarding technologists with deep expertise across a range of specialized fields.[525] This included experts across security and software engineering, data science, artificial intelligence, human-computer interaction design, and social science research.[526] These individuals brought deep knowledge and specialization within particular fields, and their collective skillsets have met the diverse needs of teams across divisions.[527]

Creating a centralized hub for technologists at the FTC has allowed OT to prioritize and triage the significant workload demands of the entire agency.[528] By working closely with the Bureaus of Consumer Protection and

518. *Tasks & Organisational Structure*, BUNDESKARTELLAMT, https://perma.cc/CSJ4-W8A5 (archived Apr. 20, 2025).

519. *See Organizational Structure*, AUTH. FOR CONSUMERS & MKTS., https://perma.cc/9G5T-D3E4 (archived Apr. 20, 2025).

520. *CCCS Divisions*, COMPETITION & CONSUMER COMM'N, https://perma.cc/5HJC-MD3A (last updated Apr. 3, 2025).

521. *See Directorio*, COMISIÓN FEDERAL DE COMPETENCIA ECONÓMICA, https://perma.cc/RQ58-8YBC (archived Apr. 20, 2025).

522. Press Release, Competition Comm'n of India, CCI Organises 8th Edition of National Conference on Economics of Competition Law: Regulators Must Not Hesitate to Intervene to Keep Markets Free From Entry Barriers, Says CEA Dr. Nageswaran (Mar. 3, 2023), https://perma.cc/8P4N-V9KT; COMPETITION COMM'N INDIA, FAIR PLAY 6-7 (2023), https://perma.cc/FT2A-BL8T.

523. *See Directorate-General for Competition*, EUR. COMM'N, https://perma.cc/875P-8952 (archived Apr. 20, 2025).

524. *Government Agencies Act to Elevate and Build Tech and Digital Capacity*, FTC: TECH. BLOG (Mar. 26, 2024), https://perma.cc/F8VQ-Z42W.

525. FTC, BUILDING TECH CAPACITY IN LAW ENFORCEMENT AGENCIES: ON STRENGTHENING FOUNDATIONS AND PATHWAYS FOR PUBLIC INTEREST TECHNOLOGISTS IN GOVERNMENT 14 (2024), https://perma.cc/XD39-U54K.

526. *Id.* at 14, 16-17.

527. Stephanie T. Nguyen, Chief Technology Officer, FTC, Prepared Remarks at the Department of Trade and Industry—Manila, Philippines: US-Philippines Bilateral Workshop on Consumer Protection in the Tech Sector (Aug. 7, 2023), https://perma.cc/L9U3-RVH9.

528. FTC, Remarks from the Office of Technology Chief Technologist, Stephanie T. Nguyen at a Convening for MIT's Internet Policy Research Initiative at the Computer Science and Artificial Intelligence Lab: Three Sharp Thorns: On Tech Innovation and Regulation (May 17, 2023), https://perma.cc/5LCN-ZUJU.

Competition, OT has embedded technologists across the agency's investigations and cases.[529] This centralized structure also allows OT staff to join a community of other technologists who are learning how to integrate with the rest of the agency, enabling regular collaboration that strengthens their agility and fluency in navigating the agency's procedures and bureaucracy.

The structure of OT has let staff identify and scale best practices and promote stronger interdisciplinary collaboration. By working on both consumer protection and competition issues, technologists have greater visibility into market trends and overarching business strategies, mitigating a siloed approach.[530] For example, the current team has engaged in several cross-agency horizon scanning research efforts by aggregating industry trends and practices and working in partnership with staff attorneys to better inform potential actions.[531]

B. Case Studies

OT has three core mandates: strengthening and supporting the agency's law enforcement investigations and actions, pursuing policy and research initiatives, and highlighting market trends and emerging technologies that implicate the FTC's work.[532] Below we offer examples of each.

1. Strengthening enforcement

A key goal for the Office of Technology was embedding within case teams to help detect lawbreaking and craft effective remedies, especially actions involving emerging technology. The agency's nimble response to AI demonstrates some key examples of this approach.

In December 2023, the FTC announced an action against Rite Aid, alleging that its reckless AI practices had violated Section 5 of the FTC Act.[533]

529. *Id.* at 6 ("Every technologist is working on critical casework and investigations across competition and consumer protection matters."). *See generally* Press Release, *supra* note 509 (discussing the creation of OT).

