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

Office of the Director
Bureau of Consumer Protection

I'll start by describing what makes the FTC a truly special agency, one that's uniquely suited to taking on contemporary privacy challenges. I'll then talk about how under the leadership of Chair Lina Khan, we are pressing those advantages to deliver stronger privacy protections for the American public.

I. Institutional advantages

The FTC is unique. We are more than a century old, yet our core authority and mission have hardly changed – to protect fair markets by combatting unfair methods of competition and unfair or deceptive practices.

Our remit is broad, covering both antitrust and consumer protection. And our consumer protection mission alone covers almost the entire economy. But when it comes to protecting consumers' privacy, I consider our expertise across markets to be a feature, not a bug.

For example, fraud has been a mainstay of the FTC's enforcement program for decades. But today, we are increasingly seeing fraudulent actors exploit consumers' data as an additional source of revenue, a conduct we are uniquely suited to spot and stop.[3] Likewise, last year we issued a report on how companies are deploying dark patterns to manipulate consumers through sophisticated design techniques,[4] a trend we are seeing both in our financial enforcement[5] work and our privacy work.[6]

The fact that our agency also has a competition mission further enhances our work. For example, we recently issued a Request for Information seeking comment about cloud computing business practices from both a competition and consumer protection perspective, with questions on issues including firms' reliance on a small number of service providers, and how the responsibility for those risks is shared between cloud customers and cloud service providers.[7] The FTC's recently

---

[3] See, e.g., Press Release, FTC Halts Operation That Unlawfully Shared and Sold Consumers' Sensitive Data, (July 5, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/07/ftc-halts-operation-unlawfully-shared-sold-consumers-sensitive-data (holding lead generator Blue Global LLC liable for tricking millions of consumers into filling out "loan applications," then selling info collected to very few lenders, and instead to anyone willing to pay for it).

[4] FTC, BRINGING DARK PATTERNS TO LIGHT (2021).

[5] In re: Credit Karma, LLC, No. C-4781, (FTC Jan. 23, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/2023138-credit-karma-combined-final-consent-without-signatures.pdf (final decision and order settling claims that Credit Karma misrepresented consumers were "approved" for credit cards).

[6] Our recent orders against GoodRx and BetterHelp include bans on the use of dark patterns to obtain consumer consent. US v. GoodRx Holdings Inc., 23-cv-460, (ND. Cal. 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_stipulated_order_for_permanent_injunction_civil_penalty_judgment_and_other_relief.pdf (first-of-its-kind settlement against telehealth & prescription drug discount provider for unauthorized disclosure of sensitive, personal health info to advertising companies & platforms including Facebook & Google); In re BetterHelp, Inc., No. C-XXXX, (FTC Mar. 2, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/202_3169_betterhelp_consent.pdf (settling claims that online counseling service shared consumers' sensitive health data, including mental health info, with third parties such as Facebook & Snapchat for advertising purposes & without authorization).

[7] Press Release, FTC Explores Rules Cracking Down on Commercial Surveillance & 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.

formed Office of Technology, which I will talk about more later, is leading this project with involvement from lawyers and economists throughout the agency.

The FTC also has a set of tools that are unique in the federal government. We are a vigorous law enforcer, and have been rightly called "the greatest public interest law firm in the country."[8] We have authority to write rules outlawing unfair methods of competition, and recently proposed a ban on noncompete agreements.

It should be apparent that rulemaking is a key plank of our overall strategy. But I want to draw your attention to our recent enforcement actions in this space. As I mentioned earlier, there is widespread agreement that the notice-and-choice regime is failing the public. The actions we've filed over the last eighteen months demonstrate significant progress in moving the market in another direction, one with actual restrictions on how consumer information is handled.

A. Restricting What Companies Can Collect and Retain

First, our actions are making clear that companies should be collecting less consumer data and deleting more. For nearly two decades, the FTC's orders have required firms to exercise greater care in handling data they've collected from consumers. But over the last two years, the FTC is going further – requiring companies to collect less data in the first place. In five actions[23] since 2021, we've secured requirements that firms minimize the data they collect and retain it no longer than is reasonably necessary. And notably, we are securing these remedies not only in our privacy actions[24] but also in our data security actions.[25] This stems from our recognition that data that isn't collected can't be compromised.

