



Bureau of Consumer Protection
Office of the Director

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Toward a Safer, Freer, and Fairer Digital Economy

How Proactive Consumer Protection Can Make the Internet Less Terrible

Remarks of Samuel Levine
Fourth Annual Reidenberg Lecture
Fordham Law School
April 17, 2024

Thank you for having me here today.¹ It's a true honor to be part of this event honoring the late Joel Reidenberg. He was someone who was constantly looking around corners, sounding the alarm on everything from the need for algorithmic fairness to the privacy risks of video games. I often like to think about the FTC's privacy work in terms like "cutting-edge" and "groundbreaking," but looking over Professor Reidenberg's scholarship, I'm reminded of how much we owe to academics, advocates, and others who dedicate much of their lives to addressing the thorny issues that the digital economy presents.

Even more so than when he passed away, today we are in a moment of real despair about the state of the internet and our digital economy. We have still not fully grappled with, let alone addressed, the consequences of commercial surveillance over the last few decades. And now these practices are not only unchecked but are spreading – to our devices, to our cars, to our schools, and to our workplaces. But while Professor Reidenberg was prescient about many of these challenges, he was also a believer in practical solutions, and he worked with policymakers

¹ The views expressed here are mine alone, and not that of the Commission or any Commissioner. I am grateful to Colin Hector for his substantial assistance in preparing these remarks.



UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Bureau of Consumer Protection
Office of the Director

to develop pioneering privacy interventions. That optimistic spirit is what I hope to channel in my remarks today.

I believe our digital economy can get better. Not because our tech giants will voluntarily change their ways, or because markets will magically fix themselves. But because, at long last, there is momentum across government – state and federal, Republicans and Democrats – to push back against unchecked surveillance. Today I will focus on the FTC’s role in this shift.

I’ll start by discussing how the notice and choice regime became entrenched, despite its well-known failures. Next, I’ll focus on an example of thoughtful government action – the FTC’s Holder Rule – that shows that this regime was not inevitable and need not be permanent. Then, I’ll lay out three goals for what a better digital economy might look like, and how the FTC is working to get us there. And finally, I’ll describe how the progress we are making on privacy is pointing the way toward a broader rethinking of how the government can make markets function better.

Part I: The Entrenchment of Notice and Choice

Let’s begin with the current privacy landscape. I’ll be brief. The problems with notice and choice have been clear for a long time. Americans are not reading every word of every privacy policy. Even if we did read the policies, it would be difficult to comprehend the full extent of how our data can be used. And even if we read the policies *and* understood them, we can hardly exercise choice given how much we rely on digital services, and the lack of competition in many

markets. So let's not mince words: notice and choice is a fantasy world, divorced from the reality of how people live or how firms operate.

The more interesting question is how we got here. Before the dot-com crash, the largest websites at the time, like AOL, earned revenue from subscriptions or banner ads, not so dissimilar from the business model for magazines and newspapers.² But when the crash hit in 2000, businesses needed to retool and find new sources of revenue. That year, Google began exploring how it could mine its user data logs for behavioral insights.³ To make a long story very short, this discovery transformed Google, and ultimately the internet. Companies realized that the data collected through digital interfaces could be used to target advertisements based on the behavior of particular consumers. And they realized they could *control* these interfaces, optimizing them for data collection, while obscuring the amount and sensitivity of the information being harvested. When the mobile internet took off, that cycle of more data extraction and less transparency accelerated further, now enriched by detailed information on consumers' location and social networks.

It's easy to fault tech companies for pursuing this strategy. But they were simply responding to incentives. The more striking aspect of this history is the government's failure to shift those incentives or otherwise take steps to protect the public. By the late 1990s there was a view in both major political parties that government should stay out of the way and firms should

² For instance, AOL's 10-K filing for fiscal year 2000 continued to describe the company's advertising and commerce strategy as focused on direct sales, subscriptions, and advertising placement, including sponsored ads. See AOL, Form 10-K for the fiscal year ending June 30, 2000, <https://www.sec.gov/Archives/edgar/data/883780/000088378000000098/0000883780-00-000098-0001.txt>.