530. *Id.*

531. *See, e.g.*, *Tick, Tick, Tick. Office of Technology's Summit on AI*, FTC: TECH. BLOG (Jan. 18, 2024), https://perma.cc/RJ7K-F5LW (describing the FTC's Summit on AI); Nick Jones, *Cloud Computing RFI: What We Heard and Learned*, FTC: TECH. BLOG (Nov. 16, 2023), https://perma.cc/5XV5-E7ZG (summarizing insights the agency learned through a Request for Information and a public panel on cloud computing); *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FTC: TECH. BLOG (Mar. 16, 2023), https://perma.cc/5MUP-FAMU.

532. Press Release, *supra* note 509.

533. *See* Rite Aid Proposed Order Press Release, *supra* note 256; Complaint ¶¶ 35-36, FTC v. Rite Aid Corp., No. 23-cv-5023 (E.D. Pa. Dec. 19, 2023), 2023 WL 8869509, ECF No. 1.

Specifically, the FTC alleged that Rite Aid had deployed facial recognition technology surveillance systems in various pharmacy locations and failed to take reasonable steps to mitigate risks to consumers.[534] For example, the complaint noted that Rite Aid's systems falsely identified innocent shoppers as shoplifters, including—at one point—an eleven-year-old girl.[535]

Working together, the agency's attorneys and technologists crafted a first-of-its-kind order to protect people from Rite Aid's reckless use of this technology.[536] Specifically, the proposed order banned Rite Aid from using facial recognition in any retail store, pharmacy or online platform for five years; required strict monitoring of automated decision-making systems for inaccuracy; and required the deletion of data products trained on biometric data collected unlawfully and the deletion of biometric information along with retention limits going forward.[537] Technologists' input in this matter helped establish a rigorous set of standards that can serve as a model.[538]

2. Advising on policy and research initiatives

Another part of the Office of Technology's mandate is advising the Commission on policy and research initiatives. This includes pursuing work outside of law enforcement, such as studies pursuant to section 6(b) of the FTC Act, reports, requests for information, research initiatives, and policy statements.[539] Harnessing technologists' expertise to these in-house

534. Complaint ¶¶ 3-5, FTC v. Rite Aid Corp., No. 23-cv-5023 (E.D. Pa. Dec. 19, 2023), 2023 WL 8869509, ECF No. 1.

535. *Id.* at 24.

536. *See* Kirk J. Nahra, Frank Gorman, Arianna Evers, Ali A. Jessani & Amy Olivero, *FTC Announces Groundbreaking Action Against Rite Aid for Unfair Use of AI*, WILMERHALE PRIV. & CYBERSECURITY L. BLOG (Jan. 11, 2024), https://perma.cc/A3D2-QERT (noting the case represented "the first time the FTC has taken enforcement action against a company for using AI in an allegedly biased and unfair manner").

537. Proposed Stipulated Order, 6-7, 15, FTC v. Rite Aid Corp., No. 23-cv-5023 (E.D. Pa. Dec. 19, 2023).

538. *Cf.* Nahra et al., *supra* note 536 (warning "this enforcement action highlights the importance of conducting risk assessments to understand potential consumer impacts, implementing bias mitigation strategies, overseeing vendors, employee training, and complying with company security standards at every stage of the procurement and deployment of an AI system").

539. In addition to the AI Partnerships and Investments inquiry detailed below, the Office of Technology has also published initial findings from its inquiry into how people's precise location or browser history may be used to target individual consumers with different prices for the same goods and services, as well as findings from a public inquiry into the business practices of cloud computing providers amidst rapid developments in artificial intelligence. *See* Press Release, FTC, FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices (Jan. 17, 2025), https://perma.cc/R36H-DHBK; Jones, *supra* note 531.

deliverables has equipped the agency to closely monitor technological developments and provide timely guidance and notice to market participants about what types of practices could risk running afoul of the laws that the FTC enforces.

