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

Office of the Chair

Statement of Chair Lina M. Khan
Regarding the Commercial Surveillance and Data Security
Advance Notice of Proposed Rulemaking
Commission File No. R111004

August 11, 2022

Today, the Federal Trade Commission initiated a proceeding to examine whether we should implement new rules addressing data practices that are unfair or deceptive.

The Commission brought its first internet privacy case 24 years ago against GeoCities, one of the most popular websites at the time.[1] In the near quarter-century since, digital technologies and online services have rapidly evolved, with transformations in business models, technical capabilities, and social practices. These changes have yielded striking advancements and dazzling conveniences—but also tools that enable entirely new forms of persistent tracking and routinized surveillance. Firms now collect personal data on individuals on a massive scale and in a stunning array of contexts, resulting in an economy that, as one scholar put it, "represents probably the most highly surveilled environment in the history of humanity."[2] This explosion in data collection and retention, meanwhile, has heightened the risks and costs of breaches—with Americans paying the price.[3]

As the country's de facto law enforcer in this domain, the FTC is charged with ensuring that our approach to enforcement and policy keeps pace with these new market realities. The agency has built a wealth of experience in the decades since the *GeoCities* case, applying our century-old tools to new products in order to protect Americans from evolving forms of data

---

[1] Press Release, Fed. Trade Comm'n, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (Aug. 13, 1998), https://www.ftc.gov/news-events/news/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting-personal-information-agencys-first.

[2] NEIL RICHARDS, WHY PRIVACY MATTERS 84 (2021). *See also* OSCAR GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (2021).

[3] *See, e.g.*, Press Release, Fed. Trade Comm'n, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach. *See also* Eamon Javers, *The Extortion Economy: Inside the Shadowy World of Ransomware Payouts*, CNBC (Apr. 6, 2021), https://www.cnbc.com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html; Dan Charles, *The Food Industry May Be Finally Paying Attention To Its Weakness To Cyberattacks*, NPR (July 5, 2021), https://www.npr.org/2021/07/05/1011700976/the-food-industry-may-be-finally-paying-attention-to-its-weakness-to-cyberattack; William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

abuses.[4] Yet the growing digitization of our economy—coupled with business models that can incentivize endless hoovering up of sensitive user data and a vast expansion of how this data is used[5]—means that potentially unlawful practices may be prevalent, with case-by-case enforcement failing to adequately deter lawbreaking or remedy the resulting harms.

Indeed, a significant majority of Americans today feel that they have scant control over the data collected on them and believe the risks of data collection by commercial entities outweigh the benefits.[6] Evidence also suggests that the current configuration of commercial data practices do not actually reveal how much users value privacy or security.[7] For one, the use of dark patterns and other conduct that seeks to manipulate users underscores the limits of treating present market outcomes as reflecting what users desire or value.[8] More fundamentally, users often seem to lack a real set of alternatives and cannot reasonably forego using technologies that are increasingly critical for navigating modern life.[9]

The data practices of today's surveillance economy can create and exacerbate deep asymmetries of information—exacerbating, in turn, imbalances of power. And the expanding contexts in which users' personal data is used—from health care and housing to employment and education—mean that what's at stake with unlawful collection, use, retention, or disclosure is not just one's subjective preference for privacy, but one's access to opportunities in our economy and society, as well as core civil liberties and civil rights.

The fact that current data practices can have such consequential effects heightens both the importance of wielding the full set of tools that Congress has given us, as well as the responsibility we have to do so. In particular, Section 18 of the FTC Act grants us clear authority

---

[4] *See* Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, ___ Fed. Reg. ___ § III(a) [hereinafter "ANPR"]. *See also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

[5] Remarks of Chair Lina M. Khan, IAPP Global Privacy Summit 2022 (Apr. 11, 2022), https://www.ftc.gov/news-events/news/speeches/remarks-chair-lina-m-khan-prepared-delivery-iapp-global-privacy-summit-2022.

[6] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (noting that 81% of Americans believe that they "have very little/no control over the data companies collect" and that "the potential risks of companies collecting data about them outweigh the benefits").

[7] *See, e.g.*, Daniel Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 22-32 (2021).

[8] The FTC recently brought a case against Age of Learning, Inc., an educational subscription service that allegedly utilized dark patterns to scam millions of dollars from families. *See* Stipulated Order for Permanent Injunction and Monetary Judgement, *FTC v. Age of Learning, Inc.*, No. 2:20-cv-7996 (C.D. Cal. Sept. 8, 2020). *See also* Zeynep Tufekci, *The Latest Data Privacy Debacle*, N.Y. TIMES (Jan. 30, 2018), http://www.nytimes.com/2018/01/30/opinion/strava-privacy.html ("Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices.").

