



Comments of

TechFreedom

Berin Szóka,ⁱ Bilal Sayyed,ⁱⁱ & Andy Jungⁱⁱⁱ

In the Matter of

Trade Regulation Rule on Commercial Surveillance and Data Security

DOCKET ID: FTC-2022-17752

September 15, 2022

ⁱ Berin Szóka is President of TechFreedom, a nonprofit, nonpartisan technology policy think tank. He can be reached at bszoka@techfreedom.org.

ⁱⁱ Bilal Sayyed is Senior Competition Counsel at TechFreedom. He can be reached at bsayyed@techfreedom.org.

ⁱⁱⁱ Andy Jung is a Legal Fellow at TechFreedom. He can be reached at ajung@techfreedom.org.

I. Introduction

On September 8, 2022, three of TechFreedom’s policy experts delivered remarks at the FTC’s Commercial Surveillance and Data Security Public Forum, held to discuss the Commission’s Advanced Notice of Proposed Rulemaking (ANPR) on commercial surveillance and data security practices.¹ Their oral remarks are presented here, lightly edited for clarity.

II. Comments of Berin Szóka

I’m Berin Szóka, President of TechFreedom, a think tank dedicated to Internet law.

The Federal Trade Commission has uniquely broad powers over nearly the entire economy—especially the power to decide what is “fair.”² In the 1970s, the FTC’s conception of unfairness had practically no limits.³

By 1980, the FTC was becoming an unelected second national legislature. Huge bipartisan supermajorities in Congress imposed procedural safeguards to ensure that unfairness and deception rulemakings focused on clear problems with no effective alternative to regulation.⁴

That’s why past Advanced Notices of Proposed Rulemaking focused on *discrete* issues, such as impersonating government agents, negative option marketing, and clothing washing labels.⁵ By contrast, this ANPR is as broad as is the concept of “privacy” itself.⁶

¹ Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022).

² 15 U.S.C. § 45(a)(1) (“Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful”).

³ J. Howard Beales III, *The Federal Trade Commission’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 JOURNAL OF PUB. POL’Y & MARKETING 192 (2003).

⁴ Federal Trade Commission Improvements Act of 1980, Pub. L. No. 98-620 (1984).

⁵ Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Impersonation of Government and Businesses, 86 Fed. Reg. 72901 (Dec. 23, 2021); Advanced Notice of Proposed Rulemaking, Rule Concerning the Use of Prenotification Negative Option Plans, 84 Fed. Reg. 52393 (Oct. 2, 2019); Supplemental Notice of Proposed Rulemaking, Trade Regulation Rule on Care Labeling of Textile Wearing Apparel and Certain Piece Goods, 85 Fed. Reg. 44485 (Sept. 21, 2020).

⁶ Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022). *See also Dissenting Statement of Commissioner Phillips Regarding the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking* (Aug. 11, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/dissenting-statement-commissioner-phillips-regarding-commercial-surveillance-data-security-advance> (“The areas of inquiry are vast and amorphous, and the objectives and regulatory alternatives are just not there. It is impossible to discern from this sprawling document—which meanders in and out of the jurisdiction of the FTC and goes far afield from traditional data privacy and security—the number and scope of rules the Commission envisions.”).

Past ANPRs identified administrative orders or court decisions establishing the unfairness or deceptiveness of specific practices.⁷ This ANPR cites only complaints, settlements, and news reports across a wide range of data practices.⁸ Any proposed rule *must* describe, with “particularity,” why the Commission has “reason to believe” that specific practices are unfair or deceptive.⁹ And any final rule *must* explain why proscribed practices actually violate the FTC Act.

An unfair practice must “cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”¹⁰ Some data practices *do* cross that line. But the Commission must prove its case regarding each practice it seeks to regulate by rule—just as in any enforcement action.¹¹ The Commission must also establish the *prevalence* of any practice subject to a rule.¹² If case-by-case enforcement has already effectively deterred harmful practices, they won’t be “widespread” enough to justify a rule.

To ensure that its rules survive judicial review, the Commission must do what it’s done in every past Magnusson-Moss rulemaking: focus on discrete, egregious practices that clearly harm or deceive consumers. It should continue to police hard privacy questions case by case. But it should leave *major* questions around privacy to the elected representatives of the American people.¹³

⁷ See, e.g., 86 Fed. Reg. 72901 § II(A) (Dec. 23, 2021).

⁸ 87 Fed. Reg. 51273 § I n.11 (Aug. 21, 2022).

⁹ 15 U.S.C. § 45(b)(1); 16 C.F.R. B § 1.11 (a)(3) (2003).