Between 2010 and 2019, Alphabet, Amazon, Apple Facebook, and Microsoft collectively pursued over 600 acquisitions.[540] While none of these deals was challenged by the antitrust agencies at the time, enforcers later concluded that several of these firms' acquisition strategies constituted illegal monopolization.[541] A decade later, as generative AI tools took off, several of these same leading players announced investments in and partnerships with generative AI companies. To gain visibility into the nature and function of these deals, the FTC issued orders in January 2024 under its section 6(b) authority to Alphabet, Inc., Amazon.com, Inc., Anthropic PBC, Microsoft Corp., and OpenAI, Inc.[542] As firms raced to develop and gain a foothold in these emerging markets, the FTC's inquiry sought to examine "whether investments and partnerships pursued by dominant companies risk distorting innovation and undermining fair competition."[543]

Within a year, the FTC published a staff report on the AI partnerships and investments, offering key details about the structure of the partnerships between cloud service providers and AI developers, as well as identifying areas where these arrangements could risk undermining competition or innovation.[544] Because these partnerships "have continued to evolve and expand," FTC staff adopted a targeted approach that balanced "speed and

540. *See* Press Release, FTC, FTC Staff Presents Report on Nearly a Decade of Unreported Acquisitions by the Biggest Technology Companies (Sept. 15, 2021), https://perma.cc/N6C7-N2KC (analyzing acquisitions of Alphabet, Amazon, Apple, Facebook, and Microsoft between 2010 and 2019).

541. *See, e.g.*, Press Release, FTC, FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate (Aug. 19, 2021), https://perma.cc/43NL-2MS8; Press Release, U.S. Dep't of Just., Justice Department Sues Google for Monopolizing Digital Advertising Technologies (Jan. 24, 2023), https://perma.cc/4NJJ-3YVU.

542. Press Release, FTC, FTC Launches Inquiry into Generative AI Investments and Partnerships (Jan. 25, 2024), https://perma.cc/R2ZN-7LD8. The FTC's section 6(b) authority "enables it to conduct wide-ranging studies that do not have a specific law enforcement purpose." Memorandum from the FTC, *supra* note 225.

543. Press Release, *supra* note 542.

544. FTC, PARTNERSHIPS BETWEEN CLOUD SERVICE PROVIDERS AND AI DEVELOPERS: FTC STAFF REPORT ON AI PARTNERSHIPS & INVESTMENTS 6(B) STUDY 1-3 (2025), https://perma.cc/XHN8-3F7C [hereinafter AI PARTNERSHIPS AND INVESTMENTS REPORT]; *see also* Press Release, FTC, FTC Issues Staff Report on AI Partnerships & Investments Study (Jan. 17, 2025), https://perma.cc/868Q-S46K.

timeliness with a desire to understand the significance of these quickly moving partnerships."[545]

While section 6(b) studies can often take several years,[546] OT's agility allowed the agency to provide timely information to the public on a key issue with significant implications for competition and AI markets.[547]

3. Engaging the public and experts

The third mandate for the Office of Technology is to proactively engage with external stakeholders to identify emerging issues that implicate the Commission's consumer protection and competition mandates and use these findings to advance the Commission's work. This can be done through events and workshops,[548] roundtables,[549] research community engagement,[550] and public guidance such as technical blog posts.[551]

With the significant growth of generative AI, creative professionals have faced a series of challenges around the unauthorized use of their content.[552] To better understand the impact of generative AI on creative fields, the FTC in October 2023 held a roundtable discussion with artists, writers, graphic

545. *See* AI PARTNERSHIPS AND INVESTMENTS REPORT, *supra* note 544, at 5.

546. *See, e.g.*, Press Release, FTC, FTC Staff Report Finds Many Internet Service Providers Collect Troves of Personal Data, Users Have Few Options to Restrict Use (Oct. 21, 2021), https://perma.cc/87JR-BN37 (publicizing a staff report on privacy practices of internet service providers based on information orders first issued in March 2019); Press Release, FTC, FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens (Sept. 19, 2024), https://perma.cc/P2YA-4BRA (sharing a September 2024 staff report on data collection and use practices of major social media and video streaming services based on information orders first issued in December 2020).

547. *See* AI PARTNERSHIPS AND INVESTMENTS REPORT, *supra* note 544, at 5 ("Given the rapidly changing generative AI landscape, staff adopted a targeted approach to this study, carefully drafting the Special Orders to balance speed and timeliness with a desire to understand the significance of these quickly moving partnerships.").

548. *See, e.g.*, *Tick, Tick, Tick. Office of Technology's Summit on AI, supra* note 531.

549. *See, e.g.*, *Creative Economy and Generative AI*, FTC (Oct. 4, 2023), https://perma.cc/AQ3B-S86C.

550. *See, e.g.*, *P = NP? Not Exactly, but Here Are Some Research Questions from the Office of Technology*, FTC: TECH. BLOG (May 16, 2024), https://perma.cc/9J2N-M9U9.