[9] Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, HARV. BUS. REV. (Jan. 30, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data (noting that "even if users wanted to negotiate more data agency, they have little leverage. Normally, in well-functioning markets, customers can choose from a range of competing providers. But this is not the case if the service is a widely used digital platform."); *see also* Solove, *supra* note 7, at 29 ("In one survey, 81% of respondents said that they had at least once 'submitted information online when they wished that they did not have to do so.' People often are not afforded much choice or face a choice between two very bad options.").

to issue rules that identify specific business practices that are unlawful by virtue of being "unfair" or "deceptive."[10] Doing so could provide firms with greater clarity about the scope of their legal obligations. It could also strengthen our ability to deter lawbreaking, given that first-time violators of duly promulgated trade regulation rules—unlike most first-time violators of the FTC Act[11]—are subject to civil penalties. This would also help dispense with competitive advantages enjoyed by firms that break the law: all companies would be on the hook for civil penalties for law violations, not just those that are repeat offenders.

Today's action marks the beginning of the rulemaking proceeding. In issuing an Advance Notice of Proposed Rulemaking (ANPR), the Commission is seeking comments from the public on the extent and effects of various commercial surveillance and data security practices, as well as on various approaches to crafting rules to govern these practices and the attendant tradeoffs. Our goal at this stage is to begin building a rich public record to inform whether rulemaking is worthwhile and the form that potential proposed rules should take. Robust public engagement will be critical—particularly for documenting specific harmful business practices and their prevalence, the magnitude and extent of the resulting consumer harm, the efficacy or shortcomings of rules pursued in other jurisdictions, and how to assess which areas are or are not fruitful for FTC rulemaking.

Because Section 18 lays out an extensive series of procedural steps, we will have ample opportunity to review our efforts in light of any new developments. If Congress passes strong federal privacy legislation—as I hope it does—or if there is any other significant change in applicable law, then the Commission would be able to reassess the value-add of this effort and whether continuing it is a sound use of resources. The recent steps taken by lawmakers to advance federal privacy legislation are highly encouraging, and our agency stands ready to continue aiding that process through technical assistance or otherwise sharing our staff's expertise.[12] At minimum, the record we will build through issuing this ANPR and seeking public comment can serve as a resource to policymakers across the board as legislative efforts continue.

The ANPR poses scores of broad and specific questions to help elicit and encourage responses from a diverse range of stakeholders. I look forward to engaging with and learning from the record that we develop on the wide range of issues covered. Highlighted below are a few topics from the ANPR on which I am especially eager for us to build a record:

- Procedural protections versus substantive limits: Growing recognition of the limits of the "notice and consent" framework prompts us to reconsider more generally the adequacy of procedural protections, which tend to create process requirements while sidestepping

[10] 15 U.S.C. § 57a. Commissioner Slaughter's statement cogently lays out why our authority here is unambiguous. *See* Statement of Commissioner Rebecca Kelly Slaughter Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking (Aug. 11, 2022), at 5-6. *See also* Kurt Walters, *Reassessing the Mythology of Magnuson-Moss: A Call to Revive Section 18 Rulemaking at the FTC*, 16 HARV. L. & POL'Y REV. (forthcoming 2022).

[11] 15 U.S.C. §§ 53, 57b, 45(l). The FTC's penalty offense authority also provides a basis for seeking civil penalties from some first-time violators. 15 U.S.C. § 45(m)(1)(B).

[12] Maria Curi, *Landmark Tech Privacy Protection Bill Approved by House Panel*, BLOOMBERG (July 20, 2022), https://news.bloomberglaw.com/privacy-and-data-security/landmark-tech-privacy-protection-bill-approved-by-house-panel.

more fundamental questions about whether certain types of data collection and processing should be permitted in the first place.[13] Are there contexts in which our unfairness authority reaches a greater set of substantive limits on data collection?[14] When might bans and prohibitions on certain data practices be most appropriate?[15]

- Administrability: Information asymmetries between enforcers and market participants can be especially stark in the digital economy. How can we best ensure that any rules that we pursue can be easily and efficiently administered and that these rules do not rest on determinations that we are not well positioned to make or commitments that we are not well positioned to police? How have jurisdictions successfully managed to police obligations such as "data minimization"?[16]

- Business models and incentives: How should we approach business models that are premised on or incentivize persistent tracking and surveillance, especially for products or services that consumers may not be able to reasonably avoid?[17]