¹⁰ 15 U.S.C. § 45(n).

¹¹ “The Commission may prescribe... rules which define *with specificity* acts or practices which are unfair or deceptive acts or practices” 15 U.S.C. § 57a(a)(1)(B) (emphasis added). “Because the prohibitions of section 5 of the Act are quite broad, trade regulation rules are needed to define with specificity conduct that violates the statute and to establish requirements to prevent unlawful conduct.” See *Katharine Gibbs Sch. (Inc.) v. FTC*, 612 F.2d 658, 662 (2d Cir. 1979) (vacating FTC rule for not defining unfair acts with specificity) (quoting Conf.Rep. No. 93-1408, Joint Explanatory Statement of the Committee of Conference, *reprinted in* [1974] U.S.Code Cong. Ad.News, pp. 7702, 7755, 7763.). Mag-Moss rulemaking and case-by-case enforcement actions involving unfairness are equally subject to 15 U.S.C. § 45(n): “The Commission shall have no authority under this section or section 57a of this title [Section 18 of the FTC Act] to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”

¹² 15 U.S.C. § 45(b)(3); 16 C.F.R. B § 1.14 (a)(1)(i).

¹³ See *West Virginia v. EPA*, 597 U.S. ___, 2022 WL 2347278 (June 30, 2022).

III. Comments of Bilal Sayyed

Timely and stable guidance with respect to privacy and the collection, use, and security of data is necessary. But the scope of the ANPR and the 3–2 vote on its release indicate that the Commission has embarked on a path with little likelihood of providing this guidance in a timely manner or in a manner that withstands changes in Commission makeup and leadership.¹⁴ The Commission should rethink its approach.

It would be far better for the Commission to provide a policy statement on privacy and data, or, alternatively, a statement that identifies with specificity how the principles in the Statements on Deception and Unfairness will be applied in such matters.¹⁵

A policy statement will provide substantial guidance to attorneys, privacy officers and the many firms likely to conform their behavior to the principles underlying the statement, and to Congress.

Consumers benefit when Commission guidance is grounded in core principles of consumer protection, support for vigorous competition, cost-benefit considerations, materiality of harm, and robust economic analysis. Thus, a statement should reflect the principles of consumer welfare, reasonableness, countervailing benefits, and economic analysis that are reflected in the Deception and Unfairness Statements and the FTC Act.¹⁶

¹⁴ Press Release, FTC, 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>; *Statement of Chair Khan Regarding the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking* (Aug. 22, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chair-khan-regarding-commercial-surveillance-data-security-advance-notice-proposed>; *Statement of Commissioner Slaughter Regarding the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking* (Aug. 11, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-commissioner-slaughter-regarding-commercial-surveillance-data-security-advance-notice>; *Statement of Commissioner Bedoya Regarding the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking* (Aug. 11, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-commissioner-bedoya-regarding-commercial-surveillance-data-security-advance-notice>; *Dissenting Statement of Commissioner Phillips Regarding the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking* (Aug. 11, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/dissenting-statement-commissioner-phillips-regarding-commercial-surveillance-data-security-advance>; *Dissenting Statement of Commissioner Wilson on the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking* (Aug. 11, 2022), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/dissenting-statement-commissioner-wilson-commercial-surveillance-data-security-advance-notice>.

¹⁵ *FTC Policy Statement on Deception* (1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf; *FTC Policy Statement on Unfairness* (1980), <https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness>.

¹⁶ *Id.*; 15 U.S.C. §§ 41-58.

A statement is a legally sound approach and unlikely to lead to the litigation delays associated with an administrative rulemaking. A statement also provides more flexibility in addressing new issues and incorporating new information and academic and empirical research into decisionmaking. The Commission should work to make such a statement unanimous, to better provide certainty to firms and consumers, and so that the statement has a reasonable chance of withstanding changes in Commission leadership and members.

Each Commissioner,¹⁷ and the agency, has significant experience with privacy and data security issues.¹⁸ Accordingly, the Commission should act quickly to identify its framework, and support for that framework, for deciding matters within the scope of its legal authority.