³ For a detailed discussion of this history, see Shoshana Zuboff, *THE AGE OF SURVEILLANCE CAPITALISM* (2019), at 63-96.

be trusted to police themselves. In 1999, an FTC Commissioner called for a three-year moratorium on online privacy regulation, arguing that:

Consumers have to be accountable and bear some level of responsibility for their actions. 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.⁴

This unflinching confidence in the market to drive out bad practices was not shared by everyone. The same year those remarks were given, Professor Reidenberg described self-regulation as “pure sophistry” and explained that the marketplace for data was a “classic case of market failure[.]”⁵

But that warning did not prevail on regulators. On the contrary, two years later, the then-Chairman of the FTC argued that “it is clear that industry will continue to make privacy a priority[.]” and cautioned that legislation would be premature and could hold back the growth of the internet. Instead, the FTC announced an initiative to ensure privacy policies were posted and honored, and to encourage industry self-regulation.⁶

⁴ Orson Swindle, *Regulation of Privacy on the Internet: Where Do You Want to Go Today?*, April 8, 1999, <https://www.ftc.gov/news-events/news/speeches/regulation-privacy-internet-where-do-you-want-go-today>.

⁵ Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 Berkeley Tech. L.J. 771, 775-76 (Spring 1999).

⁶ Timothy J. Muris, Former Chairman, FTC, *Protecting Consumers' Privacy: 2002 and Beyond: Remarks at The Privacy 2001 Conference*, Oct. 4, 2001, <https://www.ftc.gov/news-events/news/speeches/protecting-consumers-privacy-2002-beyond>; see also John Schwartz, *F.T.C. Plans to Abandon New Bills On Privacy*, N.Y. TIMES, Oct. 3, 2001, <https://www.nytimes.com/2001/10/03/business/ftc-plans-to-abandon-new-bills-on-privacy.html>; Edmund Sanders, *FTC to Drop Push for More Privacy Laws*, L.A. TIMES, Oct. 2, 2001, <https://www.latimes.com/archives/la-xpm-2001-oct-02-fi-52289-story.html>; Jeffrey Benner, *FTC Refocuses Privacy Agenda*, WIRED, Oct. 5, 2001, <https://www.wired.com/2001/10/ftc-refocuses-privacy-agenda/>.

Looking back over the last quarter-century, I think it's fair to say that industry did not, in fact, make privacy a priority. Instead, the notice and choice regime became a way for companies to give invasive data practices a thin veneer of legitimacy, or what Daniel Solove recently called "a fiction of consent that is too fanciful even for magical realism."⁷ The results have been predictable. For the American public, deep cynicism has set in about their ability protect their personal information online.⁸ And this dissatisfaction is no longer confined to privacy.

Last year, the American Dialect Society crowned as its word the year "Enshittification" – Cory Doctorow's term for how leading internet firms degrade the quality of their offerings once consumers are locked in.⁹ It is no surprise that today, nearly three in four Americans – including strong majorities of both Democrats and Republicans – support stronger internet regulation.¹⁰

This malaise was not inevitable. In earlier periods of our history, government stepped in to make the market work better. As we hear warnings today that any government action will only make things worse, it is worth revisiting that history.

⁷ Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 Boston University Law Review 593, 597 (2024).

⁸ See, e.g., Joseph Turow, et al., *Americans Can't Consent to Companies' Use of Their Data*, Annenberg School for Communication, University of Pennsylvania (February 2023), available at https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf.

⁹ American Dialectic Society, *2023 Word of the Year is "Enshittification,"* Jan. 5, 2024, <https://americandialect.org/2023-word-of-the-year-is-enshittification/>; Corey Doctorow, *Pluralistic: Tiktok's enshittification*, PLURALISTIC, Jan. 21, 2023, <https://pluralistic.net/2023/01/21/potemkin-ai/>; see also Kyle Chayka, *Why the Internet Isn't Fun Anymore*, NEW YORKER, Oct. 9, 2023, <https://www.newyorker.com/culture/infinite-scroll/why-the-internet-isnt-fun-anymore> (arguing that the internet has become less fun in large part because a handful of giant social networks have taken over the open space of the Internet, with no comparable platform to replace an incumbent platform that has decayed).

¹⁰ Colleen McClain et al., *How Americans View Data Privacy*, Oct. 18, 2023, <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.

Part II: A Lesson from History

The mid-century growth of consumer credit is one area that offers some lessons. In the 50s and 60s, there was a massive push by businesses into the retail credit market.¹¹ Everything from boats to ovens to sewing machines were increasingly being bought through complex credit arrangements. And these contracts were designed to protect profits, not consumers.

Most notably, credit contracts included clauses that “cut off” a consumer’s rights once a loan was assigned, so that the consumer would be legally bound to pay the creditor even if the sale was fraudulent. Drawing on the holder in due course doctrine, these provisions allowed sellers and creditors to brazenly escape liability for bad practices. First, a seller would make a fraudulent sale on credit. The seller would insert a provision in the contract that barred the consumer from raising any of these problems against the holder of the loan. The seller would assign the loan, and the ripped-off consumer would be legally bound to pay on a bad deal.

This legal maneuver was a boon for a dizzying array of scam artists and unscrupulous businesses – everything from health clubs selling phony memberships to cemetery plot schemes. As the credit market grew, the “cut off” clauses became standard and consumers were routinely presented with a “take it or leave it” agreement, without any opportunity or ability to bargain, and often no alternatives to dealing with certain merchants.

As the FTC observed, the result in the credit market was “the externalization of seller misconduct costs.”¹² The Commission responded to this problem with the Holder Rule, which

¹¹ Much of the discussion of the credit market and Holder Rule is drawn from the statement of basis and purpose that the Commission published in 1975, when the rule was issued. Federal Trade Commission, *Part 433—Preservation of Consumers’ Claims and Defenses, Promulgation of Trade Regulation Rule and Statement of Basis and Purpose* (hereinafter “*Holder Rule SBP*”), 40 F.R. 53506 (Nov. 18, 1975).

¹² 40 F.R. 53523.

reallocated these costs by closing the underlying contractual loophole, allowing borrowers to assert claims and defenses against purchasers of their loans.¹³ Where creditors previously had little incentive to police the retail market, they now needed to worry about seller misconduct, because they could be left holding the bag. And for consumers, the Rule simply reflected the common-sense expectation that if the merchant doesn't follow through on its promises, you shouldn't have to follow through on yours.

The Rule was one of several laws and regulations that imposed limits on consumer credit practices.¹⁴ Despite dire warnings from industry, these changes did not make the sky fall or cause the credit market to dry up. Consumer credit continues to be very competitive, and the Holder Rule continues to provide fundamental protections that promote confidence in the lending system.¹⁵

While the mid-century consumer credit market differs from today's digital landscape in many ways, there are some important similarities. Both involved rapid changes in complex markets. Both involved an enormous difference in power between the businesses drafting the agreements and the consumers on the other side of transaction. And in both situations, industry used a version of notice and choice, weaponizing fine-print contractual provisions to shift risk and responsibility away from themselves and onto consumers.

¹³ 16 C.F.R. pt. 433.

¹⁴ These included the Truth in Lending Act, 15 U.S.C. § 1601 et seq., the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., and the Equal Credit Opportunity Act, 15 U.S.C. § 1691 et seq.

¹⁵ It is notable that during the FTC's most recent review of the rule, all commenters and all five Commissioners supported retaining it. See <https://www.ftc.gov/news-events/news/press-releases/2019/05/ftc-completes-review-holder-rule>.

As the Holder Rule shows, well designed government action does not distort the free market – it makes it work better. By properly aligning incentives and allocating legal responsibility, trust grows and firms can compete on value. To be clear, humility is an important virtue for regulators – unintended consequences, regulatory burden, and imperfect information are all ever-present concerns. But there are also risks to inaction, and the consequences of failing to act can leave the public worse off, especially when it allows businesses to shift the cost of misconduct onto consumers. We saw that in credit markets half a century ago, and we see it in our digital economy today.

Part III. Three Goals for a Better Digital Economy

I now want to turn to what the FTC is doing to address misaligned privacy incentives and make the digital economy work better. We've been busy – bringing scores of enforcement actions, proposing new rules, and launching important market studies. But amidst all this activity it's easy to miss the forest for the trees. We are not nibbling around the edges and pretending the status quo is acceptable. Our work reflects a concerted strategy to make our digital economy work better for *people*, rather than a handful of tech giants.

I will focus on three goals we are working to advance. First, we want Americans to be able to enjoy a zone of privacy on the internet, rather than needing to surrender to constant surveillance that undermines our fundamental freedoms. Second, we want the internet to feel less like a casino – where kids can get hooked, and all consumers face a minefield of tricks and traps. And third, we want to make sure AI tools are serving *people*, and not the other way around.

I'll discuss each of these goals in turn, and describe the work the FTC is doing to drive them forward.

1. Establishing a Zone of Privacy on the Internet.

The first goal, quite simply, is an internet with less surveillance. Today's commercial surveillance practices are threatening not only our privacy but our fundamental freedoms.