551. The FTC's Office of Technology Blog allows in-house "technologists [to] dive into issues at the intersection of technology, consumer protection and competition," while informing both private sector client alerts and advocacy by civil society organizations. *See Office of Technology Blog*, FTC, https://perma.cc/J99F-RB7F (archived Apr. 20, 2025).

552. FTC, GENERATIVE ARTIFICIAL INTELLIGENCE AND THE CREATIVE ECONOMY STAFF REPORT: PERSPECTIVES AND TAKEAWAYS 6-7 (2023), https://perma.cc/54AG-XQ22.

designers, fashion models, and others in the creative arts.[553] Participants highlighted how their past work was being collected and used without their consent or awareness to train generative AI models.[554] They also expressed concerns that AI developers do not publicly disclose which works have been included in training data, stressing that AI-generated content trained on their work could unfairly divert business from the original creators.[555]

The agency outlined the key themes and concerns of the discussion in a Staff Report.[556] The learnings from this convening then informed the FTC's submission to the Copyright Office in a comment advocating for policymakers to safeguard fair competition in markets involving the creative arts.[557]

C. Future Outlook and the Work Ahead

It is much too early to declare victory on adequately safeguarding consumers from unfair and deceptive practices in the age of AI. But unlike its responses to previous market trends—such as subprime lending[558] or the explosion in student debt[559]—the FTC this time has been nimble in monitoring market developments and acting expeditiously to bring cases, publish research, and actively engage with and learn from market participants and the public.[560] Agency leadership made clear they were scrutinizing bottlenecks across the AI tech stack, examining how business models drive incentives, aligning liability with capability and control, and crafting effective remedies that establish bright-line rules on the development, use, and management of AI inputs.[561] By

553. *Creative Economy and Generative AI*, *supra* note 549.

554. *See generally* Transcript of Creative Economy and Generative AI Roundtable, FTC (Oct. 4, 2023), https://perma.cc/9EN8-EEMJ (participant commentary detailing how artists' past work was used without their consent to train AI models; one artist noted, for example, that "[their] work and the work of almost every artist [they] know was stolen without consent, credit, or compensation").

555. *See* FTC, *supra* note 552 (explaining the Commission's takeaways regarding AI after the discussion).

556. *Id.* at 3.

557. Press Release, FTC, In Comment Submitted to U.S. Copyright Office, FTC Raises AI-related Competition and Consumer Protection Issues, Stressing That It Will Use Its Authority to Protect Competition and Consumers in AI Markets (Nov. 7, 2023), https://perma.cc/RL27-4U79.

558. *See, e.g.*, *supra* note 203 and accompanying text.

559. FTC, *Statement of Commissioner Rohit Chopra: In the Matter of the University of Phoenix* 1-2 (2019), https://perma.cc/4HQP-KH86 (describing the FTC's work addressing for-profit college fraud); *see also* Rohit Chopra, *Student Debt Swells, Federal Loans Now Top a Trillion*, CFPB (July 17, 2013), https://perma.cc/L5VY-UH6U.

560. *See, e.g.*, *supra* notes 542-45 and notes 552-55.

561. FTC, Remarks of Chair Lina M. Khan: Tech Summit 3-4 (2024), https://perma.cc/L74T-NXN5; Khan, *supra* note 26.

leveraging their deep expertise, technologists have strengthened the agency's enforcement, policy, and public engagement work—allowing the agency to showcase timeliness and technical rigor that would have otherwise been difficult to achieve.

The agency's ability to continue responding nimbly to AI or the next developing technology will depend as much on institutional capacity and organization as it does on the agency's legal tools and strategy. Four decades ago, establishing economists as a key component of the agency's institutional structure and enforcement work was a key goal of Chairman Miller's tenure during the Reagan administration.[562] And during Chairman Muris's tenure in the 2000s, economists played a central role in shaping the agency's hands-off approach to subprime lending and mortgage disclosures.[563] The institutional role of economists at the FTC significantly reshaped the agency's consumer protection work.[564]

While much more nascent, the Office of Technology could be positioned to have a similarly profound impact across the agency's work. As digital tools and services are further integrated across our economy, maintaining and expanding the FTC's internal technological expertise will be critical for the agency to faithfully fulfill its mission.