¹⁷ See, e.g., Remarks of Chair Lina M. Khan, *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; *Executive Session and Nominations Hearing: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 117th Cong. (2021), <https://www.commerce.senate.gov/services/files/F047A749-6887-4383-A54A-7DA1459DC10B> (Opening Statement of Alvaro M. Bedoya Nominee to the Federal Trade Commission); Remarks of Commissioner Christine S. Wilson, *Exploring Options Overcoming Barriers to Comprehensive Federal Privacy Legislation* (Sep. 21, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596632/wilsonspeechovercomingbarriersprivacy.pdf; Remarks of Commissioner Noah Joshua Phillips, *Keep it: Maintaining Competition in the Privacy Debate* (Jul. 27, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395934/phillips_-_internet_governance_forum_7-27-18.pdf; Remarks of Commissioner Rebecca Kelly Slaughter, *Raising the Standard: Bringing Security and Transparency to the Internet of Things?* (Jul. 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395854/slaughter_-_raising_the_standard_-_bringing_security_and_transparency_to_the_internet_of_things_7-26.pdf.

¹⁸ See, e.g., *Oversight of the Federal Trade Commission: Hearing before the S. Comm. on Commerce, Science, and Transportation*, 116th Cong. 7-13 (2020), https://www.ftc.gov/system/files/documents/public_statements/1578963/p180101testimonyftcoversight20200805.pdf (Prepared Statement of the Federal Trade Commission) (“Since ... 1970, the FTC has served as the chief federal agency charged with protecting consumer privacy. With the development of the internet as a commercial medium in the 1990s, the FTC expanded its focus on privacy to reflect the growing collection, use and sharing of consumer data in the commercial marketplace.” ... In addition to our enforcement work, in the privacy and security area, we have hosted about 75 workshops and issued approximately 50 reports.”); Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century: The FTC’s Approach to Consumer Privacy (Apr. 9-10, 2019), <https://www.ftc.gov/news-events/events/2019/04/ftc-hearing-12-ftcs-approach-consumer-privacy>; Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century: Data Security (Dec. 11-12, 2018), <https://www.ftc.gov/news-events/events/2018/12/ftc-hearing-9-data-security>; Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century: Privacy, Big Data and Competition (Nov. 6-8, 2018), <https://www.ftc.gov/news-events/events/2018/11/ftc-hearing-6-privacy-big-data-competition>; FTC INFORMATIONAL INJURY WORKSHOP, BE AND BCP STAFF PERSPECTIVE (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf; *Transcript of Informational Injury Workshop* (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_events/1256463/informational_injury_workshop_transcript_with_index_12-2017.pdf; FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012),

IV. Comments of Andy Jung

I'm Andy Jung. I'm a Legal Fellow at TechFreedom, a nonpartisan technology law and policy think tank.

In Question 26, the Advance Notice of Proposed Rulemaking asks: “*To what extent would any given new trade regulation rule on data security or commercial surveillance impede or enhance innovation?*”¹⁹

I commend the Commission for addressing innovation, which is a factor in the FTC’s cost-benefit analysis required by Section 5(n) of the FTC Act.²⁰ Broad and sweeping trade rules on privacy and data security could impede innovation in three primary ways:

First, new regulations can create higher compliance costs and raise barriers to entry for companies developing online tools and services. This may disincentivize firms, especially small ones and startups, from building or investing in online tools and services.²¹

Second, new privacy and data security regulations could make online tools and services less effective and less accessible.²² For example, rules limiting how firms collect and use consumer data would restrict the ability of firms to offer targeted, personalized services based on behavioral and browsing data.

Third, privacy and data security rules may force firms to start charging for online tools and services that are currently ad-supported. New privacy and data security rules would limit firms’ ability to monetize free online services, forcing them to switch to paid models which charge consumers upfront.

Section 5(n) requires the FTC to weigh injury to consumers against “countervailing benefits to consumers or to competition” when issuing new rules.²³ How to assess innovation in

<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

¹⁹ Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 § IV(c) (Aug. 22, 2022) (“How should the Commission balance costs and benefits?”).

²⁰ 15 U.S.C. § 45(n).

²¹ See Anja Lambrecht, E-Privacy Provisions And Venture Capital Investments In The EU (2017), <https://www.ceps.eu/wp-content/uploads/2017/10/E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments%20in%20the%20EU.PDF>; See also James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRUCTURE 47-73 (2015), <https://onlinelibrary.wiley.com/doi/abs/10.1111/jems.12079>.

²² See Avi Goldfarb & Catherine Tucker, *Privacy and Innovation*, 12 INNOVATION POL’Y & ECON. 65-89 (2012), <https://www.journals.uchicago.edu/doi/full/10.1086/663156>.

²³ 15 U.S.C. § 45(n).

relation to such tradeoffs will be among the most important disputes of material fact in this rulemaking—and critical to whether any rules the Commission issues can survive judicial review.

Respectfully submitted,



Berin Szóka



Bilal Sayyed



Andy Jung

TechFreedom
110 Maryland Ave. NE
Suite 205
Washington, DC 20002

Date: September 15, 2022