

epic.org

**ELECTRONIC
PRIVACY
INFORMATION
CENTER**

Statement of John Davisson

Director of Litigation and Senior Counsel, Electronic Privacy Information Center (EPIC)

Hearing on “Federal Trade Commission Practices: A Discussion on Past Versus Present”

Before the

House Committee on Energy and Commerce
Innovation, Data, and Commerce Subcommittee
United States House of Representatives

September 19, 2024

Chair Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee: thank you for the opportunity to testify today about the past, present, and future of the Federal Trade Commission’s consumer and data protection work. My name is John Davisson, and I am the Director of Litigation and Senior Counsel at the Electronic Privacy Information Center, or EPIC. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. For 30 years, EPIC has been one the foremost advocates for privacy rights in both the public and private sectors.

Today’s hearing explores how the FTC’s approach to protecting consumers has changed in recent years. As a leading and longtime proponent of FTC action to safeguard consumer privacy, EPIC agrees that the Commission’s approach has changed—and changed for the better. Too often since the internet rose to prominence in the 1990s, the FTC has failed to keep pace with dramatic shifts in technology and data-driven business practices, exposing consumers to privacy violations and unfair data practices in the digital age. Although the data protection crisis we face today is a systemic failure far bigger than any one agency, missed opportunities by the FTC and a regrettable tendency toward “notice and choice” and “self-regulation” enabled that crisis to swell for years.

But the Commission has begun to turn the tide. Under recent leadership, the FTC has stepped up enforcement against abusive data practices and unfair algorithmic systems, undertaken sorely needed rulemakings to establish rules of the road for industry, adapted remedies to meet the moment, built deeper technical expertise, refocused its privacy agenda on the harms suffered by consumers, and brought greater transparency and public engagement to its proceedings. And it has done all these things with far fewer resources than peer regulators in

other democracies.¹ This work is well within the FTC’s principal mandate to prohibit unlawful trade practices, including “[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.”²

For consumers anxious about their privacy in the online era, the recent shifts in the FTC’s data protection work are a welcome sight. But in a way, they’re also a return to form: the FTC boasts a long tradition of evolving regulatory strategies. Since the FTC’s founding over a century ago, Congress has entrusted the Commission with expansive powers and given it the flexibility to respond to novel risks to consumers as they emerge. Throughout its history, the Commission has used that toolkit to fashion new regulatory approaches to new regulatory problems—from cigarettes to green marketing to information privacy.³ The FTC’s latest efforts to make privacy and civil rights protections a reality for consumers represent the next chapter in that history.

Of course, establishing meaningful protections for personal data across a \$28 trillion economy⁴ is an immense challenge, and that work is far from done. Some key pillars of the FTC’s privacy and civil rights agenda—including its rulemaking on commercial surveillance and data security⁵—are still in progress. The news abounds with reports of data breaches, invasive tracking practices, and dubious AI systems that put consumers at risk, underscoring the continued importance of vigorous FTC enforcement. And the need for Congress to enact

¹ See Fed. Trade Comm’n, *FTC Report to Congress on Privacy and Security* at 7 (2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

² 15 U.S.C. § 45(a)(1).

³ Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* xvi (2016).

⁴ Press Release, Bureau Econ. Analysis, Gross Domestic Product (Second Estimate), Corporate Profits (Preliminary Estimate), Second Quarter 2024 (Aug. 29, 2024), <https://www.bea.gov/news/2024/gross-domestic-product-second-estimate-corporate-profits-preliminary-estimate-second>.

⁵ Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022) (to be codified at 16 C.F.R. ch. 1), <https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security>.

comprehensive privacy legislation is greater than ever. The FTC's ability to safeguard consumer privacy would be dramatically strengthened by the passage of a federal privacy law backed by robust enforcement resources. Like all five sitting members of the Commission, EPIC supports the Committee's ongoing bipartisan efforts to enact such legislation.

Until then, it will fall to the FTC to confront harmful commercial data practices with the tools at its disposal. To fulfill its consumer protection mandate, the Commission must continually adapt its regulatory strategies to respond to technological and economic change. Mechanical adherence to the ways of the past will not protect consumers from the hazards of the present and the future. EPIC is pleased that today's FTC has taken that lesson to heart and recommitted itself to delivering real results for consumers. We hope the Committee will continue to support the Commission in that endeavor.

In my testimony today, I will (1) offer a brief overview of the data protection crisis confronting U.S. consumers; (2) identify some of the key shortcomings in the data protection strategies of the FTC over the past two decades; (3) explain how the Commission's recent enforcement, rulemaking, and public engagement efforts are meeting the moment to stop unfair trade practices; and (4) respond to several unfounded critiques of the current Commission's data protection work.

I. The data protection crisis

As the Committee well understands, the United States faces a data protection crisis. The lack of comprehensive privacy laws and regulations has allowed abusive data practices to flourish, creating a persistent power imbalance that threatens both individual rights and

competitive markets.⁶ Through the failure of policymakers—including the FTC—to establish adequate data protection standards, online firms have been allowed to deploy commercial surveillance systems that collect and commodify every bit of our personal data. The platforms and data brokers that track us across the internet and build detailed profiles used to target us with advertisements also expose us to an ever-increasing risk of breaches, data misuse, manipulation, and discrimination.⁷ The impacts of these commercial surveillance systems are especially acute for marginalized communities,⁸ where they foster discrimination and inequities in employment, government services, healthcare, education, and other life necessities.⁹

Many of the companies building and fueling the commercial surveillance ecosystem do not even have a direct relationship with consumers. These data brokers only exist to collect, store, sell, transfer, trade, and analyze data to profile and track us. They analyze our personal data and sell profiles to advertisers, publishers, and other entities for their own purposes. In many cases, data brokers and ad tech companies use these profiles to target or shape consumers' experience of the websites and services they visit in ways that are entirely opaque to them.

⁶ See generally Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019).

⁷ See EPIC, Comments on the Fed. Trade Comm'n Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 45–55 (Nov. 21, 2022), <https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf> [hereinafter *Disrupting Data Abuse*]; Caroline Kraczon, *Google Ad Topics: Another Cog in the Surveillance Advertising Machine*, EPIC Blog (Sept. 22, 2023), <https://epic.org/google-ad-topics-another-cog-in-the-surveillance-advertising-machine/>.

⁸ Legislative Solutions to Protect Kids Online and Ensure Americans' Data Privacy Rights: Hearing before the Subcomm. on Innovation, Data, and Com. of the H. Comm. on Energy & Com., 118th Cong. (2024) (testimony of David Brody), <https://www.lawyerscommittee.org/wp-content/uploads/2024/04/David-Brody-Lawyers-Committee-House-EC-Cmte-Written-Testimony-4-17-24-PM-Final.pdf>.

⁹ *Disrupting Data Abuse*, supra note 7, at 109–51; Anita Allen, *Dismantling the “Black Opticon”: Privacy, Race Equity, and Online Data-Protection Reform*, 131 Yale L.J.F. 907, 913–28 (Feb. 20, 2022), <https://www.yalelawjournal.org/forum/dismantling-the-black-opticon>. See also generally Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (2018).

Businesses use these profiles to alter what we see, what prices we pay, and whether we can find the information we seek online.

The dimensions of the data protection crisis are difficult to fathom. To participate in today's economy is to have our personal data extracted, aggregated, commercialized, and sold—as we work,¹⁰ eat,¹¹ pray,¹² study,¹³ socialize,¹⁴ browse the internet,¹⁵ seek medical advice,¹⁶

¹⁰ See, e.g., *Workplace Privacy*, EPIC (2023), <https://epic.org/issues/data-protection/workplace-privacy/>; Benjamin Wiseman, Fed. Trade Comm'n, Remarks of Benjamin Wiseman at the Harvard Journal of Law & Technology on Worker Surveillance and AI (Feb. 8, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Jolt-2-8-24-final.pdf.

¹¹ See, e.g., Nicole Ozer & Jay Stanley, *Diners Beware: That Meal May Cost You Your Privacy and Security*, ACLU (July 27, 2021), <https://www.aclu.org/news/privacy-technology/diners-beware-that-meal-may-cost-you-your-privacy-and-security>.

¹² See, e.g., Emily Baker-White, *Nothing Sacred: These Apps Reserve The Right To Sell Your Prayers*, BuzzFeed (Jan. 25, 2022), <https://www.buzzfeednews.com/article/emilybakerwhite/apps-selling-your-prayers>; Press Release, Fed. Trade Comm'n, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other> [hereinafter *FTC Sues Kochava*].

¹³ See, e.g., *Student Privacy*, EPIC (2023), <https://epic.org/issues/data-protection/student-privacy/>; Lesley Fair, *FTC to Ed Tech: Protecting kids' privacy is your responsibility*, Fed. Trade Comm'n: Bus. Blog (May 19, 2022), <https://www.ftc.gov/business-guidance/blog/2022/05/ftc-ed-tech-protecting-kids-privacy-your-responsibility>; Press Release, Fed. Trade Comm'n, *FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts* (May 22, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising>.