Conclusion

The FTC's 1980 Policy Statement on Unfairness augured a new approach to consumer protection.[565] Government action to restrict predatory or exploitative business practices would be strongly disfavored, as markets were viewed as "self-correcting."[566] Consumers, the Policy Statement proclaimed, could protect themselves by avoiding "inadequate or unsatisfactory" products or services.[567] The principal focus of the agency's unfairness work would be "on the maintenance of consumer choice or consumer sovereignty."[568]

562. Paul A. Pautler, *A History of the FTC's Bureau of Economics* 73 n.268, 78 (Am. Antitrust Inst., Working Paper No. 15-03, 2015), https://perma.cc/VVA4-4UFQ (noting that economists obtained policy-related roles during the Miller Administration).

563. *See id.* at 76.

564. *Id.* at 79 (noting that economics has had a "major" impact since the mid-1970s).

565. *See* Letter from Pertschuk et al., *supra* note 178; *see also* Herrine, *supra* note 173, at 441-42 (describing the FTC's shift to a focus on consumer sovereignty).

566. Letter from Pertschuk et al., *supra* note 178.

567. *Id.*

568. Int'l Harvester Co., 104 F.T.C. 949, 1061 n.47 (1984).

This cramped vision of the agency's role would have a profound impact over the decades to come.[569] In the 1980s, the agency largely stopped writing rules or bringing unfairness cases.[570] The following decade, this timidity led the Commission to reject a staff recommendation to challenge the marketing of tobacco products to minors as unfair[571]—leading to accusations that Commissioners "had 'made themselves irrelevant.'"[572] And in the 2000s—as predatory mortgages ripped through the economy—the FTC stood on the sidelines, at times even applauding subprime lending as highly beneficial.[573]

By willfully retiring its own tools and authorities, the FTC defied its statutory mandate. And the practical stakes of its anemic approach became apparent in 2008, when markets "self-corrected" in the form of a financial meltdown.[574] Soon after, Congress would strip the FTC of key authorities to protect financial markets and create a new agency armed with new powers to rein in unfair, deceptive, and abusive practices.[575]

The global financial crisis presented a stark example of how the FTC's post-1980 approach failed the public. But this framework also had a profound impact on the agency's approach to enforcement in the digital age. On the one hand, the agency presciently warned about growing privacy threats in the 1990s. But especially after 2001, when key architects of the agency's 1980 revolution retook power, the FTC actively promoted "self-regulation" by private industry over vigorous enforcement and expressed abiding confidence

569. *See* Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC Act's Penalty Offense Authority*, 170 U. PA. L. REV. 71, 121-22 (2021) ("The takeover and subsequent gutting of the Federal Trade Commission by Chairman Miller is an underappreciated milestone in our nation's economic history.").

570. *See* Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935, 1958-60 (2000) (highlighting the dearth of FTC actions related to the Unfairness Statement); *see also* J. Howard Beales, Dir., Bureau of Consumer Prot., *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection,* FTC (May 30, 2003), https://perma.cc/9GPX-L3FE (noting that "[s]ubsequent to the codification of the unfairness test, however, the Commission showed extreme reluctance to assert its unfairness authority").

571. *See* John Harrington, *Up in Smoke: The FTC's Refusal to Apply the "Unfairness Doctrine" to Camel Cigarette Advertising*, 47 FED. COMMS. L.J. 593, 594 & n.6, 595 (1995).

572. *FTC Closing Its Camel Cigarettes Investigation Without Action*, FTCWATCH (June 6, 1994), https://perma.cc/BJ7Y-LTHD (quoting a Capitol Hill staff member).

573. *See* J. Howard Beales, Dir., Bureau of Consumer Prot., Prepared Statement of the Federal Trade Commission on Efforts to Combat Unfair and Deceptive Subprime Lending Before the Senate Special Committee on Aging 2-3 (Feb. 24, 2004), https://perma.cc/RJ7C-XFVW.

574. Chopra & Levine, *supra* note 569, at 76-77.

575. Keith Goodwin, *Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010*, FED. RSRV. HIST. (July 21, 2010), https://perma.cc/RZS3-4AT7 (describing the creation of the Bureau of Consumer Financial Protection).

in tech companies' ability to police themselves.[576] The agency limited its focus to the downstream consequences from data abuses, like identity theft and robocalls, and neglected the root causes driving and facilitating these illegal practices.

As with the agency's approach to subprime lending, this did not end well. Despite the agency's new focus on downstream harms, robocalls and identity theft actually exploded in the 2000s.[577] And while there was no single point of failure akin to the collapse of Lehman Brothers, the Cambridge Analytica scandal in 2018 led to severe criticism of the FTC's approach to privacy.[578] Many would call for the creation of a new standalone agency to serve as a digital regulator, in another parallel to the financial crisis.[579]

When we assumed leadership roles at the Commission in 2021, it was not to cede the agency's role to new enforcers. On the contrary, we wanted to harness the agency's exceptional strengths—its unique legal tools, its broad mission and jurisdiction, and its institutional expertise and committed staff—to vigorously protect the public from illegal business practices.

This Feature details how we aimed to reengineer the agency's approach to consumer protection in the digital age. Rejecting notice and consent, we advocated for—and repeatedly secured—actual limits on firms' ability to collect, use, and share consumers' data, including by targeting upstream actors.[580] Recognizing that the internet had become laden with traps—a place one of us has referred to as a virtual casino[581]—we also confronted manipulative online interfaces, overcoming doubts that unfairness could be a viable tool to combat "dark patterns."[582] And we paid particular attention to how the internet was harming young people, building a bipartisan consensus that the agency's unfairness authority could be used to protect teens online.[583]

Today there is a broader rethinking of the government's role in protecting the public and promoting fair dealing in our economy. The FTC has launched similarly ambitious efforts around junk fees,[584] gig

576. *See supra* Part I.A.

577. *See, e.g.*, *supra* note 132 (robocalls); *supra* note 217 (identify theft).

578. *See, e.g.*, Confessore & Kang, *supra* note 211.

579. *See supra* note 212 and accompanying text.

580. *See supra* Part II.A.

581. Samuel Levine, Dir., Bureau of Consumer Prot., Toward a Safer, Freer, and Fairer Digital Economy: How Proactive Consumer Protection Can Make the Internet Less Terrible, Remarks at Fordham Law School's Fourth Annual Reidenberg Lecture 8 (Apr. 17, 2024), https://perma.cc/VTB7-UPT2.

582. *See supra* Part II.A.

583. *See supra* Part II.B.

584. Press Release, FTC, Federal Trade Commission Announces Bipartisan Rule Banning Junk Ticket and Hotel Fees (Dec. 17, 2024), https://perma.cc/V4V5-VRHK.

work,[585] fake and deceptive reviews,[586] impersonation fraud,[587] tenant abuses,[588] small business credit reporting,[589] and franchising,[590] among other areas. In each of these domains, the FTC deployed a full set of tools—including rulemaking,[591] enforcement,[592] guidance,[593] and public notices[594]—to make markets fairer and more honest, whether by banning deceptive reviews,[595] prohibiting gag clauses that silenced franchisees,[596] or arming small businesses with new tools to protect their credit reports.[597] And the FTC is already demonstrating that it is prepared to confront the next wave of emerging technology—including artificial intelligence. [598]

These efforts have aimed to turn the page on four decades of neoliberal governance.[599] The 2024 election, in which Republicans retook control of the White House, raises questions about the institutional durability of these shifts.

Just as key tenets of the FTC's 1980s approach—such as the agency's abdication of its unfairness and rulemaking authorities—lasted decades beyond the Reagan-Bush era, it appears unlikely that the FTC will return to an entirely hands-off approach to consumer protection in the digital age.

---

585. Press Release, FTC, FTC to Crack Down on Companies Taking Advantage of Gig Workers (Sept. 15, 2022), https://perma.cc/MMH6-4QEB.

586. Press Release, FTC, Federal Trade Commission Announces Final Rule Banning Fake Reviews and Testimonials (Aug. 14, 2024), https://perma.cc/AB6S-XKVG.

587. Press Release, FTC, FTC Proposes New Protections to Combat AI Impersonation of Individuals (Feb. 15, 2024), https://perma.cc/3SG5-ZL6A.

588. Press Release, FTC, FTC Takes Action Against Invitation Homes for Deceiving Renters, Charging Junk Fees, Withholding Security Deposits, and Employing Unfair Eviction Practices (Sept. 24, 2024), https://perma.cc/MM2A-5W3R.

589. Press Release, FTC, FTC Launches Inquiry into Small Business Credit Reports (Mar. 16, 2023), https://perma.cc/9CUC-6FD2.

590. Press Release, FTC, FTC Takes Action to Ensure Franchisees' Complaints are Heard and to Protect Against Illegal Fees (July 12, 2024), https://perma.cc/MPV9-UESS.

591. *Rulemaking*, FTC, https://perma.cc/7BJ5-VU39 (archived Apr. 20, 2025).

592. *Enforcement*, FTC, https://perma.cc/KKK9-TZ8N (archived Apr. 20, 2025).

593. *Business Blog*, FTC, https://perma.cc/SYC7-PM2H (archived Apr. 18, 2025) (displaying FTC guidance blog posts).

594. *The Latest in Consumer Advice*, FTC CONSUMER ADVICE, https://perma.cc/EC27-HMMG (archived Apr. 20, 2025) (providing advice for consumers).

595. Press Release, *supra* note 586.

596. Press Release, *supra* note 590.

597. Press Release, *supra* note 589.

598. FTC, *Technology Is at an Inflection Point. The FTC Is on the Front Lines* (June 2025), https://perma.cc/U679-6QDT.

599. In January 2025, the Commission published a comprehensive account of its work during the Khan era. *See* FTC, FEDERAL TRADE COMMISSION ACCOMPLISHMENTS: JUNE 2021-JANUARY 2025 (2025).

First, key wins in court show the FTC's efforts are faithful to the law and a clearly permissible exercise of its authorities.[600] Second, polls and the extraordinary volume of public comments show the public widely supporting the FTC's most ambitious work, such as its efforts to protect children online.[601] Further, there is now bipartisan recognition of the threats posed by mass surveillance by private entities, with the Republican Chair of the Energy and Commerce Committee warning that "the massive commercial surveillance of data" is imperiling our liberties and fueling manipulation and discord.[602] Bipartisan support for protecting teens and cracking down on harmful data brokering can be seen both at the Commission[603] and in Congress.[604] Even "red" states like Texas are taking aim at dark patterns[605] and seeking algorithmic deletion remedies pioneered by the FTC.[606] To be sure, certain of the agency's more aggressive efforts to rein in harmful data abuses—especially rule-writing—is likely to slow down considerably.[607] But efforts to

600. *See* Order, FTC v. Amazon, Inc., No. 23-cv-00932 (W.D. Wash. May 28, 2024) (denying Amazon's motion to dismiss the FTC's lawsuit alleging that Amazon illegally made it difficult to cancel Prime subscriptions).

601. *See, e.g.*, Anika Dandekar & Marissa Farmer, *The FTC's Recent Actions and Proposals Command Wide, Bipartisan Support*, DATA FOR PROGRESS (Aug. 15, 2024), https://perma.cc/A5DA-CWAX.

602. Press Release, House Energy & Commerce Comm., Chair Rodgers Statement on the American Privacy Rights Act (June 27, 2024), https://perma.cc/GA2Q-ZGVA.

603. *See, e.g.*, *supra* note 428 and accompanying text (noting a unanimous vote). On multiple occasions, Republican commissioners have expressed support for these actions. *See* Melissa Holyoak, Comm'r, FTC, Concurring Statement in the Matter of Kochava, Inc. (July 15, 2024), https://perma.cc/S5UL-RTCJ; Christine S. Wilson, Comm'r, FTC, Concurring Statement Regarding Epic Games, Inc. (Dec. 19, 2022), https://perma.cc/ANR2-WC8T; *see also* Laura Kim, Terrell McSweeny, Andrew Smith & Emmie Habtemariam, *FTC Returns to Bipartisan Commission with Confirmation of Two New Republican Commissioners*, COVINGTON: INSIDE PRIVACY (Mar. 11, 2024), https://perma.cc/72XC-GAZ3 (listing Commissioner affiliations).

604. *See, e.g.*, Press Release, Senator Ted Cruz, Sen. Cruz Celebrates Senate Passage of Landmark Legislation to Protect Children Online (July 30, 2024), https://perma.cc/N8VP-WP63; Press Release, Rep. Davidson, Reps. Davidson, Lofgren, Nadler, Biggs, Buck, Jayapal, Massie, & Jacobs Introduce Bipartisan Fourth Amendment Is Not for Sale Act, Closing Warrantless Surveillance Loophole (July 18, 2023), https://perma.cc/4ACZ-D8X2.

605. TEX. BUS. & COM. CODE § 541.001(10) ("'Dark pattern' means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice, and includes any practice the Federal Trade Commission refers to as a dark pattern.").

606. *See* Plaintiff's Petition at 25, Texas v. Meta Platforms, Inc., No. 22-0121 (Tex. Dist. Ct. Feb. 14, 2022) (seeking an order requiring Meta to "[d]estroy any neural network or algorithm trained or improved using biometric identifiers unlawfully captured in Texas").