The Constitution ensures that we can make choices about our personal behavior by guarding against unfettered government surveillance. But it doesn't protect us against commercial surveillance – that our private movements, behaviors, and decisions could be revealed to employers, companies, neighbors, or anyone else who's willing to pay.

One of the most valuable aspects of privacy is that it allows us to order our private lives in ways that reflect our beliefs and preferences, even if we might be out of step with others. So with commercial surveillance, the danger is not just the erosion of privacy. It's that we will lose the breathing space for a host of other freedoms, including our freedom of thought, our freedom of religion, and our freedom of expression.

At a high level, the solution is straightforward. Firms need to collect and retain less data about us, and secure it better. Yet the behavioral ad-driven business model that has shaped the internet for decades has pushed firms in the opposite direction – contributing to privacy abuses growing worse, and data breaches growing ever more catastrophic.¹⁶ And until very recently, there was little in the way of government pushback – binding efforts to realign incentives in the public interest, rather than simply urging companies to disclose what they're doing.

¹⁶ Businesses can also be harmed from fraudulent web traffic and inflated claims of ad efficiency, calling into question the value proposition from behavioral advertising. *See, e.g.,* Morgan Meaker, *How Bots Corrupted Advertising*, Sept. 29, 2022, WIRED, available at <https://www.wired.com/story/bots-online-advertising/>; *see also* Musti Schnadower et. al., *Behavioral Advertising and Consumer Welfare: An Empirical Investigation*, March 23, 2023, available at <http://dx.doi.org/10.2139/ssrn.4398428>.

But today, that is changing. We are seeing significant momentum in Congress and in states across the country to pass privacy legislation. And at the FTC, we are securing real limits on the handling of people’s data that people did not believe was possible just a few years ago.

Consider our work on location data. Nowhere is the failure of notice and choice more apparent than in the ability of just about anyone – from scammers to domestic abusers to foreign adversaries – to track our movements. The FTC has warned against the improper sharing of sensitive location data for many years. But today, for the first time, we are challenging these practices head-on.

In two recent orders against data brokers, we secured binding prohibitions on the sale of sensitive location information.¹⁷ One of these firms used this data to build profiles of consumers, like “Christian church goers” and “wealthy and not healthy.”¹⁸ Our order prohibited that practice, too. And both firms are required to ensure the data they obtain from others is collected lawfully.¹⁹ As with the Holder Rule and sales fraud, this requirement will help ensure that downstream actors stop the flow of illegally collected data, instead of profiting off it.²⁰

We’ve notched similar wins in other areas. Over the last three years, we have secured bright-line bans in five cases on the sharing of sensitive health data for advertising purposes –

¹⁷ Proposed Order, *In re InMarket Media, LLC*, FTC No. 2023088, available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023088-inmarket-media-llc>; Final Order, *In re X-Mode*, Dkt. No. C-4802, available at https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf.

¹⁸ Press Release, *FTC Order Will Ban InMarket from Selling Precise Consumer Location Data*, Jan. 18, 2024, <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data>.

¹⁹ See Provision VI, Proposed Order, *In re InMarket Media*; Provision VII, Final Order, *In re X-Mode*.

²⁰ Notably, these actions are helping to catalyze industry-wide changes. See Network Advertising Initiative, *NAI Working with Members to Develop New Industry Guidelines for Sensitive Location Data*, Jan. 24, 2024, <https://thenai.org/press/nai-working-with-members-to-develop-new-industry-guidelines-for-sensitive-location-data/>.

two of them announced over the last week.²¹ We've secured sixteen orders with data minimization requirements.²² We secured our first-ever ban on the sharing of browsing data.²³ We proposed changes to COPPA that strengthen security requirements, restrict targeted advertising, and make clear that kids' data cannot be retained indefinitely.²⁴ And all of this work is helping inform our ongoing surveillance rulemaking proceeding, where we are considering market-wide rules to protect consumers' data.²⁵

Importantly, we were able to take these actions by embracing the “U” in our UDAP authority – unfairness. Deception is a critical tool, and we expect firms to tell the truth. But these cases reflect the view that not all harms can be solved by disclosures, even truthful ones. Just as we utilized our unfairness authority 50 years ago by issuing the Holder Rule to curb predatory credit provisions, today we are using that same authority to challenge harmful data practices.

²¹ Proposed Order, *United States v. Cerebral, Inc.*, No. 1:24-cv-21376 (S.D. Fla. Apr. 15, 2024), available at https://www.ftc.gov/system/files/ftc_gov/pdf/cerebral_joint_stipulation_order_permanent_injunction.pdf; Proposed Order, *United States v. Monument*, No. 12:24-cv-01034 (D.D.C. Apr. 11, 2024), available at https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf; Order, *United States v. GoodRx Holdings, Inc.*, No. 23-cv-460 (N.D. Cal. 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/goodrxfinalstipulatedorder.pdf”https://www.ftc.gov/system/files/ftc_gov/pdf/goodrxfinalstipulatedorder.pdf; Order, *In re BetterHelp, Inc.*, FTC Dkt. C-4796, available at https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpfinalorder.pdf; Order, *United States v. Easy Healthcare Corp.*, No. 23-cv-03107 (N.D. Ill. 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.22_easy_healthcare_signed_order_2023.pdf.

²² 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](#) (f/k/a Weight Watchers).

²³ Press Release, *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://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over>.

²⁴ Press Release, *FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data*, Dec. 20, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens>.

²⁵ Press Release, *FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices*, Aug. 11, 2022, <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices>.

And we recently secured a significant win when a federal court found that the invasion of privacy can be a cognizable harm under the FTC Act’s unfairness prohibition.²⁶

I strongly support both state and federal efforts to pass strong data protection legislation. Indeed, these efforts are urgent. But at the FTC, we are not just watching and waiting. We are undertaking a concerted strategy to demonstrate how the FTC Act requires substantive protections for people’s data, rather than simply more disclosures. And the wins that we are securing point the way toward how our digital future can afford us more autonomy, more privacy, and more freedom than is possible under the status quo.

2. Making the Internet Less Like a Casino

One of the key consequences of our status quo of unchecked surveillance has been the emergence of a casino-like interface across the web, with firms using sophisticated behavioral techniques – refined and perfected by hoovering up data – to manipulate us. That is why another key goal for the FTC is to make the internet safer by cracking down on harmful online interfaces.

We have a lot of work to do. In 2022, we published a staff report warning about the increasing prevalence of dark patterns across the internet.²⁷ Gig platforms are reportedly using nudges and other gaming-like features to keep drivers on the road.²⁸ Investment apps are

²⁶ Mem. Decision & Order, *FTC v. Kochava, Inc.*, No. 2:22-cv-00377-BLW, at 10-13 (D. Idaho Feb. 3, 2024), available at https://www.ftc.gov/system/files/ftc_gov/pdf/71-OpiniononMTD.pdf.

²⁷ FTC Staff Report, *Bringing Dark Patterns to Light*, Sept. 2022., https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

²⁸ Veena Dubal, *The House Always Wins: The Algorithmic Gambification of Work*, Jan. 23, 2023, THE LPE PROJECT, <https://lpeproject.org/blog/the-house-always-wins-the-algorithmic-gambification-of-work/>; Noam Scheiber, *How Uber Uses Psychological Tricks to Push Its Drivers’ Buttons*, Apr. 2, 2017, N.Y. TIMES, <https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html>.

designed to lure users into making bigger and riskier bets.²⁹ And as many firms turn from a model of selling goods to a model of selling subscriptions, too many of them are embracing user interfaces that obscure fees or deter cancellation.³⁰

The FTC’s work to limit overcollection is addressing one of the root causes of this phenomenon, but we are also challenging harmful and coercive interfaces more directly. In a string of actions, most recently against Amazon and three of its top executives, we have charged that the use of dark patterns to trap people in subscriptions or rack up junk fees is unlawful.³¹ In our action against Publishers Clearing House, our order required an overhaul of PCH’s design interface, a ban on hidden fees, and a requirement that PCH preserve “any market, behavioral, or psychological research[.]”³² After we charged Epic Games with employing unfair default settings, we secured an order requiring stronger privacy settings to protect children and teens, along with more than \$500,000,000 in monetary relief for privacy violations and for other illegal conduct.³³ We have pioneered the use of our Section 19 authority to compensate consumers when their time is wasted by harmful interfaces.³⁴ And we have been using our rulemaking

²⁹ See, e.g., Am. Admin. Complaint, *In re Robinhood Financial, LLC*, Dkt. No. E-2020-0047, Oct. 21, 2021, available at <https://www.sec.state.ma.us/divisions/securities/download/MSD-Robinhood-Amended-Complaint-Docket%20No-%20E-2020-0047.pdf>.

³⁰ These practices are discussed in the FTC staff report on dark patterns, *supra* n. 27.

³¹ Press Release, *FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel*, June 21, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their>.

³² Provision XII.C, Order, *FTC v. Publishers Clearing House*, No. 2:23-cv-04735-ENV-LGD (E.D.N.Y. June 30, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/15StipulatedOrderasenteredbycourt.pdf.

³³ Press release, *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://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations>.

³⁴ Press release, *FTC Takes Action Against Publishers Clearing House for Misleading Consumers About Sweepstakes Entries*, June 27, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-publishers-clearing-house-misleading-consumers-about-sweepstakes-entries> (discussing order including

authority to establish across-the-board protections, including by proposing a market-wide ban on hidden fees, a requirement to make subscriptions easy to cancel, and limits on nudges that keep kids hooked.³⁵

Our work is not going to fix the internet overnight. And I worry constantly that for kids today, who are facing an onslaught of harmful design practices, a better internet may come too late. But as with our efforts on data minimization, it's important to step back and recognize the leap we've made. Manipulative design choices do not always involve misleading claims. But through our rulemaking, our unfairness actions, and our forward-leaning remedies, we're making clear that they are not beyond the reach of our authority. And this shift – while early – creates a path for more assertive actions across the board.

With the emergence of AI, this shift cannot come soon enough. We know that firms are under enormous pressure to maximize engagement, and artificial intelligence threatens to become a force multiplier, creating far more powerful feedback loops to manipulate user behavior and maintain ever-higher levels of engagement. Making sure that AI works for people, and not the other way around, is the third issue I want to discuss.

3. Ensuring AI Work for Us, and Not the Other Way Around

I don't need to tell you that we are seeing a lot of hype around artificial intelligence. At the FTC, just as we examined the broader credit ecosystem in crafting the Holder Rule, we are

\$18.5 million monetary judgment); Press release, *FTC Takes Action to Stop Credit Karma From Tricking Consumers With Allegedly False "Pre-Approved" Credit Offers*, Sept. 1, 2022, <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-takes-action-stop-credit-karma-tricking-consumers-allegedly-false-pre-approved-credit-offers>.

³⁵ Press release, *FTC Proposes Rule to Ban Junk Fees*, Oct. 11, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-proposes-rule-ban-junk-fees>; Press release, *Federal Trade Commission Proposes Rule Provision Making it Easier for Consumer to "Click to Cancel" Recurring Subscriptions and Memberships*, Mar. 23, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/03/federal-trade-commission-proposes-rule-provision-making-it-easier-consumers-click-cancel-recurring>; Press release, *supra* note 24.

looking at every layer of the AI tech stack, including cloud infrastructure, microprocessors, and foundation models.³⁶ Today I want to focus particularly on AI tools, where the FTC is working to ensure they work for *people*, and not the other way around.

In these early days, people are using AI tools in all sorts of exciting ways – from learning a new language to disputing medical bills. But we know from the development of the web over the last three decades that these dynamics can change. Young people today might enjoy using image generation tools to imagine how they’ll look in the future. But these same tools – trained on millions of faces – can be used by private and public actors alike to surveil and manipulate us in harmful ways. Likewise, while job applicants might appreciate being able to enhance their resume with the help of AI, we may soon find employers relying on AI recommendation systems that replicate discriminatory practices we’ve tried to eradicate in the real world.

Against this backdrop, the FTC is making clear that we will not repeat the mistakes of the 2000s. We’ve been stressing that there is no AI exception in the law. And we are following up with action.

First, we want to make sure AI tools aren’t used to defraud people. We’re deploying our rulemaking authority to arm us with new tools to combat AI-powered impersonation frauds, and to hold accountable firms that provide the means and instrumentalities to commit such fraud.³⁷

We’ve made clear that AI robocalls are not exempt from our Telemarketing Sales Rule.³⁸ We

³⁶ See, e.g., FTC Office of Technology, *Tick, Tick, Tick. Office of Technology’s Summit on AI*, Jan. 18, 2024, <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/tick-tick-tick-office-technologys-summit-ai>.

³⁷ Press release, *FTC Proposes New Protections to Combat AI Impersonation of Individuals*, Feb. 15, 2024, <https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals>.

³⁸ Press release, *FTC Implements New Protections for Businesses Against Telemarketing Fraud and Affirms Protections Against AI-enabled Scam Calls*, Mar. 7, 2024, <https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-implements-new-protections-businesses-against-telemarketing-fraud-affirms-protections-against-ai>.

launched a groundbreaking Voice Cloning Challenge to generate ideas on tools to fight back against voice cloning fraud.³⁹ And we proposed a rule cracking down on firms that generate fake reviews – yet another online scourge that AI threatens to turbocharge.⁴⁰

We also want to make sure that AI tools are developed responsibly, and are not trained on illegally collected data. We’ve put out business guidance making clear that firms can’t sneak changes into their terms of services to Hoover up more data to train AI,⁴¹ and we’ve laid the groundwork for challenging such practices in a recent enforcement action.⁴² Our proposed amendments to COPPA make clear that firms can’t retain kids’ data indefinitely to train models.⁴³ And many firms have noticed that in nine cases and counting over the last few years, we’ve required firms to delete work product or models trained on illegal collected data.⁴⁴

Finally, we want to make sure that AI decision-making tools are not being used to discriminate illegally, and that the use of technology doesn’t become a liability shield for those who use these tools in harmful ways. In 2021 we made clear that discrimination can be an unfair practice under the FTC Act, and we’ve now followed up with actions challenging harmful practices that target Black, Latino, and Native American consumers, as well as consumers who

³⁹ The FTC Voice Cloning Challenge, <https://www.ftc.gov/news-events/contests/ftc-voice-cloning-challenge>.

⁴⁰ Press release, *Federal Trade Commission Announces Proposed Rule Banning Fake Reviews and Testimonials*, June 30, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/06/federal-trade-commission-announces-proposed-rule-banning-fake-reviews-testimonials>.

⁴¹ FTC Tech. Blog, *AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive*, Feb. 13, 2024, <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive>.

⁴² Press release, *FTC Says Genetic Testing Company 1Health Failed to Protect Privacy and Security of DNA Data and Unfairly Changed its Privacy Policy*, June 16, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-says-genetic-testing-company-1health-failed-protect-privacy-security-dna-data-unfairly-changed>.

⁴³ *Supra* n. 24.

⁴⁴ See, e.g., Provision II, Modified Order, *In re RiteAid*, FTC Dkt. C-4308, https://www.ftc.gov/system/files/ftc_gov/pdf/c4308riteaidmodifiedorder.pdf. The other orders are in the FTC’s cases against [Ring](#), [Edmodo](#), [X-Mode Social](#), [InMarket Media](#), [Kurbo](#) (f/k/a Weight Watchers), [Avast](#), [CRI Genetics](#), [EverAlbum](#), and [Monument](#).

receive public benefits.⁴⁵ We are also vigorously enforcing one of the original data protection laws, the Fair Credit Report Act, and last year joined with the CFPB to bring our largest-ever action involving inaccurate tenant screening products.⁴⁶ And at the end of last year, we brought a groundbreaking action against Rite Aid, charging the company with recklessly using AI facial recognition technology that falsely tagged consumers, especially women and people of color, as shoplifters.⁴⁷

Our Rite Aid action underscores how our approach to AI is departing from our approach to Web 2.0. Our lawsuit was brought under an unfairness theory, which encompassed the myriad ways Rite Aid’s practices were harming consumers.⁴⁸ And the order we secured did not require Rite Aid to install bigger signs that consumers were being surveilled. It banned the practice for five years, and imposed sweeping restrictions on Rite Aid’s future use of biometric surveillance systems – including by requiring rigorous testing for discrimination and inaccuracy.⁴⁹

⁴⁵ Press release, *Federal Trade Commission Takes Action Against Passport Automotive Group for Illegally Charging Junk Fees and Discriminating Against Black and Latino Customers*, Oct. 18, 2022, <https://www.ftc.gov/news-events/news/press-releases/2022/10/federal-trade-commission-takes-action-against-passport-automotive-group-illegally-charging-junk-fees>; Press release, *FTC Acts to Stop FloatMe’s Deceptive ‘Free Money’ Promises, Discriminatory Cash Advance Practices, and Baseless Claims around Algorithmic Underwriting*, Jan. 24, 2024, <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-acts-stop-floatmes-deceptive-free-money-promises-discriminatory-cash-advance-practices-baseless>; *FTC Takes Action Against Multistate Auto Dealer Napleton for Sneaking Illegal Junk Fees onto Bills and Discriminating Against Black Consumers*, Apr. 1, 2022, <https://www.ftc.gov/news-events/news/press-releases/2022/04/ftc-takes-action-against-multistate-auto-dealer-napleton-sneaking-illegal-junk-fees-bills>.

⁴⁶ Press release, *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://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-cfpb-settlement-require-trans-union-pay-15-million-over-charges-it-failed-ensure-accuracy-tenant>.

⁴⁷ FTC Legal Library, *FTC v. Rite Aid Corp.*, <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v>.

⁴⁸ Complaint, *FTC v. Rite Aid Corp.*, No. 2:23-cv-05023 (D. Penn. Dec. 19, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf (Count I).

⁴⁹ Stip. Order, *FTC v. Rite Aid Corp.*, No. 2:23-cv-05023-KBH (D. Penn. Feb. 26, 2024), available at https://www.ftc.gov/system/files/ftc_gov/pdf/DE019-StipulatedOrderforPermanentInjunctionandOtherRelief.pdf.

Here again, the FTC has much work to do to keep pace with the rapid development and deployment of AI tools. Indeed, we're already seeing some firms trying to return the familiar notice-and-choice playbook.⁵⁰ But in contrast to the late 90s, today we see enforcers and policymakers across the government committed to making sure AI tools work for *us*.⁵¹ Few are calling for a repeat of the laissez-faire approach that failed. And that gives me hope.

Conclusion

So let me conclude on an optimistic note. While we have a long way to go between the digital economy we have and the digital economy we need, I am proud of the progress the FTC has made over the past three years. We are taking bold action, using every tool we have, to protect privacy, combat online manipulation, safeguard the public from AI-related harms, and more. And we are frankly and firmly rejecting the view that consumers can protect themselves from harmful practices by reading more disclosures.

Our proactive approach to privacy should not be viewed in a vacuum. Rather, it represents the tip of the spear in a broader rethinking of the government's role in making markets work better. Across our agency, we are taking on some of the most pressing challenges facing the public. We've proposed a ban on junk fees, and delivered significant new protections for small businesses against fraud. We've cracked down on patent abuses that jack up the cost of medical devices, prompting manufacturers to cut the price of inhalers. We've worked with states across

⁵⁰ Geoffrey A. Fowler, *Your Gmail and Instagram are training AI. There's little you can do about it*, WASH. POST, Sept. 8, 2023, <https://www.washingtonpost.com/technology/2023/09/08/gmail-instagram-facebook-trains-ai/>.

⁵¹ For example, recently the United States House of Representatives established a bipartisan AI taskforce, and last week Senator Cantwell and Rep. McMorris-Rogers unveiled the American Privacy Rights Act. *See* Press Release, Mike Johnson, Speaker of the House, *House Launches Bipartisan Task Force on Artificial Intelligence*, Feb. 20, 2024, <https://www.speaker.gov/house-launches-bipartisan-task-force-on-artificial-intelligence/>; Press Release, U.S. Senate Committee on Commerce, Science & Transportation, *Committee Chairs Cantwell, McMorris, Rodgers Unveil Historic Draft of Comprehensive Privacy Legislation*, Apr. 7, 2024, <https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-data-privacy-legislation>.

the country to make it easier for consumers to repair their products. We've launched important market studies on PBMs, cloud computing, and social media fraud. And we proposed a ban on noncompete agreements that suppress wages and undermine innovation. Across markets and across our mission, we are fighting for the public interest with every tool we have.

These actions also serve a broader purpose. They are a reminder that government can and will take bold action to make people's lives better. We received more than 60,000 comments on our proposal to ban junk fees, and more than 27,000 comments on our proposal to ban noncompetes. Having such broad engagement with our work is something the FTC has not seen in decades. Whether you look at our rulemaking docket, watch one of our Open Commission Meetings, or attend one of our recent workshops, it is clear we have tapped into grassroots frustration with how markets are working. And our engagement with the public is helping us lay out clear proposals for how we can make markets work better.

So at the FTC and across the government, the tide is turning. We are actively tackling the biggest problems facing the public, and we are building a track record of real wins for the American people. This paradigm shift would not be possible without the imaginative work of people like Luke Herrine, Frank Pasquale, Julia Angwin, and Samantha Vaughn. And of course, their work stands on the shoulders of giants, none more so than Professor Reidenberg. After he passed away, Professor Reidenberg was lauded for his "daring optimism."⁵² I think we'd all agree that it is hard to be optimistic about our digital future. But we won't make progress unless we can dare to do so.

⁵² Jedidiah Bracy, *Joel Reidenberg: 1961-2020*, THE PRIVACY ADVISOR, Apr. 23, 2020, <https://iapp.org/news/a/joel-reidenberg-1961-2020/>.

Thank you for inviting me today. I am honored to be here, and am looking forward to our discussion.