¹⁴ See, e.g., *Social Media Privacy*, EPIC (2023), <https://epic.org/issues/data-protection/student-privacy/>; Press Release, Fed. Trade Comm'n, *FTC Investigation Leads to Lawsuit Against TikTok and ByteDance for Flagrantly Violating Children's Privacy Law* (Aug. 2, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law>.

¹⁵ *Disrupting Data Abuse*, *supra* note 7, at 34–41; see also Press Release, Fed Trade Comm'n, *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>.

¹⁶ See, e.g., *Health Privacy*, EPIC (2024), <https://epic.org/issues/data-protection/health-privacy/>; Elisa Jillson, *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, Fed. Trade Comm'n: Bus. Blog (July 25, 2023), <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases>.

plan our families,¹⁷ raise our children,¹⁸ exercise our political freedoms,¹⁹ or simply move about the world.²⁰ Data-driven risks to consumers have only grown as businesses have dramatically increased their reliance on opaque, unaccountable, and often discriminatory automated decision-making systems to screen, score, and sort us.²¹

Until relatively recently, the U.S. policy response to this personal data free-for-all was dominated by the failed doctrine of “notice and choice.” This unfortunate focus has led to longer and more complicated privacy policies that users do not read and could not change even if they did. And modern surveillance systems, including the schemes used to track our digital and physical activities across the web and across devices, are too complex and opaque for the vast majority of internet users to understand or control. Clear, robust data protection standards are

¹⁷ Sara Geoghegan, *Two Years Post-Dobbs: A Commercial Surveillance Landscape That is Confusing, Complicated, and Harmful to Abortion Seekers*, EPIC (June 25, 2022), <https://epic.org/two-years-post-dobbs-a-commercial-surveillance-landscape-that-is-confusing-complicated-and-harmful-to-abortion-seekers/>; Suzanne Bernstein, *The Role of Digital Privacy in Ensuring Access to Abortion and Reproductive Health Care in Post-Dobbs America*, EPIC (June 13, 2024), <https://epic.org/the-role-of-digital-privacy-in-ensuring-access-to-abortion-and-reproductive-health-care-in-post-dobbs-america/>; Lesley Fair, *FTC says Premom shared users’ highly sensitive reproductive health data: Can it get more personal than that?*, Fed. Trade Comm’n: Bus. Blog (May 17, 2023), <https://www.ftc.gov/business-guidance/blog/2023/05/ftc-says-premom-shared-users-highly-sensitive-reproductive-health-data-can-it-get-more-personal>.

¹⁸ See, e.g., *Children’s Privacy*, EPIC (2023), <https://epic.org/issues/data-protection/childrens-privacy/>; Press Release, Fed. Trade Comm’n, *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://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>.

¹⁹ See, e.g., *Privacy in Public*, EPIC (2024), <https://epic.org/issues/surveillance-oversight/privacy-in-public/>; Zak Doffman, *Black Lives Matter: U.S. Protesters Tracked By Secretive Phone Location Technology*, Forbes (June 26, 2020), <https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-blacklives-matter-protesters/>.

²⁰ See, e.g., *Location Tracking*, EPIC (2024), <https://epic.org/issues/data-protection/location-tracking/>; Press Release, Fed. Trade Comm’n, *FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data* (Jan. 9, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data>.

²¹ See, e.g., *AI & Human Rights*, EPIC (2024), <https://epic.org/issues/ai/>; Press Release, Fed. Trade Comm’n, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards* (Dec. 19, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>.

essential to restore the balance of power between individuals and technology companies and to ensure the preservation of our privacy and civil rights. Yet outside of a small number of subject- and sector-specific statutes, those clear standards have been elusive at the federal level.

II. The data protection missteps of the FTC's past

In the absence of a comprehensive privacy law or dedicated federal privacy regulator, the task of safeguarding personal data in the United States has fallen chiefly to the Federal Trade Commission. The FTC was established in 1914 to prevent unfair methods of competition in commerce.²² In 1938, Congress expanded the Commission's mandate to include a broad prohibition against unfair and deceptive acts or practices, and since then the FTC has been assigned to enforce a variety of consumer protection laws,²³ including several sectoral privacy statutes. Equipped with this toolkit of legal authorities, the Commission is charged with protecting the public from unfair and deceptive business practices and unfair methods of competition.²⁴

Unfortunately, the Commission has often failed to deliver on this charge where privacy and data protection are concerned. Although the FTC has taken notable steps to protect consumer privacy over the past two decades, the Commission's enforcement and regulatory strategies have too often failed to meet the moment, and the Commission has too often neglected to use the full authority Congress has given it. The FTC's repeated failure to take effective enforcement action and to block harmful mergers has allowed abusive data practices by Facebook, Google, and other

²² *About the FTC*, Fed. Trade Comm'n, <https://www.ftc.gov/about-ftc> (last visited Sept. 17, 2024).

²³ *Id.*

²⁴ *Id.*

industry giants to flourish.²⁵ Some statutory authorities—including the FTC’s power to promulgate industry-wide trade rules—have simply never been used before to advance the Commission’s data protection mission.

To its credit, the FTC recognized from an early stage that the collection, use, and retention of personal data by businesses posed a risk of harm to consumers. As early as 1951 and running through a “series of cases in the 1970s, [the Commission] recognized the general consumer preference against commercialization of personal data.”²⁶ In the mid-1990s, the Commission took an interest in the emerging issue of online privacy and held a series of workshops that led, in part, to the passage of the Children’s Online Privacy Protection Act (COPPA); the issuance of reports critical of the data practices of early internet companies; and calls for additional regulatory authority. In 1998, the Commission brought its first internet-related privacy case.²⁷

But despite this promising start, the Commission’s early data protection work led to a framing of privacy law in the United States as a matter of “notice and choice” and deference to industry-backed “self-regulation.”²⁸ Both notice and choice and self-regulation have failed to meaningfully protect consumer privacy online. Notice and choice mechanisms are particularly ineffective, as the services most consumers rely on in their daily lives are interlinked with

²⁵ See, e.g., Facebook: Transparency and Use of Consumer Data: Hearing before the H. Comm. on Energy & Com., 115th Cong. (2018) (testimony of EPIC), <https://archive.epic.org/testimony/congress/EPIC-HEC-Facebook-Apr2018.pdf>.

²⁶ Chris Jay Hoofnagle et al., *The FTC Can Rise to the Privacy Challenge, but Not Without Help From Congress*, Lawfare (Aug. 9, 2019), <https://www.lawfareblog.com/ftc-can-rise-privacy-challenge-notwithout-help-congress>.

²⁷ *In re GeoCities*, FTC File No. 982-3015 (1998).

²⁸ See Consumer Reps. & EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking 1* (2022), <https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/>.

surveillance platforms and third-party data brokers. “When monitoring is built into services and presented as necessary for the provision of the service, it constrains the relevance and utility of the notice-and-choice regime.”²⁹ Moreover, notice and choice completely fails to address the threat from data brokers and other third parties that have no direct interaction with the consumer.³⁰

Even as the FTC has embraced its role as a regulator of commercial data practices, the Commission’s efforts have often come up short. In the 2000s, the FTC began to expand the scope of its privacy investigations and eventually formed a Division of Privacy and Identity Protection within the Bureau of Consumer Protection. But the Commission’s enforcement actions did not lead to substantial changes in business practices or sufficient monetary penalties, and it became clear that companies under consent decrees would have no incentive to protect consumer data if they did not expect real consequences for violating those decrees. And as EPIC detailed in its 2021 report *What the FTC Could Be Doing (But Isn’t) To Protect Privacy: The FTC’s Unused Authorities*,³¹ the Commission left many regulatory tools on the table for years as the crisis deepened. That trend finally began to reverse over the last few years as the agency took on new enforcement and rulemaking priorities.

III. Data protection and today’s FTC

Today’s hearing asks how the current practices of the FTC differ from those of Commissions past. In EPIC’s view, answering this question requires asking another: are consumers—and in particular, the privacy and personal data of consumers—better protected by

²⁹ Hoofnagle, *supra* note 3, at 333.

³⁰ *Id.* at 173.

³¹ EPIC, *What the FTC Could Be Doing (But Isn’t) To Protect Privacy: The FTC’s Unused Authorities* (June 2021), <https://epic.org/wp-content/uploads/2021/10/EPIC-FTC-Unused-Authorities-Report-June2021.pdf>.

today's FTC than by Commissions past? The answer is a resounding yes. I say this for three reasons in particular.

First, the scope and impact of the Commission's data protection enforcement work has significantly grown under current leadership. Since 2021, the Commission has initiated dozens of enforcement actions against companies engaged in unfair, deceptive, and otherwise unlawful personal data practices.³² The businesses targeted in these actions run the gamut from major brands and household names like Amazon,³³ Facebook,³⁴ Microsoft,³⁵ Twitter,³⁶ TikTok,³⁷

³² *Cases Tagged with Privacy and Security*, Fed. Trade Comm'n, <https://www.ftc.gov/enforcement/cases-proceedings/terms/1420> (last visited Sept. 18, 2024).

³³ Press Release, Fed. Trade Comm'n, *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://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>.

³⁴ Press Release, Fed. Trade Comm'n, *FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data* (May 3, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data>.

³⁵ Press Release, Fed. Trade Comm'n, *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://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information>.

³⁶ Press Release, Fed. Trade Comm'n, *FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads* (May 25, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>.

³⁷ Press Release, Fed. Trade Comm'n, *FTC Investigation Leads to Lawsuit Against TikTok and ByteDance for Flagrantly Violating Children's Privacy Law* (Aug. 2, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law>.

Rite Aid,³⁸ and Epic Games³⁹ to the firms and brokers that form the underbelly of the surveillance economy like Kochava,⁴⁰ InMarket,⁴¹ and X-Mode.⁴²

More than their number, it is the substance of the consent decrees and stipulated orders secured by the FTC that sets the Commission’s recent enforcement work apart. For example, the Commission has made growing use of its Section 5 unfairness authority⁴³ to target and prohibit data practices that are intrinsically unfair to consumers—not just harmful uses of personal data that business fail to disclose.⁴⁴ This includes the FTC’s ongoing case against data broker Kochava, which challenges Kochava’s unfair sale of sensitive location information that can “reveal people’s visits to reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities.”⁴⁵ Other unfair practices targeted by the

³⁸ Press Release, Fed. Trade Comm’n, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards (Dec. 19, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>.

³⁹ Press Release, Fed. Trade Comm’n, 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>.

⁴⁰ *FTC Sues Kochava*, *supra* note 12.

⁴¹ Press Release, Fed. Trade Comm’n, 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>.

⁴² Press Release, Fed. Trade Comm’n, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data>.

⁴³ 15 U.S.C. § 45(a)(1).

⁴⁴ See Lina M. Khan, Chair, FTC, Remarks of Chair Lina M. Khan As Prepared for Delivery at the IAPP Global Privacy Summit 2022 (Apr. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf (“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.”).

⁴⁵ *FTC Sues Kochava*, *supra* note 12.

Commission include Amazon’s indefinite retention of recordings of children’s voices,⁴⁶ Epic Games’ enabling of on-by-default chat features for children and teens,⁴⁷ and GoodRx’s failure to maintain sufficient policies to protect its users’ health data.⁴⁸ Brick by brick, the FTC has used these unfairness enforcement actions to build a foundation of substantive privacy protections, putting businesses on notice that they cannot escape accountability for harmful data practices simply by burying a disclosure in a privacy policy.

The FTC has also begun to make more effective use of its sector-specific data protection authorities. In its enforcement actions against GoodRx⁴⁹ and ovulation tracking app Premom,⁵⁰ the Commission used the Health Breach Notification Rule to target both businesses’ unlawful disclosure of sensitive health data to third parties without notice to consumers. In cases against

⁴⁶ Press Release, Fed. Trade Comm’n, 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://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>.

⁴⁷ Press Release, Fed. Trade Comm’n, 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>.

⁴⁸ Press Release, Fed. Trade Comm’n, FTC Enforcement Action to Bar GoodRx from Sharing Consumers’ Sensitive Health Info for Advertising (Feb. 1, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>.

⁴⁹ Press Release, Fed. Trade Comm’n, FTC Enforcement Action to Bar GoodRx from Sharing Consumers’ Sensitive Health Info for Advertising (Feb. 1, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>.

⁵⁰ Press Release, Fed. Trade Comm’n, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>.

Epic Games,⁵¹ Amazon,⁵² Edmodo,⁵³ and Microsoft,⁵⁴ the Commission breathed new life into COPPA, reinforcing privacy protections for children online, at school, and at home. And in its latest enforcement action against Meta, the Commission seeks to use its longstanding authority to revise consent decrees based on changed facts to ban Meta from monetizing the data of minors⁵⁵—a step made necessary by Meta’s repeated failure to adhere to multiple FTC consent decrees.⁵⁶

As the preceding cases reflect, today’s FTC has focused much of its enforcement work on two particularly urgent categories of cases: those implicating sensitive personal data, and those that involve an acute risk of harm to marginalized populations. Given the special risks that attach to the use and disclosure of health, location, and children’s data, it is encouraging to see the Commission concentrate on cases implicating these sensitive data types. And the necessity of committing enforcement resources to protecting marginalized populations is evident from the

⁵¹ Press Release, Fed. Trade Comm’n, 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/fornite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations>.

⁵² Press Release, Fed. Trade Comm’n, 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://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>.

⁵³ Press Release, Fed. Trade Comm’n, FTC Says Ed Tech Provider Edmodo Unlawfully Used Children’s Personal Information for Advertising and Outsourced Compliance to School Districts (May 22, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising>.

⁵⁴ Press Release, Fed. Trade Comm’n, 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://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information>.

⁵⁵ Press Release, Fed. Trade Comm’n, FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data (May 3, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data>.

⁵⁶ See *Meta Launches Kitchen Sink Constitutional Attack on FTC to Evade New Privacy Limits*, EPIC (Nov. 30, 2023), <https://epic.org/meta-launches-kitchen-sink-constitutional-attack-on-ftc-to-evade-new-privacy-limits/>.

Commission’s recent case against Rite Aid, which targeted the pharmacy chain’s use of unproven facial recognition technology to identify potential shoplifters.⁵⁷ The FTC’s complaint revealed that Rite Aid’s failure to ensure the accuracy of its AI-powered facial recognition system led to alarming rates of false positives, particularly for women and people of color.⁵⁸

EPIC is also encouraged by the FTC’s recent incorporation of forward-thinking remedies in its settlements with offending businesses. These include the disgorgement of ill-gotten personal data and algorithms,⁵⁹ rigorous data minimization obligations,⁶⁰ and remedies applied to individual corporate officers who have engaged in unlawful data practices.⁶¹ More than ever, the Commission is ensuring that its consent decrees and stipulated orders actually prevent future instances of data-driven harms to consumers—not just creating additional paperwork burdens or imposing new costs of doing business.

Second, the Commission has shown a new willingness to establish clear and enforceable data protection standards using its rulemaking authority. Though much of the FTC’s impact on privacy and data protection has historically come through case-by-case enforcement, Congress has also entrusted the FTC with significant rulemaking authority. Just in

⁵⁷ Press Release, Fed. Trade Comm’n, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards (Dec. 19, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>.

⁵⁸ *See id.*

⁵⁹ *See, e.g., FTC Finds Amazon Ring Cameras Responsible for “Egregious Violations of Users’ Privacy,” Requires Data Deletion*, EPIC (May 31, 2023), <https://epic.org/ftc-finds-amazon-ring-cameras-egregious-violations-of-users-privacy-requires-data-deletion/>.

⁶⁰ *See, e.g., EPIC Commends FTC for Including Data Minimization & Data Rights in Chegg Settlement*, EPIC (Dec. 14, 2022), <https://epic.org/epic-commends-ftc-for-including-data-minimization-data-rights-in-chegg-settlement/>.

⁶¹ *See* Press Release, Fed. Trade Comm’n, FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers (Oct. 24, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million>.

the past year, the Commission has amended the Safeguards Rule to require non-bank financial institutions to report data security breaches,⁶² updated the Health Breach Notification Rule to clarify its application to health apps,⁶³ and proposed major changes to the COPPA rule to place strict new limits on targeted advertising to children and the monetization of children’s personal data.⁶⁴

But the most significant data protection rulemaking undertaken by the FTC is the Trade Regulation Rule on Commercial Surveillance and Data Security, first announced in an August 2022 advanced notice of proposed rulemaking (ANPRM).⁶⁵ Although the Commission has not yet published proposed rule text, the ANPRM indicates that the rulemaking could yield data minimization and data security mandates, heightened protections for the data of minors, accuracy and testing requirements for AI and automated decision-making systems, civil rights protections, and prohibitions on deceptive design practices. As EPIC wrote in its extensive comments on the rulemaking (*Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*), “EPIC, alongside other consumer protection and civil rights organizations, has previously urged the Commission to undertake a trade regulation rulemaking that would

⁶² Press Release, Fed. Trade Comm’n, *FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches* (Oct. 27, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches>.

⁶³ Press Release, Fed. Trade Comm’n, *FTC Finalizes Changes to the Health Breach Notification Rule*, (Apr. 26, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule>.

⁶⁴ Press Release, Fed. Trade Comm’n, *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>.

⁶⁵ See Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022) (to be codified at 16 C.F.R. ch. 1), <https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security>.

define unfair and deceptive commercial data practices and unlock the FTC’s dormant enforcement power. EPIC is heartened to see the Commission considering such a rule now, and we are eager to work with the FTC to ensure that this process yields the strongest possible privacy and civil rights protections for consumers.”⁶⁶

Third, the Commission has deepened its technological expertise and engagement with the public. In 2023, the Commission established the Office of Technology, a reflection of the FTC’s commitment to better understanding the types of data-driven and algorithmic systems at the root of its enforcement actions and rulemakings. Although the FTC has long employed technologists to assist in its work, the formation of the Office has crystallized that role and allowed the FTC to produce a steady stream of public- and business-facing technical guidance on topics like surveillance pricing,⁶⁷ open-weights AI models,⁶⁸ personal data processing by vehicles,⁶⁹ data aggregators,⁷⁰ and privacy-enhancing technologies.⁷¹ The Commission has also made better use of its 6(b) authority⁷² to conduct wide-ranging studies of commercial

⁶⁶ *Disrupting Data Abuse*, *supra* note 7, at 6.

⁶⁷ FTC Staff, *Behind the FTC’s Inquiry into Surveillance Pricing Practices*, FTC Tech. Blog (July 23, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/behind-ftcs-inquiry-surveillance-pricing-practices>.

⁶⁸ Staff in the Off. Tech., *On Open-Weights Foundation Models*, FTC Tech. Blog (July 10, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/open-weights-foundation-models>.

⁶⁹ Staff in the Off. Tech. & Div. Priv. & Identity Prot., *Cars & Consumer Data: On Unlawful Collection & Use*, FTC Tech. Blog (May 14, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use>.

⁷⁰ *FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket*, FTC Tech. Blog (Mar. 4, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket>.

⁷¹ Simon Fondrie-Teitler, *Keeping Your Privacy Enhancing Technology (PET) Promises*, FTC Tech. Blog (Feb. 1, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/keeping-your-privacy-enhancing-technology-pet-promises>.

⁷² 15 U.S.C. § 46(b).

surveillance technologies and business practices, as in the study on social media and video streaming platforms due to be released today.⁷³

Moreover, the FTC has strengthened its public engagement by holding regular open Commission meetings.⁷⁴ These meetings have offered individuals and businesses a clearer window into the Commission's work, as well as an opportunity for consumers to speak directly to commissioners themselves about the struggles and dubious business practices—data-driven or otherwise—that they face each day. These meetings are supplemented by the steady drumbeat of business guidance and analysis of key matters before the Commission offered through channels such as the FTC's Business Blog.⁷⁵

In highlighting these refinements to the FTC's privacy and data protection work, I do not mean to discount the efforts of prior Commissions in bringing us to this point. The regulatory shifts identified above build on the past efforts of FTC commissioners and civil servants who have taken up the charge of data protection in the online era. Nor do I mean to suggest that today's FTC has perfected the art of regulating commercial data practices. EPIC, our peers in civil society, members of this Committee, and the Commission itself recognize that we are a long way from defusing the data protection crisis and realizing the promise of a privacy- and rights-respecting future.

⁷³ Press Release, Fed. Trade Comm'n, *FTC Announces Tentative Agenda for September 19 Open Commission Meeting* (Sept. 12, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-tentative-agenda-september-19-open-commission-meeting>.

⁷⁴ Open Meetings, Fed. Trade Comm'n, <https://www.ftc.gov/news-events/events/open-meetings> (last visited Sept. 18, 2024).

⁷⁵ Business Blog Archive, Fed. Trade Comm'n, <https://www.ftc.gov/business-guidance/blog/archive> (last visited Sept. 18, 2024).

But EPIC believes the combination of steady, strategic, and effective enforcement actions; the expanded use of rulemaking to safeguard privacy and civil rights; and the Commission’s heightened commitment to understanding the consumers harms, technologies, and business practices at the heart of its work have substantially elevated the Commission’s data protection efforts and left consumers better off in the process. Between the FTC practices of the past and those of the present, we choose the present without hesitation.

IV. Misplaced critiques of the FTC’s data protection efforts

Despite the material improvements in the scope, ambition, and efficacy of the Commission’s data protection work, several criticisms of that work have been raised that merit a brief response.

First, some have charged that the FTC’s data and consumer protection work has become too partisan under current leadership. This argument misses the mark in at least three ways. First, many of the most consequential actions the Commission has taken to protect consumer privacy and civil rights in recent years have earned bipartisan support—from Commission’s case against data broker Kochava⁷⁶ to its enforcement actions over children’s privacy violations by Epic

⁷⁶ *FTC Sues Kochava*, *supra* note 12. (“The Commission vote authorizing the staff to file the complaint against Kochava was 4-1.”).

Games⁷⁷ and Amazon⁷⁸ to its recent initiation of a 6(b) study into surveillance pricing⁷⁹ and its case against an Arizona car dealership over discriminatory pricing.⁸⁰ Second, while bipartisan cooperation is alive and well at the FTC, some disagreement between commissioners—partisan or otherwise—is nothing new. Past Commissions have divided sharply on major privacy actions, including notably the FTC’s 2019 settlements with Facebook⁸¹ and Google.⁸² Finally, although bipartisan consensus is a worthy goal and can strengthen the FTC’s enforcement and regulatory undertakings, it is not (and should not be) the Commission’s primary objective. Congress’s charge to the FTC is to protect consumers, not to pursue political unanimity at all costs. Indeed,

⁷⁷ Press Release, Fed. Trade Comm’n, *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> (“The Commission voted 4-0 to issue the proposed administrative complaint and to accept the consent agreement with Epic related to its deceptive billing practices.”).

⁷⁸ Press Release, Fed. Trade Comm’n, *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://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever> (“The Commission voted 4-0 to refer the complaint to the Department of Justice for filing.”).

⁷⁹ Press Release, Fed. Trade Comm’n, *FTC Issues Orders to Eight Companies Seeking Information on Surveillance Pricing* (July 23, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-issues-orders-eight-companies-seeking-information-surveillance-pricing> (“The Commission voted 5-0 to issue the 6(b) orders to the eight companies.”).

⁸⁰ Press Release, Fed. Trade Comm’n, *FTC, State of Arizona Take Action Against Coulter Motor Company ofr Deceptive Pricing and Discriminatory Practices*, (Aug. 15, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-state-arizona-take-action-against-coulter-motor-company-deceptive-pricing-discriminatory> (“The Commission vote authorizing the staff to file the complaint and stipulated final order was 5-0.”).

⁸¹ Press Release, Fed. Trade Comm’n, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook> (“The Commission vote to refer the complaint and stipulated final order to the Department of Justice for filing was 3-2.”).

⁸² Press Release, Fed. Trade Comm’n, *Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law* (Sept. 4, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law> (“The Commission voted 3-2 to authorize the complaint and stipulated final order to be filed.”).

disagreement is a feature, not a flaw, of a Commission designed to reflect a variety of perspectives.⁸³

Second, some have argued that the data protection rulemakings undertaken by today's FTC—in particular, the anticipated Trade Regulation Rule on Commercial Surveillance and Data Security—are an encroachment on Congressional authority. This, too, misses the mark. There is of course widespread agreement that a robust, comprehensive privacy law enacted by Congress and backed by meaningful enforcement resources would be the best policy tool to solve the data protection crisis we face. EPIC and the members of the Commission continue to support this Committee's bipartisan efforts to pass such legislation. However, until Congress enacts a comprehensive privacy law, it is the obligation of the FTC to use every existing tool at its disposal to protect consumers from harmful commercial data practices, up to and including trade rulemaking authority. It is well within the Commission's section 18 power to take aim at prevalent data practices causing harm to consumers and to set rules of the road to prevent further injury to consumers.⁸⁴

Finally, some have objected that the FTC's more muscular data protection work of recent vintage represents an abuse of power. But this view miscasts efficacy as overreach, ignores the Commission's long history of forward-thinking regulatory approaches, and overlooks the significant substantive, procedural, and resource limitations that constrain the FTC's authority. Indeed, not long ago the FTC lost one of its most valuable statutory powers:⁸⁵ its ability under

⁸³ See 15 U.S.C. § 41 (“A commission is created and established, to be known as the Federal Trade Commission (hereinafter referred to as the Commission), which shall be composed of five Commissioners, who shall be appointed by the President, by and with the advice and consent of the Senate. Not more than three of the Commissioners shall be members of the same political party.”).

⁸⁴ See 15 U.S.C. § 57a.

⁸⁵ See *AMG Cap. Mgmt., LLC v. Fed. Trade Comm'n*, 141 S. Ct. 1341, 1344 (2021).

section 13(b)⁸⁶ to secure equitable monetary relief on behalf of consumers early in the progression of a case. EPIC urges the Committee to move forward legislation restoring that 13(b) power again this session,⁸⁷ and we urge Congress to provide the FTC with the resources necessary to carry out the task of establishing strong data protection standards throughout the U.S. economy.

V. Conclusion

Addressing the data protection crisis and reining in abusive commercial data practices is an enormous undertaking for any regulator, and one that remains very much a work in progress at the FTC. But given the Commission’s encouraging track record of enforcement, rulemaking, and consumer engagement in recent years, EPIC is more optimistic than ever about the FTC’s ability to carry out that charge.

Thank you for the opportunity to testify today.

⁸⁶ Fed. Trade Comm’n Act § 13(b), Pub. L. No. 93-153 (codified at 15 U.S.C. § 53(b)).

⁸⁷ See Protecting America’s Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Commerce, 117th Cong. (2022) (testimony of Caitriona Fitzgerald, Deputy Director, EPIC), <https://epic.org/documents/hearing-on-protecting-americas-consumers-bipartisan-legislation-to-strengthen-data-privacy-and-security/> (“Enabling the Commission to seek civil penalties against first-time violators will be a powerful deterrent against exploitative data practices and a key tool for holding lawbreaking companies accountable.”).