607. *See* Cristiano Lima-Strong, *Lina Khan's FTC Went After Big Tech. Trump Could Dial That Back*, WASH. POST (Nov. 12, 2024), https://perma.cc/U9QZ-SHSD.

issue[608] and enforce[609] new rules have earned bipartisan support, as have efforts to apply older rules to emerging data abuses.[610] This, combined with bipartisan support for a more expansive interpretation of unfairness,[611] suggests that the agency will not soon return to its post-1980 neoliberal approach.

The final week of the Khan Administration and first few months of the FTC under President Trump further demonstrate the potential durability of the agency's updated approach to digital oversight. In the span of five days at the end of Khan's tenure, the Commission strengthened protections for kids' privacy,[612] released interim findings around a major AI study,[613] challenged unsubstantiated claims that AI facial recognition software was bias-free,[614] brought its first-ever action challenging the marketing of loot boxes to children,[615] and finalized orders banning the sale of sensitive geolocation data[616]—all on a bipartisan basis. The Commission also notched its biggest win to date in its efforts to protect geolocation data, reaching a historic settlement with General Motors banning the automaker for five years from selling driver

608. Press Release, *supra* note 586 (unanimous vote to approve and issue a final rule banning fake reviews and testimonials).

609. Press Release, FTC, FTC Acts to Stop Student Loan Debt Relief Scheme that Took Millions from Consumers in First Case Under the Impersonation Rule (June 28, 2024), https://perma.cc/MD7V-EQDN (unanimous vote to stop a fraudulent student loan debt relief scheme in the agency's first action enforcing the Impersonation Rule, which went into effect in April 2024).

610. *See* GoodRx Enforcement Action Press Release, *supra* note 256.

611. *See supra* Part II.C.

612. Press Release, FTC, FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data (Jan. 16, 2025), https://perma.cc/E3Q2-R9F2.

613. Press Release, *supra* note 544.

614. Press Release, FTC, FTC Finalizes Order Prohibiting IntelliVision from Making Deceptive Claims About Its Facial Recognition Software (Jan. 13, 2025), https://perma.cc/64LG-2XSQ.

615. Press Release, FTC, Genshin Impact Game Developer Will be Banned from Selling Lootboxes to Teens Under 16 Without Parental Consent, Pay a $20 Million Fine to Settle FTC Charges (Jan. 17, 2025), https://perma.cc/J4KS-4Y59; *see also* FTC, Concurring Statement of Commissioner Rebecca Kelly Slaughter: Regarding *United States v. Cognosphere, LLC* 1 (Jan. 17, 2024), https://perma.cc/29SN-S7H6 (characterizing the case as "the first" to address video game loot box practices).

616. Press Release, FTC, FTC Finalizes Order Prohibiting Gravy Analytics, Venntel from Selling Sensitive Location Data (Jan. 14, 2025), https://perma.cc/CRU4-4BNS; Press Release, FTC, FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data (Jan. 14, 2025), https://perma.cc/4N5N-EEV4.

and location data and banning the use of dark patterns to obtain consent.[617] And within the first few months of the new administration, the new FTC Chair announced his intention to continue pursuing some of the initiatives highlighted in this Feature, including to enforce COPPA vigorously,[618] pursue an upstream approach to robocalls,[619] target injurious data practices,[620] prioritize the protection of teens,[621] and examine addictive digital design features.[622]

The FTC's consumer protection work these last few years modeled a break from the laissez-faire framework that had largely persisted since the Reagan revolution. By pursuing an approach rooted in fidelity to the FTC's full suite of authorities and the market realities of the digital age, the agency set out a new paradigm for consumer protection. While it is too early to tell how durable these changes will prove across administrations,[623] key programmatic victories in court, rare bipartisan agreement, and broad public support for the FTC's work may fortify these protections and help achieve a lasting shift away from disclosure-based regimes.

617. Press Release, FTC, FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent (Jan. 16, 2025), https://perma.cc/82RV-KRWG.

618. *Testimony of Chair Andrew N. Ferguson Before the House Appropriations Subcomm. on Fin. Servs. & Gen. Gov't*, 119TH CONG., at 13 (2025) (statement of Andrew N. Ferguson, Chair, FTC).

619. *Id.* at 4.

620. *Id.* at 13.

621. *Id.*

622. *Id.* at 14.

623. *See* Jordan Weissman, *Biden Led a Consumer Protection Revival. Will the Election Cut It Short?*, YAHOO! FINANCE (updated Nov. 4, 2024), https://perma.cc/N5TA-6SQ2.