B. Limiting the Sharing of Sensitive Data

In addition to restricting collection and retention, our recent actions also demonstrate the Commission's commitment to sharply limiting the sharing of consumers' sensitive data. For example, we recently charged GoodRx[26] with sharing consumers' medication data without their authorization. The order we secured did not require GoodRx to obtain consumer consent before sharing their data to fuel advertising. Rather, it banned the practice altogether.[27] That remedy we

[23] In re Drizly, LLC, Case No. C-4780 (FTC Jan. 10, 2023), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/2023185-drizly-llc-matter (final decision & order); In re Chegg, Inc., Case No. C-4782 (FTC Jan. 26, 2023), available at https://www.ftc.gov/legal-

consumers' sensitive data.[34] We were not bluffing. Earlier this year, we brought our first action ever enforcing the Rule. It will not be our last.[35]

We also continue to enforce one of the nation's first data protection laws, the Fair Credit Reporting Act. Last year, for example, we obtained an order against a data aggregator limiting how the firm could handle consumer data and requiring it to pay a civil penalty.[36] And we recently announced a Request for Information with the Consumer Financial Protection Bureau around background screening in the rental market, which can implicate both the FCRA and the FTC Act.[37]

D. Ensuring Accountability for Violators

The last point I want to make about our enforcement actions is that the marketplace should be paying attention. We are making clear that firms will face serious consequences for breaking the law.

First, in spite of the Supreme Court having taken away the agency's strongest tool to disgorge profits and recover funds for consumers,[38] we are breaking new ground when it comes to securing monetary relief in privacy actions. Over the last six months, we have obtained the largest COPPA penalty ever,[39] the first civil penalty for a violation of the HBNR,[40] and the first redress judgment for health privacy violations.[41] Going forward, we are considering steps to further ensure that companies pay a price for violations. For example, if we undertake a rulemaking in this area, it would trigger stiff civil penalties of up to $50,120 per violation.[42]

---

[34] FTC Policy Statement on Breaches by Health Apps & Other Connected Devices (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

[35] US v. GoodRx Holdings Inc., 23-cv-460, (N.D. Cal. 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_stipulated_order_for_permanent_injunction_civil_penalty_judgment_and_other_relief.pdf

[36] FTC v. ITMedia Sols. LLC, 2:22-cv-00073 DSF (C.D. Cal. Jan. 10, 2022), available at https://www.ftc.gov/system/files/documents/cases/ftc_v_itmedia_-_doc_840561_-_stipulated_order_for_permanent_injunction.pdf (stip. order §§ II, V).

[37] Press Release, FTC and CFPB Seek Public Comment on How Background Screening May Shut Renters out of Housing (Feb. 28, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-cfpb-seek-public-comment-how-background-screening-may-shut-renters-out-housing. Separately, the CFPB recently announced a Request for Information concerning the business practices of data brokers, and whether the FCRA might be implicated. Press Release, CFPB Launches Inquiry into the Business Practices of Data Brokers (Mar. 15, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/

[38] AMG Capital Mgmt., LLC v. FTC, 141 S.Ct. 1341 (2021).

[39] US v. Epic Games, Inc., 5:22-CV-00518-

Monetary relief is not the only consequence companies can face for violating the law. We are also requiring companies to delete ill-gotten data, and to alert other firms if they are in receipt of the same. In some instances, we are requiring firms to not only delete ill-gotten data but also delete any algorithmic work product trained on such data.[43] One remedy we recently obtained – for the first time ever – against a company charged with violating COPPA.

Finally, we know that companies tend to underinvest in data protection, often because the costs of breaches are often borne by customers or third parties.[44] Recognizing this, we are making sure that key decisionmakers are being held accountable for privacy and data security failures. For example, our data security action against Drizly named the company's CEO, and our order binds him for the next decade

short or require close scrutiny.[49] We have also made clear that companies should not be making claims about AI unless they're prepared to back those claims up.[50] And in 2021, we warned that it may violate the FTC Act to use automated tools that have a discriminatory impact,

that allow us to share our decades of experience in enforcement cooperation to inform the development of suitable frameworks for cooperation.[55]

Third, to keep up with emerging trends, staff in DPIP, the Office of Technology, and throughout the agency, meet regularly with technology and privacy researchers in the academic, consumer advocacy, industry, and government sectors. Indeed, two of our premier experts – Joe Calandrino and Olivier Sylvain – are attending this conference.

In addition, we regularly convene public events where experts present their latest research related to data collection and use issues. One important such event is the FTC's annual PrivacyCon, which last year included panels on important topics including ad tech and automated decision-making systems, augment (i)-2 ncnol pcndtc0tih th t e f ao12 (2)3 (s(ugm)-2 .a]k)4 (a)(our)14 de [-22 (

that government oversight long accords consumers have "choices [59] This view aptly