- Discrimination based on protected categories: Automated systems used by firms sometimes discriminate based on protected categories—such as race, color, religion, national origin, or sex—including in contexts where this discrimination is unlawful.[18] How should we consider whether new rules should limit or forbid discrimination based on protected categories under our Section 5 unfairness authority?[19]

---

[13] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1693 (2020) ("[D]ata protection regimes seek to permit more ethical surveillance and data processing at the expense of foundational questions about whether that surveillance and processing should be allowed in the first place."); Solove, *supra* note 7, at 29 ("The fact that people trade their privacy for products or services does not mean that these transactions are desirable in their current form… [T]he mere fact that people make a tradeoff doesn't mean that the tradeoff is fair, legitimate, or justifiable. For example, suppose people could trade away food safety regulation in exchange for cheaper food. There would be a price at which some people would accept greater risks of tainted food. The fact that there is such a price doesn't mean that the law should allow the transaction.").

[14] ANPR at § IV(b) Q.21; ANPR at § IV(d) Q.43; ANPR at § IV(d) Q.48.

[15] ANPR at § IV(d) Q.76.

[16] ANPR at § IV(d) Q.49.

[17] ANPR at § IV(a) Q.11.

[18] ANPR at § I nn.38–45. *See also* Fed. Trade Comm 'n, *Serving Communities of Color: A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color*, at 1-3 (Oct. 2021), https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf; Latanya Sweeney, *Discrimination in Online Ad Delivery: Google Ads, Black Names and White Names, Racial Discrimination, and Click Advertising*, 11 QUEUE 10, 29 (Mar. 2013); Muhammad Ali et al., *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes*, 3 PROC. ACM ON HUM.-COMPUTER INTERACTION (2019).

[19] ANPR at § IV(d) Q.65–72. *See* 15 U.S.C. 45(n) ("In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."). *Cf.* Joint Statement of Chair Lina M. Khan and Commissioner Rebecca Kelly Slaughter In the Matter of Napleton Automotive Group (Mar. 31, 2022), https://www.ftc.gov/news-events/news/speeches/joint-statement-chair-lina-m-khan-commissioner-rebecca-kelly-slaughter-matter-napleton-automotive. Other agencies are also examining these practices. *See* Assistant Attorney General Kristen Clark, Keynote Address on AI and Civil Rights for the Department of Commerce's National Telecommunications and Information Administration's Virtual Listening Session (Dec. 14, 2021), https://www.justice.gov/opa/speech/assistant-attorney-general-kristen-clarke-delivers-keynote-ai-and-civil-rights-

- Workplace surveillance: Reports suggest that extensive tracking, collection, and analysis of consumer data in the workplace has expanded exponentially.[20] Are there particular considerations that should govern how we consider whether data abuses in the workplace may be deceptive or unfair?[21]

To facilitate wide-ranging participation, we are seeking to make this process widely accessible. Our staff has published a "frequently asked questions" resource to demystify the rulemaking process and identify opportunities for the public to engage.[22] We will also host a virtual public forum on September 8, where people will be able to provide oral remarks that will be part of the ANPR record.[23]

I am grateful to our agency staff for their work on this ANPR and my colleagues on the Commission for their engagement and input. Protecting Americans from unlawful commercial surveillance and data security practices is critical work, and I look forward to undertaking this effort with both the necessary urgency and rigor.

***

department; Dep't of Lab., Off. of Fed. Contract Compliance Programs, Internet Applicant Recordkeeping Rule, FAQ, https://www.dol.gov/agencies/ofccp/faqs/internet-applicants; Press Release, Equal Emp. Opportunity Comm'n, EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness (Oct. 28, 2021), https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness.

[20] ANPR at § I nn.14–15. *See, e.g.*, Danielle Abril & Drew Harwell*, Keystroke Tracking, Screenshots, and Facial Recognition: The Box May Be Watching Long After the Pandemic Ends*, WASH. POST (Sept. 24, 2021), https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/; Adam Satariano, *How My Boss Monitors Me While I Work From Home*, N.Y. TIMES (May 6, 2020), https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html.

[21] ANPR at §§ I, IV(a) Q.12.

[22] The FAQ can be found both in English, available at https://www.ftc.gov/enforcement/rulemaking/public-participation-section-18-rulemaking-process, as well as in Spanish, available at https://www.ftc.gov/es/participacion-publica-en-el-proceso-de-reglamentacion-de-la-ftc-conforme-la-seccion-18.

[23] The public forum will include a brief presentation on the rulemaking process and this ANPR comment period, panel discussions, and a public remarks section. More information can be found at https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum.