072–36262A, dated September 14, 2021, specifies to submit certain information to the manufacturer, this AD does not include that requirement.

(i) Other FAA AD Provisions

The following provisions also apply to this AD:

(1) *Alternative Methods of Compliance (AMOCs):* The Manager, Large Aircraft Section, International Validation Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or responsible Flight Standards Office, as appropriate. If sending information directly to the Large Aircraft Section, International Validation Branch, send it to the attention of the person identified in paragraph (j)(2) of this AD. Information may be emailed to: *9-AVS-AIR-730-AMOC@faa.gov.* Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the responsible Flight Standards Office.

(2) *Contacting the Manufacturer:* For any requirement in this AD to obtain instructions from a manufacturer, the instructions must be accomplished using a method approved by the Manager, Large Aircraft Section, International Validation Branch, FAA; or the United Kingdom Civil Aviation Authority (U.K. CAA); or BAE Systems (Operations) Limited's U.K. CAA Design Organization Approval (DOA). If approved by the DOA, the approval must include the DOA-authorized signature.

(j) Related Information

(1) Refer to Mandatory Continuing Airworthiness Information (MCAI) U.K. CAA AD G–2022–0002, dated February 11, 2022, for related information. This MCAI may be found in the AD docket at *https://www.regulations.gov* by searching for and locating Docket No. FAA–2022–1053.

(2) For more information about this AD, contact Todd Thompson, Aerospace Engineer, Large Aircraft Section, FAA, International Validation Branch, 2200 South 216th St., Des Moines, WA 98198; telephone 206–231–3228; email *todd.thompson@faa.gov.*

(3) For service information identified in this AD, contact BAE Systems (Operations) Limited, Customer Information Department, Prestwick International Airport, Ayrshire, KA9 2RW, Scotland, United Kingdom; telephone +44 1292 675207; fax +44 1292 675704; email *RApublications@baesystems.com;* internet *https://www.baesystems.com/Businesses/RegionalAircraft/index.htm.* You may view this service information at the FAA, Airworthiness Products Section, Operational Safety Branch, 2200 South 216th St., Des Moines, WA. For information on the availability of this material at the FAA, call 206–231–3195.

Issued on August 10, 2022.

Gaetano A. Sciortino,

Deputy Director for Strategic Initiatives, Compliance & Airworthiness Division, Aircraft Certification Service.

[FR Doc. 2022–17985 Filed 8–19–22; 8:45 am]

BILLING CODE 4910–13–P

FEDERAL TRADE COMMISSION

16 CFR Chapter I

Trade Regulation Rule on Commercial Surveillance and Data Security

AGENCY: Federal Trade Commission.

ACTION: Advance notice of proposed rulemaking; request for public comment; public forum.

SUMMARY: The Federal Trade Commission (''FTC'') is publishing this advance notice of proposed rulemaking (''ANPR'') to request public comment on the prevalence of commercial surveillance and data security practices that harm consumers. Specifically, the Commission invites comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.

DATES:

Comments due date: Comments must be received on or before October 21, 2022.

Meeting date: The Public Forum will be held virtually on Thursday, September 8, 2022, from 2 p.m. until 7:30 p.m. Members of the public are invited to attend at the website *https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum.*

ADDRESSES: Interested parties may file a comment online or on paper by following the instructions in the Comment Submissions part of the **SUPPLEMENTARY INFORMATION** section below. Write ''Commercial Surveillance ANPR, R111004'' on your comment, and file your comment online at *https://www.regulations.gov.* If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC–5610 (Annex B), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: James Trilling, 202–326–3497; Peder Magee, 202–326–3538; Olivier Sylvain, 202–326–3046; or *commercialsurveillancerm@ftc.gov.*

I. Overview

Whether they know it or not, most Americans today surrender their personal information to engage in the most basic aspects of modern life. When they buy groceries, do homework, or apply for car insurance, for example, consumers today likely give a wide range of personal information about themselves to companies, including their movements,[1] prayers,[2] friends,[3] menstrual cycles,[4] web-browsing,[5] and faces,[6] among other basic aspects of their lives.

Companies, meanwhile, develop and market products and services to collect and monetize this data. An elaborate and lucrative market for the collection,

[1] *See, e.g.,* Press Release, Fed. Trade Comm'n, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22, 2016), *https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked. See also* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy,* N.Y. Times (Dec. 19, 2019), *https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html;* Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data,* The Markup (Sept. 30, 2021), *https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data;* Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not,* Associated Press (Aug. 13, 2018), *https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb.*

[2] *See, e.g.,* Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps,* Motherboard (Nov. 16, 2020), *https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.*

[3] *See, e.g.,* Press Release, Fed. Trade Comm'n, Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), *https://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.*

[4] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021), *https://www.ftc.gov/news-events/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared.*

[5] *See, e.g.,* Fed. Trade Comm'n, *A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major internet Service Providers: An FTC Staff Report* (Oct. 21, 2021), *https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.*

[6] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology (May 7, 2021), *https://www.ftc.gov/news-events/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse. See also* Tom Simonite, *Face Recognition Is Being Banned—but It's Still Everywhere,* Wired (Dec. 22, 2021), *https://www.wired.com/story/face-recognition-banned-but-everywhere/.*

retention, aggregation, analysis, and onward disclosure of consumer data incentivizes many of the services and products on which people have come to rely. Businesses reportedly use this information to target services—namely, to set prices,[7] curate newsfeeds,[8] serve advertisements,[9] and conduct research on people's behavior,[10] among other things. While, in theory, these personalization practices have the potential to benefit consumers, reports note that they have facilitated consumer harms that can be difficult if not impossible for any one person to avoid.[11]

Some companies, moreover, reportedly claim to collect consumer data for one stated purpose but then also use it for other purposes.[12] Many such firms, for example, sell or otherwise monetize such information or compilations of it in their dealings with advertisers, data brokers, and other third parties.[13] These practices also appear to exist outside of the retail consumer setting. Some employers, for example, reportedly collect an assortment of worker data to evaluate productivity, among other reasons [14]—a practice that has become far more pervasive since the onset of the COVID–19 pandemic.[15]

Many companies engage in these practices pursuant to the ostensible consent that they obtain from their consumers.[16] But, as networked devices and online services become essential to navigating daily life, consumers may have little choice but to accept the terms that firms offer.[17] Reports suggest that consumers have become resigned to the ways in which companies collect and monetize their information, largely because consumers have little to no actual control over what happens to their information once companies collect it.[18]

In any event, the permissions that consumers give may not always be meaningful or informed. Studies have shown that most people do not generally understand the market for consumer data that operates beyond their monitors and displays.[19] Most consumers, for example, know little about the data brokers and third parties who collect and trade consumer data or build consumer profiles [20] that can expose intimate details about their lives and, in the wrong hands, could expose unsuspecting people to future harm.[21]

---

[7] *See, e.g.,* Casey Bond, *Target Is Tracking You and Changing Prices Based on Your Location,* Huffington Post (Feb. 24, 2022), *https://www.huffpost.com/entry/target-tracking-location-changing-prices_l_603fd12bc5b6ff75ac410a38;* Maddy Varner & Aaron Sankin, *Suckers List: How Allstate's Secret Auto Insurance Algorithm Squeezes Big Spenders,* The MarkUp (Feb. 25, 2020), *https://themarkup.org/allstates-algorithm/2020/02/25/car-insurance-suckers-list. See generally* Executive Office of the President of the United States, *Big Data and Differential Pricing,* at 2, 12–13 (Feb. 2015), *https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf.*

[8] *See, e.g.,* Will Oremus et al., *Facebook under fire: How Facebook shapes your feed: The evolution of what posts get top billing on users' news feeds, and what gets obscured,* Wash. Post (Oct. 26, 2021), *https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works/.*

[9] *See, e.g.,* Nat Ives, *Facebook Ad Campaign Promotes Personalized Advertising,* Wall. St. J. (Feb. 25, 2021), *https://www.wsj.com/articles/facebook-ad-campaign-promotes-personalized-advertising-11614261617.*

[10] *See, e.g.,* Elise Hu, *Facebook Manipulates Our Moods for Science and Commerce: A Roundup,* NPR (June 30, 2014), *https://www.npr.org/sections/alltechconsidered/2014/06/30/326929138/facebook-manipulates-our-moods-for-science-and-commerce-a-roundup.*

[11] *See, e.g.,* Matthew Hindman et al., *Facebook Has a Superuser-Supremacy Problem,* The Atlantic (Feb. 10, 2022), *https://www.theatlantic.com/technology/archive/2022/02/facebook-hate-speech-misinformation-superusers/621617/;* Consumer Protection Data Spotlight, Fed. Trade Comm'n, *Social Media a Gold Mine for Scammers in 2021* (Jan. 25, 2022), *https://www.ftc.gov/news-events/blogs/data-spotlight/2022/01/social-media-gold-mine-scammers-2021;* Jonathan Stempel, *Facebook Sued for Age, Gender Bias in Financial Services Ads,* Reuters (Oct. 31, 2019), *https://www.reuters.com/article/us-facebook-lawsuit-bias/facebook-sued-for-age-gender-bias-in-financial-services-ads-idUSKBN1XA2G8;* Karen Hao, *Facebook's Ad Algorithms Are Still Excluding Women from Seeing Jobs,* MIT Tech. Rev. (Apr. 9, 2021), *https://www.technologyreview.com/2021/04/09/1022217/facebook-ad-algorithm-sex-discrimination;* Corin Faife & Alfred Ng, *Credit Card Ads Were Targeted by Age, Violating Facebook's Anti-Discrimination Policy,* The MarkUp (Apr. 29, 2021), *https://themarkup.org/citizen-browser/2021/04/29/credit-card-ads-were-targeted-by-age-violating-facebooks-anti-discrimination-policy.* Targeted behavioral advertising is not the only way in which internet companies automate advertising at scale. Researchers have found that contextual advertising may be as cost-effective as targeting, if not more so. *See, e.g.,* Keach Hagey, *Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests,* Wall St. J. (May 29, 2019), *https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195* (discussing Veronica Marotta et al., *Online Tracking and Publishers' Revenues: An Empirical Analysis* (2019), *https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf*).

[12] *See, e.g.,* Drew Harvell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?,* Wash. Post (Apr. 10, 2019), *https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/;* Jon Keegan & Alfred Ng, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users,* The MarkUp (Dec. 6, 2021), *https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.*

[13] *See, e.g.,* Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. See also, e.g.,* Press Release, Fed. Trade Comm'n, FTC Puts an End to Data Broker Operation that Helped Scam More Than $7 Million from Consumers' Accounts (Nov. 30, 2016), *https://www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million;* Press Release, Fed. Trade Comm'n, Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers (Feb. 18, 2016), *https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive.*

[14] *See, e.g.,* Drew Harwell, *Contract Lawyers Face a Growing Invasion of Surveillance Programs That Monitor Their Work,* Wash. Post (Nov. 11, 2021), *https://www.washingtonpost.com/technology/2021/11/11/lawyer-facial-recognition-monitoring/;* Annie Palmer, *Amazon Is Rolling Out Cameras That Can Detect If Warehouse Workers Are Following Social Distancing Rules,* CNBC (June 16, 2020), *https://www.cnbc.com/2020/06/16/amazon-using-cameras-to-enforce-social-distancing-rules-at-warehouses.html;* Sarah Krouse, *How Google Spies on Its Employees,* The Information (Sept. 23, 2021), *https://www.theinformation.com/articles/how-google-spies-on-its-employees;* 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.*

[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/.*

[16] *See* Tr. of FTC Hr'g, *The FTC's Approach to Consumer Privacy* (Apr. 9, 2019), at 50, *https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_1_4-9-19.pdf* (remarks of Paul Ohm). *See also* Fed. Trade Comm'n, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* 26 (May 2000), *https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.*

[17] *See* Tr. of FTC Hr'g, *The FTC's Approach to Consumer Privacy* (Apr. 10, 2019), at 129, *https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_2_4-10-19.pdf* (remarks of FTC Commissioner Rebecca Kelly Slaughter, describing privacy consent as illusory because consumers often have no choice other than to consent in order to reach digital services that have become necessary for participation in contemporary society).

[18] *See* Joe Nocera, *How Cookie Banners Backfired,* N.Y. Times (Jan. 29, 2022), *https://www.nytimes.com/2022/01/29/business/dealbook/how-cookie-banners-backfired.html* (discussing concept of ''digital resignation'' developed by Nora Draper and Joseph Turow). *See also* Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation,* 21 New Media & Soc'y 1824–39 (2019).

[19] *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent,* 96 Wash. U.L. Rev. 1461, 1477–78, 1498–1502 (2019); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* 126 Harv. L. Rev. 1879, 1885–86 (2013) (''Solove Privacy Article'').

[20] *See generally* Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.*

[21] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Puts an End to Data Broker Operation that Helped Scam More Than $7 Million from Consumers' Accounts (Nov. 30, 2016), *https://www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million;* Press Release, Fed. Trade Comm'n, Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers

Many privacy notices that acknowledge such risks are reportedly not readable to the average consumer.[22] Many consumers do not have the time to review lengthy privacy notices for each of their devices, applications, websites, or services,[23] let alone the periodic updates to them. If consumers do not have meaningful access to this information, they cannot make informed decisions about the costs and benefits of using different services.[24]

This information asymmetry between companies and consumer runs even deeper. Companies can use the information that they collect to direct consumers' online experiences in ways that are rarely apparent—and in ways that go well beyond merely providing the products or services for which consumers believe they sign up.[25] The Commission's enforcement actions have targeted several pernicious dark pattern practices, including burying privacy settings behind multiple layers of the user interface [26] and making misleading representations to ''trick or trap'' consumers into providing personal information.[27] In other instances, firms may misrepresent or fail to communicate clearly how they use and protect people's data.[28] Given the reported scale and pervasiveness of such practices, individual consumer consent may be irrelevant.

The material harms of these commercial surveillance practices may be substantial, moreover, given that they may increase the risks of cyberattack by hackers, data thieves, and other bad actors. Companies' lax data security practices may impose enormous financial and human costs. Fraud and identity theft cost both businesses and consumers billions of dollars, and consumer complaints are on the rise.[29] For some kinds of fraud, consumers have historically spent an average of 60 hours *per victim* trying to resolve the issue.[30] Even the nation's critical infrastructure is at stake, as evidenced by the recent attacks on the largest fuel pipeline,[31] meatpacking plants,[32] and water treatment facilities [33] in the United States.

Companies' collection and use of data have significant consequences for consumers' wallets, safety, and mental health. Sophisticated digital advertising systems reportedly automate the targeting of fraudulent products and services to the most vulnerable consumers.[34] Stalking apps continue to endanger people.[35] Children and teenagers remain vulnerable to cyber bullying, cyberstalking, and the distribution of child sexual abuse material.[36] Peer-reviewed research has linked social media use with depression, anxiety, eating disorders, and suicidal ideation among kids and teens.[37]

Finally, companies' growing reliance on automated systems is creating new

(Feb. 18, 2016), *https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive; FTC* v. *Accusearch,* 570 F.3d 1187, 1199 (10th Cir. 2009). *See also* Molly Olmstead, *A Prominent Priest Was Outed for Using Grindr. Experts Say It's a Warning Sign,* Slate (July 21, 2021), *https://slate.com/technology/2021/07/catholic-priest-grindr-data-privacy.html.*

[22] *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* Pew Res. Ctr. (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/. See also* Solove Privacy Article, 126 Harv. L. Rev. at 1885; Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S J. of L. & Pol'y for Info. Society 543 (2008); Irene Pollach, *What's Wrong with Online Privacy Policies?,* 50 Comm's ACM 103 (2007).

[23] Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster,* N.Y. Times (2019), *https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html;* Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days,* The Atlantic (Mar. 1, 2012), *https://www.theatlantic.com/technology/archive/2012/03/reading-theprivacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/. See also* FTC Comm'r Rebecca Kelly Slaughter, *Wait But Why? Rethinking Assumptions About Surveillance Advertising: IAPP Privacy Security Risk Closing Keynote* (''Slaughter Keynote'') (Oct. 22, 2021), at 4, *https://www.ftc.gov/system/files/documents/public_statements/1597998/iapp_psr_2021_102221_final2.pdf.*

[24] *See* FTC Comm'r Christine S. Wilson, *A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation,* Remarks at the Future of Privacy Forum (Feb. 6, 2020), *https://www.ftc.gov/news-events/news/speeches/remarks-commissioner-christine-s-wilson-future-privacy-forum.*

[25] *See generally* Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power,* 117 Colum. L. Rev. 1623 (2017); Ryan Calo, *Digital Market Manipulation,* 82 Geo. Wash. L. Rev. 995 (2014).

[26] *See* Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), *https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.*

[27] *See* Press Release, Fed. Trade Comm'n, FTC Takes Action against the Operators of Copycat Military websites (Sept. 6, 2018), *https://www.ftc.gov/news-events/press-releases/2018/09/ftc-takes-action-against-operators-copycat-military-websites.*

[28] *See generally infra* Item III(a).

[29] Press Release, Fed. Trade Comm'n, New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021 (Feb. 22, 2022), *https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.*

[30] Fed. Trade Comm'n, *Identity Theft Survey Report* (Sept. 2003), *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-identity-theft-program/synovatereport.pdf.*

[31] 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.*

[32] 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.*

[33] Josh Margolin & Ivan Pereira, *Outdated Computer System Exploited in Florida Water Treatment Plant Hack,* ABC News (Feb. 11, 2021), *https://abcnews.go.com/US/outdated-computer-system-exploited-florida-water-treatment-plant/story?id=75805550.*

[34] *See, e.g.,* Zeke Faux, *How Facebook Helps Shady Advertisers Pollute the internet,* Bloomberg (Mar. 27, 2019), *https://www.bloomberg.com/news/features/2018-03-27/ad-scammers-need-suckers-and-facebook-helps-find-them* (noting an affiliate marketer's claim that Facebook's ad system ''find[s] the morons for me'').

[35] *See* Consumer Advice, Fed. Trade Comm'n, *Stalking Apps: What to Know* (May 2021), *https://consumer.ftc.gov/articles/stalking-apps-what-know.*

[36] *See* Ellen M. Selkie, Jessica L. Fales, & Megan A. Moreno, *Cyberbullying Prevalence Among U.S. Middle and High School-Aged Adolescents: A Systematic Review and Quality Assessment,* 58 J. Adolescent Health 125 (2016); Fed. Trade Comm'n, *Parental Advisory: Dating Apps* (May 6, 2019), *https://consumer.ftc.gov/consumer-alerts/2019/05/parental-advisory-dating-apps;* Subcommittee on Consumer Protection, Product Safety, and Data Security, U.S. Senate Comm. on Com., Sci. & Transp., Hearing, *Protecting Kids Online: internet Privacy and Manipulative Marketing* (May 18, 2021), *https://www.commerce.senate.gov/2021/5/protecting-kids-online-internet-privacy-and-manipulative-marketing; Aisha Counts, Child Sexual Abuse Is Exploding Online. Tech's Best Defenses Are No Match., Protocol (Nov. 12, 2021), https://www.protocol.com/policy/csam-child-safety-online.*

[37] *See, e.g.,* Elroy Boers et al., *Association of Screen Time and Depression in Adolescence,* 173 JAMA Pediatr. 9 (2019) at 857 (''We found that high mean levels of social media over 4 years and any further increase in social media use in the same year were associated with increased depression.''); Hugues Sampasa-Kanyinga & Rosamund F. Lewis, *Frequent Use of Social Networking Sites Is Associated with Poor Psychological Functioning Among Children and Adolescents,* 18 Cyberpsychology, Behavior, and Social Networking 7 (2015) at 380 (''Daily [social networking site] use of more than 2 hours was . . . independently associated with poor self-rating of mental health and experiences of high levels of psychological distress and suicidal ideation.''); Jean M. Twenge et al., *Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time,* 6 Clinical Psychological Sci. 1 (2018) at 11 (''[A]dolescents using social media sites every day were 13% more likely to report high levels of depressive symptoms than those using social media less often.''); H.C. Woods & H. Scott, *#Sleepyteens: Social Media Use in Adolescence is Associated with Poor Sleep Quality, Anxiety, Depression, and Low Self-Esteem,* 51 J. of Adolescence 41–9 (2016) at 1 (''Adolescents who used social media more . . . experienced poorer sleep quality, lower self-esteem and higher levels of anxiety and depression.''); Simon M. Wilksch et al., *The relationship between social media use and disordered eating in young adolescents,* 53 Int'l J. of Eating Disorders 1 at 96 (''A clear pattern of association was found between [social media] usage and [disordered eating] cognitions.'').

forms and mechanisms for discrimination based on statutorily protected categories,[38] including in critical areas such as housing,[39] employment,[40] and healthcare.[41] For example, some employers' automated systems have reportedly learned to prefer men over women.[42] Meanwhile, a recent investigation suggested that lenders' use of educational attainment in credit underwriting might disadvantage students who attended historically Black colleges and universities.[43] And the Department of Justice recently settled its first case challenging algorithmic discrimination under the Fair Housing Act for a social media advertising delivery system that unlawfully discriminated based on protected categories.[44] Critically, these kinds of disparate outcomes may arise even when automated systems consider only *unprotected* consumer traits.[45]

The Commission is issuing this ANPR pursuant to Section 18 of the Federal Trade Commission Act (''FTC Act'') and the Commission's Rules of Practice [46] because recent Commission actions, news reporting, and public research suggest that harmful commercial surveillance and lax data security practices may be prevalent and increasingly unavoidable.[47] These developments suggest that trade regulation rules reflecting these current realities may be needed to ensure Americans are protected from unfair or deceptive acts or practices. New rules could also foster a greater sense of predictability for companies and consumers and minimize the uncertainty that case-by-case enforcement may engender.

Countries around the world and states across the nation have been alert to these concerns. Many accordingly have enacted laws and regulations that impose restrictions on companies' collection, use, analysis, retention, transfer, sharing, and sale or other monetization of consumer data. In recognition of the complexity and opacity of commercial surveillance practices today, such laws have reduced the emphasis on providing notice and obtaining consent and have instead stressed additional privacy ''defaults'' as well as increased accountability for businesses and restrictions on certain practices.

For example, European Union (''EU'') member countries enforce the EU's General Data Protection Regulation (''GDPR''),[48] which, among other things, limits the processing of personal data to six lawful bases and provides consumers with certain rights to access, delete, correct, and port such data. Canada's Personal Information Protection and Electronic Documents Act [49] and Brazil's General Law for the

[38] A few examples of where automated systems may have produced disparate outcomes include inaccuracies and delays in the delivery of child welfare services for the needy; music streaming services that are more likely to recommend men than women; gunshot detection software that mistakenly alerts local police when people light fireworks in majority-minority neighborhoods; search engine results that demean black women; and face recognition software that is more likely to misidentify dark-skinned women than light-skinned men. *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* 81 Proc. of Mach. Learning Res. (2018); 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); Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2018); Andres Ferraro, Xavier Serra, & Christine Bauer, *Break the Loop: Gender Imbalance in Music Recommenders,* CHIIR '21: Proceedings of the 2021 Conference on Human Information Interaction and Retrieval, 249–254 (Mar. 2021), *https://dl.acm.org/doi/proceedings/10.1145/3406522. See generally* Anita Allen, *Dismantling the ''Black Opticon'': Privacy, Race, Equity, and Online Data-Protection Reform,* 131 Yale L. J. Forum 907 (2022), *https://www.yalelawjournal.org/pdf/F7.AllenFinalDraftWEB_6f26iyu6.pdf;* Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism (2018); Danielle Citron, Hate Crimes in Cyberspace (2014).

[39] *See* Ny Magee, *Airbnb Algorithm Linked to Racial Disparities in Pricing,* The Grio (May 13, 2021), *https://thegrio.com/2021/05/13/airbnb-racial-disparities-in-pricing/;* Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms,* ABC News & The MarkUp (Aug. 25, 2021), *https://abcnews.go.com/Business/wireStory/secret-bias-hidden-mortgage-approval-algorithms-79633917. See generally* Fed. Trade Comm'n, Accuracy in Consumer Reporting Workshop (Dec. 10, 2019), *https://www.ftc.gov/news-events/events-calendar/accuracy-consumer-reporting-workshop. See also* Alex P. Miller & Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias,* Harv. Bus. Rev. (Nov. 8, 2019), *https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias.*

[40] *See* Ifeoma Ajunwa, *The ''Black Box'' at Work,* Big Data & Society (Oct. 19, 2020), *https://journals.sagepub.com/doi/full/10.1177/2053951720938093.*

[41] *See* Donna M. Christensen et al., *Medical Algorithms are Failing Communities of Color,* Health Affs. (Sept. 9, 2021), *https://www.healthaffairs.org/do/10.1377/hblog20210903.976632/full/;* Heidi Ledford, *Millions of Black People Affected by Racial Bias in Health-Care Algorithms,* Nature (Oct. 24, 2019), *https://www.nature.com/articles/d41586-019-03228-6/.*

[42] Jeffrey Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women,* Reuters (Oct. 10, 2018), *https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G;* Dave Gershgorn, *Companies are on the hook if their hiring algorithms are biased,* Quartz (Oct. 22, 2018), *https://qz.com/1427621/companies-are-on-the-hook-if-their-hiring-algorithms-are-biased/.*

[43] Katherine Welbeck & Ben Kaufman, *Fintech Lenders' Responses to Senate Probe Heighten Fears of Educational Redlining,* Student Borrower Prot. Ctr. (July 31, 2020), *https://protectborrowers.org/fintech-lenders-response-to-senate-probe-heightens-fears-of-educational-redlining/.* This issue is currently being investigated by the company and outside parties. Relman Colfax, *Fair Lending Monitorship of Upstart Network's Lending Model, https://www.relmanlaw.com/cases-406.*

[44] Compl., *United States* v. *Meta Platforms, Inc.,* No. 22–05187 (S.D.N.Y. filed June 21, 2022), *https://www.justice.gov/usao-sdny/press-release/file/1514051/download;* Settlement Agreement, *United States* v. *Meta Platforms, Inc.,* No. 22–05187 (S.D.N.Y. filed June 21, 2022), *https://www.justice.gov/crt/case-document/file/1514126/download.*

[45] Andrew Selbst, *A New HUD Rule Would Effectively Encourage Discrimination by Algorithm,* Slate (Aug. 19, 2019), *https://slate.com/technology/2019/08/hud-disparate-impact-discrimination-algorithm.html. See also* Rebecca Kelly Slaughter, *Algorithms and Economic Justice,* 23 Yale J. L. & Tech. 1, 11–14 (2021) (''Slaughter Algorithms Paper''); Anupam Chander, *The Racist Algorithm?,* 115 Mich. L. Rev. 1023, 1029–30, 1037–39 (2017); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact,* 104 Calif. L. Rev. 671, 677–87 (2016).

[46] 15 U.S.C. 57a; 16 CFR parts 0 and 1.

[47] In May 2022, three consumer advocacy groups urged the Commission to commence a rulemaking proceeding to protect ''privacy and civil rights.'' *See* Letter of Free Press, Access Now, and UltraViolet to Chair Lina M. Khan (May 12, 2022), *https://act.freepress.net/sign/protect_privacy_civil_rights.* Late in 2021, moreover, the Commission received a petition that calls on it to promulgate rules pursuant to its authority to protect against unfair methods of competition in the market for consumer data. *See* Press Release, Accountable Tech, Accountable Tech Petitions FTC to Ban Surveillance Advertising as an 'Unfair Method of Competition' (Sept. 28, 2021), *https://accountabletech.org/media/accountable-tech-petitions-ftc-to-ban-surveillance-advertising-as-an-unfair-method-of-competition/.* In accordance with the provision of its Rules of Practice concerning public petitions, 16 CFR 1.31, the Commission published a notice about the petition, 86 FR 73206 (Dec. 23, 2021), and accepted public comments, which are compiled at *https://www.regulations.gov/docket/FTC-2021-0070/comments.* The petitioner urges new rules that address the way in which certain dominant companies exploit their access to and control of consumer data. Those unfair-competition concerns overlap with some of the concerns in this ANPR about unfair or deceptive acts or practices, and several comments in support of the petition also urged the Commission to pursue a rulemaking using its authority to regulate unfair or deceptive practices. *See, e.g.,* Cmt. of Consumer Reports & Elec. Privacy Info. Ctr., at 2 (Jan. 27, 2022), *https://downloads.regulations.gov/FTC-2021-0070-0009/attachment_1.pdf.* Accordingly, Item IV, below, invites comment on the ways in which existing and emergent commercial surveillance practices harm competition and on any new trade regulation rules that would address such practices. Such rules could arise from the Commission's authority to protect against unfair methods of competition, so they may be proposed directly without first being subject of an advance notice of proposed rulemaking. *See* 15 U.S.C. 57a(a)(2) (Section 18's procedural requirements, including an ANPR, apply to rules defining unfair or deceptive acts or practices but expressly do not apply to rules ''with respect to unfair methods of competition'').

[48] *See Data Protection in the EU,* Eur. Comm'n, *https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.*

[49] *See Personal Information Protection and Electronic Documents Act (PIPEDA),* Off. of the Privacy Comm'r of Can., *https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-*

Protection of Personal Data [50] contain some similar rights.[51] Laws in California,[52] Virginia, [53] Colorado,[54] Utah,[55] and Connecticut,[56] moreover, include some comparable rights, and numerous state legislatures are considering similar laws. Alabama,[57] Colorado,[58] and Illinois,[59] meanwhile, have enacted laws related to the development and use of artificial intelligence. Other states, including Illinois,[60] Texas,[61] and Washington,[62] have enacted laws governing the use of biometric data. All fifty U.S. states have laws that require businesses to notify consumers of certain breaches of consumers' data.[63] And numerous states require businesses to take reasonable steps to secure consumers' data.[64]

Through this ANPR, the Commission is beginning to consider the potential need for rules and requirements regarding commercial surveillance and lax data security practices. Section 18 of the FTC Act authorizes the Commission to promulgate, modify, and repeal trade regulation rules that define with specificity acts or practices that are unfair or deceptive in or affecting commerce within the meaning of Section 5(a)(1) of the FTC Act.[65] Through this ANPR, the Commission aims to generate a public record about prevalent commercial surveillance practices or lax data security practices that are unfair or deceptive, as well as about efficient, effective, and adaptive regulatory responses. These comments will help to sharpen the Commission's enforcement work and may inform reform by Congress or other policymakers, even if the Commission does not ultimately promulgate new trade regulation rules.[66]

The term ''data security'' in this ANPR refers to breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices.

For the purposes of this ANPR, ''commercial surveillance'' refers to the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information. These data include both information that consumers actively provide—say, when they affirmatively register for a service or make a purchase—as well as personal identifiers and other information that companies collect, for example, when a consumer casually browses the web or opens an app. This latter category is far broader than the first.

The term ''consumer'' as used in this ANPR includes businesses and workers, not just individuals who buy or exchange data for retail goods and services. This approach is consistent with the Commission's longstanding practice of bringing enforcement actions against firms that harm companies [67] as well as workers of all kinds.[68] The FTC has frequently used Section 5 of the FTC Act to protect small businesses or individuals in contexts involving their employment or independent contractor status.[69]

This ANPR proceeds as follows. Item II outlines the Commission's existing authority to bring enforcement actions and promulgate trade regulation rules under the FTC Act. Item III sets out the wide range of actions against commercial surveillance and data security acts or practices that the Commission has pursued in recent years as well as the benefits and shortcomings of this case-by-case approach. Item IV sets out the questions on which the Commission seeks public comment. Finally, Item V provides instructions on the comment submission process, and Item VI describes a public forum that is scheduled to take place to facilitate public involvement in this rulemaking proceeding.

II. The Commission's Authority

Congress authorized the Commission to propose a rule defining unfair or

personal-information-protection-and-electronic-documents-act-pipeda/ (last modified Dec. 8, 2021).

[50] Brazilian General Data Protection Law (Law No. 13,709, of Aug. 14, 2018), *https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.*

[51] In 2021, the European Commission also announced proposed legislation to create additional rules for artificial intelligence that would, among other things, impose particular documentation, transparency, data management, recordkeeping, security, assessment, notification, and registration requirements for certain artificial intelligence systems that pose high risks of causing consumer injury. *See Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,* COM (2021) 206 final (Apr. 21, 2021), *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.*

[52] *See* California Privacy Rights Act of 2020, Proposition 24 (Cal. 2020) (codified at Cal. Civ. Code 1798.100–199.100); State of Cal. Dep't of Just., *California Consumer Privacy Act (CCPA): Frequently Asked Questions (FAQs), https://oag.ca.gov/privacy/ccpa.*

[53] *See* Consumer Data Protection Act, S.B. 1392, 161st Gen. Assem. (Va. 2021) (codified at Va. Code Ann. 59.1–575 through 59.1–585 (2021)).

[54] *See* Protect Personal Data Privacy Act, 21 S.B. 190, 73 Gen. Assem. (Colo. 2021).

[55] *See* Utah Consumer Privacy Act, 2022 Utah Laws 462 (codified at Utah Code Ann. 13–61–1 through 13–61–4).

[56] *See* An Act Concerning Personal Data Privacy and Online Monitoring, 2022 Conn. Acts P.A. 22–15 (Reg. Sess.).

[57] *See* Act. No. 2021–344, S.B. 78, 2021 Leg., Reg. Sess., (Ala. 2021).

[58] *See* Restrict Insurers' Use of External Consumer Data Act, 21 S.B. 169, 73rd Gen. Assem., 1st Reg. Sess. (Colo. 2021).

[59] *See* Artificial Intelligence Video Interview Act, H.B. 53, 102nd Gen. Assem., Reg. Sess. (Ill. 2021) (codified at 820 Ill. Comp. Stat. Ann. 42/1 *et seq.*).

[60] *See* Biometric Information Privacy Act, S.B. 2400, 2008 Gen. Assem., Reg. Sess. (Ill. 2021) (codified at 740 Ill. Comp. Stat. Ann. 14/1 *et seq.*).

[61] *See* Tex. Bus. & Com. Code 503.001.

[62] *See* Wash. Rev. Code Ann. 19.375.010 through 19.375.900.

[63] *See* Nat'l Conf. of State Leg., *Security Breach Notification Laws* (Jan. 17, 2022), *https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.*

[64] *See* Nat'l Conf. of State Leg., *Data Security Laws, Private Sector* (May 29, 2019), *https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.*

[65] 15 U.S.C. 45(a)(1).

[66] *Cf.* Slaughter Keynote at 4; Oral Statement of Comm'r Christine S. Wilson, *Strengthening the Federal Trade Commission's Authority to Protect Consumers: Hearing before the Senate Comm. on Com., Sci. & Transp.* (Apr. 20, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1589180/opening_statement_final_for_postingrevd.pdf.*

[67] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Obtains Contempt Ruling Against 'Yellow Pages' Scam (Nov. 25, 2015), *https://www.ftc.gov/news-events/press-releases/2015/11/ftc-obtains-contempt-ruling-against-yellow-pages-scam;* Press Release, Fed. Trade Comm'n, FTC and Florida Halt internet 'Yellow Pages' Scammers (July 17, 2014), *https://www.ftc.gov/news-events/press-releases/2014/07/ftc-florida-halt-internet-yellow-pages-scammers; In re Spiegel, Inc.,* 86 F.T.C. 425, 439 (1975). *See also FTC* v. *Sperry & Hutchinson Co.,* 405 U.S. 233, 244 (1972); *FTC* v. *Bunte Bros., Inc.,* 312 U.S. 349, 353 (1941); *In re Orkin Exterminating Co., Inc.,* 108 F.T.C. 263 (1986), *aff'd, Orkin Exterminating Co., Inc.* v. *FTC,* 849 F.2d 1354 (11th Cir. 1988); *FTC* v. *Datacom Mktg., Inc.,* No. 06-c-2574, 2006 WL 1472644, at *2 (N.D. Ill. May 24, 2006). Previously, the Commission included ''businessmen'' among those Congress charged it to protect under the statute. *See* Fed. Trade Comm'n, FTC Policy Statement on Unfairness (Dec. 17, 1980), appended to *In re Int'l Harvester Co.,* 104 F.T.C. 949, 1072 n.8 (1984), *https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.*

[68] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Settles Charges Against Two Companies That Allegedly Failed to Protect Sensitive Employee Data (May 3, 2011), *https://www.ftc.gov/news-events/press-releases/2011/05/ftc-settles-charges-against-two-companies-allegedly-failed;* Press Release, Fed. Trade Comm'n, Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (July 27, 2010), *https://www.ftc.gov/news-events/press-releases/2010/07/rite-aid-settles-ftc-charges-it-failed-protect-medical-financial;* Press Release, Fed. Trade Comm'n, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009), *https://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial. See also* Press Release, Fed. Trade Comm'n, Amazon To Pay $61.7 Million to Settle FTC Charges It Withheld Some Customer Tips from Amazon Flex Drivers (Feb. 2, 2021), *https://www.ftc.gov/news-events/press-releases/2021/02/amazon-pay-617-million-settle-ftc-charges-it-withheld-some.*

[69] *See, e.g., FTC* v. *IFC Credit Corp.,* 543 F. Supp. 2d 925, 934–41 (N.D. Ill. 2008) (holding that the FTC's construction of the term ''consumer'' to include businesses as well as individuals is reasonable and is supported by the text and history of the FTC Act).

deceptive acts or practices with specificity when the Commission ''has reason to believe that the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent.'' [70] A determination about prevalence can be made either on the basis of ''cease-and-desist'' orders regarding such acts or practices that the Commission has previously issued, or when it has ''any other information'' that ''indicates a widespread pattern of unfair or deceptive acts or practices.'' [71]

Generally, a practice is unfair under Section 5 if (1) it causes or is likely to cause substantial injury, (2) the injury is not reasonably avoidable by consumers, and (3) the injury is not outweighed by benefits to consumers or competition.[72] A representation, omission, or practice is deceptive under Section 5 if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers—that is, it would likely affect the consumer's conduct or decision with regard to a product or service.[73] Under the statute, this broad language is applied to specific commercial practices through Commission enforcement actions and the promulgation of trade regulation rules.

In addition to the FTC Act, the Commission enforces a number of sector-specific laws that relate to commercial surveillance practices, including: the Fair Credit Reporting Act,[74] which protects the privacy of consumer information collected by consumer reporting agencies; the Children's Online Privacy Protection Act (''COPPA''),[75] which protects information collected online from children under the age of 13; the Gramm-Leach-Bliley Act (''GLBA''),[76] which protects the privacy of customer information collected by financial institutions; the Controlling the Assault of Non-Solicited Pornography and Marketing (''CAN–SPAM'') Act,[77] which allows consumers to opt out of receiving commercial email messages; the Fair Debt Collection Practices Act,[78] which protects individuals from harassment by debt collectors and imposes disclosure requirements on related third-parties; the Telemarketing and Consumer Fraud and Abuse Prevention Act,[79] under which the Commission implemented the Do Not Call Registry; [80] the Health Breach Notification Rule,[81] which applies to certain health information; and the Equal Credit Opportunity Act,[82] which protects individuals from discrimination on the basis of race, color, religion, national origin, sex, marital status, receipt of public assistance, or good faith exercise of rights under the Consumer Credit Protection Act and requires creditors to provide to applicants, upon request, the reasons underlying decisions to deny credit.

III. The Commission's Current Approach to Privacy and Data Security

a. Case-By-Case Enforcement and General Policy Work

For more than two decades, the Commission has been the nation's privacy agency, engaging in policy work and bringing scores of enforcement actions concerning data privacy and security.[83] These actions have alleged that certain practices violate Section 5 of the FTC Act or other statutes to the extent they pose risks to physical security, cause economic or reputational injury, or involve unwanted intrusions into consumers' daily lives.[84] For example, the Commission has brought actions for:

- the surreptitious collection and sale of consumer phone records obtained through false pretenses; [85]
- the public posting of private health-related data online; [86]
- the sharing of private health-related data with third parties; [87]
- inaccurate tenant screening; [88]
- public disclosure of consumers' financial information in responses to consumers' critical online reviews of the publisher's services; [89]
- pre-installation of ad-injecting software that acted as a man-in-the-middle between consumers and all websites with which they communicated and collected and transmitted to the software developer consumers' internet browsing data; [90]
- solicitation and online publication of ''revenge porn''—intimate pictures and videos of ex-partners, along with their personal information—and the collection of fees to take down such information; [91]
- development and marketing of ''stalkerware'' that purchasers surreptitiously installed on others' phones or computers in order to monitor them; [92]

[70] 15 U.S.C. 57a(b)(3).

[71] *Id.*

[72] 15 U.S.C. 45(n).

[73] *See* FTC Policy Statement on Deception (Oct. 14, 1983), appended to *In re Cliffdale Assocs., Inc.,* 103 F.T.C. 110, 174 (1984), *https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.*

[74] 15 U.S.C. 1681 through 1681x.

[75] 15 U.S.C. 6501 through 6506.

[76] Public Law 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

[77] 15 U.S.C. 7701 through 7713.

[78] 15 U.S.C. 1692 through 1692p.

[79] 15 U.S.C. 6101 through 6108.

[80] 16 CFR part 310.

[81] 16 CFR part 318.

[82] 15 U.S.C. 1691 through 1691f.

[83] ''Since 1995, the Commission has been at the forefront of the public debate on online privacy.'' Fed. Trade Comm'n, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* 3 (2000), *http://www.ftc.gov/reports/privacy2000/privacy2000.pdf* (third consecutive annual report to Congress after it urged the Commission to take on a greater role in policing privacy practices using Section 5 as the internet grew from a niche service to a mainstream utility). The first online privacy enforcement action came in 1998 against GeoCities, ''one of the most popular sites on the World Wide Web.'' 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), *http://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting.*

[84] *See* Fed. Trade Comm'n, *Comment to the National Telecommunications & Information Administration on Developing the Administration's Approach to Consumer Privacy,* No. 180821780–8780–01, 8–9 (Nov. 9, 2018), *https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developingadministrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf;* FTC Comm'r Christine S. Wilson, *A Defining Moment for Privacy: The Time Is Ripe for Federal Privacy Legislation: Remarks at the Future of Privacy Forum* 11, n.39 (Feb. 6, 2020), *https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf.*

[85] *See, e.g.,* Compl. for Injunctive and Other Equitable Relief, *United States* v. *Accusearch, Inc.,* No. 06–cv–105 (D. Wyo. filed May 1, 2006), *https://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf.*

[86] *See, e.g.,* Compl., *In re Practice Fusion, Inc.,* F.T.C. File No. 142–3039 (Aug. 16, 2016), *https://www.ftc.gov/system/files/documents/cases/160816practicefusioncmpt.pdf.*

[87] *See, e.g.,* Decision and Order, *In re Flo Health, Inc.,* FTC File No. 1923133 (June 22, 2021), *www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf.*

[88] *See, e.g.,* Compl. for Civ. Penalties, Permanent Injunction, and Other Equitable Relief, *United States* v. *AppFolio, Inc.,* No. 1:20-cv-03563 (D.D.C. filed Dec. 8, 2020), *https://www.ftc.gov/system/files/documents/cases/ecf_1_-_us_v_appfolio_complaint.pdf.*

[89] *See, e.g.,* Compl., *United States* v. *Mortg. Sols. FCS, Inc.,* No. 4:20–cv–00110 (N.D. Cal. filed Jan. 6, 2020), *https://www.ftc.gov/system/files/documents/cases/mortgage_solutions_complaint.pdf.*

[90] *See, e.g.,* Decision and Order, *In re Lenovo (United States) Inc.,* FTC File No. 152 3134 (Dec. 20, 2017), *https://www.ftc.gov/system/files/documents/cases/152_3134_c4636_lenovo_united_states_decision_and_order.pdf.*

[91] *See, e.g.,* Compl. for Permanent Injunction and Other Equitable Relief, *FTC and State of Nevada* v. *EMP Media, Inc.,* No. 2:18–cv–00035 (D. Nev. filed Jan. 9, 2018), *https://www.ftc.gov/system/files/documents/cases/1623052_myex_complaint_1-9-18.pdf;* Compl., *In re Craig Brittain,* F.T.C. File No. 132–3120 (Dec. 28, 2015), *https://www.ftc.gov/system/files/documents/cases/160108craigbrittaincmpt.pdf.*

[92] *See, e.g.,* Compl., *In re Support King, LLC,* F.T.C. File No. 192–3003 (Dec. 20, 2021), *https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfonecomplaint_0.pdf;* Compl., *In re Retina-X Studios, LLC,* F.T.C. File No. 172–3118

• retroactive application of material privacy policy changes to personal information that businesses previously collected from users; [93]

• distribution of software that caused or was likely to cause consumers to unwittingly share their files publicly; [94]

• surreptitious activation of webcams in leased computers placed in consumers' homes; [95]

• sale of sensitive data such as Social Security numbers to third parties who did not have a legitimate business need for the information,[96] including known fraudsters; [97]

• collection and sharing of sensitive television-viewing information to target advertising contrary to reasonable expectations; [98]

• collection of phone numbers and email addresses to improve social media account security, but then deceptively using that data to allow companies to target advertisements in violation of an existing consent order; [99]

• failure to implement reasonable measures to protect consumers' personal information,[100] including Social Security numbers and answers to password reset questions,[101] and later covering up an ensuing breach; [102] and

• misrepresentations of the safeguards employed to protect data.[103]

This is just a sample of the Commission's enforcement work in data privacy and security.[104]

The orders that the Commission has obtained in these actions impose a variety of remedies, including prohibiting licensing, marketing, or selling of surveillance products,[105] requiring companies under order to implement comprehensive privacy and security programs and obtain periodic assessments of those programs by independent third parties,[106] requiring deletion of illegally obtained consumer information [107] or work product derived from that data,[108] requiring companies to provide notice to consumers affected by harmful practices that led to the action,[109] and mandating that companies improve the transparency of their data management practices.[110] The Commission may rely on these orders to seek to impose further sanctions on firms that repeat their unlawful practices.[111]

(Mar. 26, 2020), *https://www.ftc.gov/system/files/documents/cases/172_3118_retina-x_studios_complaint_0.pdf;* Compl. for Permanent Injunction and Other Equitable Relief, *FTC* v. *CyberSpy Software, LLC.,* No. 6:08–cv–01872 (M.D. Fla. filed Nov. 5, 2008), *https://www.ftc.gov/sites/default/files/documents/cases/2008/11/081105cyberspycmplt.pdf.*

[93] *See, e.g.,* Compl., *In re Facebook, Inc.,* F.T.C. File No. 092–3184 (July 27, 2012), *https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf;* Compl., *In re Gateway Learning Corp.,* F.T.C. File No. 042–3047 (Sept. 10, 2004), *https://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917comp0423047.pdf.*

[94] *See, e.g.,* Compl. for Permanent Injunction and Other Equitable Relief, *FTC* v. *FrostWire LLC,* No. 1:11–cv–23643 (S.D. Fla. filed Oct. 7, 2011), *https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf.*

[95] *See, e.g.,* Compl., *In re DesignerWare, LLC,* F.T.C. File No. 112–3151 (Apr. 11, 2013), *https://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf;* Compl., *In re Aaron's, Inc.,* F.T.C. File No. 122–3264 (Mar. 10, 2014), *https://www.ftc.gov/system/files/documents/cases/140311aaronscmpt.pdf.*

[96] *See, e.g.,* Compl. for Permanent Injunction and Other Equitable Relief, *FTC* v. *Blue Global & Christopher Kay,* 2:17–cv–02117 (D. Ariz. filed July 3, 2017), *https://www.ftc.gov/system/files/documents/cases/ftc_v_blue_global_de01.pdf.*

[97] *See, e.g.,* Compl. for Permanent Injunction and Other Equitable Relief, *FTC* v. *Sequoia One, LLC,* Case No. 2:15–cv–01512 (D. Nev. filed Aug. 7, 2015), *https://www.ftc.gov/system/files/documents/cases/150812sequoiaonecmpt.pdf;* Compl. for Permanent Injunction and Other Equitable Relief, *FTC* v. *Sitesearch Corp.,* No. CV–14–02750–PHX–NVW (D. Ariz. filed Dec. 22, 2014), *https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf.*

[98] *See, e.g.,* Compl. for Permanent Injunction and Other Equitable and Monetary Relief, *FTC* v. *Vizio, Inc.,* No. 2:17–cv–00758 (D.N.J. filed Feb 6, 2017), *https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.*

[99] *See, e.g.,* Compl. for Civil Penalties, Permanent Injunction, Monetary Relief, and other Equitable Relief, *United States* v. *Twitter, Inc.,* Case No. 3:22–cv–3070 (N.D. Cal. filed May 25, 2022), *https://www.ftc.gov/system/files/ftc_gov/pdf/2023062TwitterFiledComplaint.pdf.*

[100] *See, e.g.,* Compl., *In re InfoTrax Sys., L.C.,* F.T.C. File No. 162–3130 (Dec. 30, 2019), *https://www.ftc.gov/system/files/documents/cases/c-4696_162_3130_infotrax_complaint_clean.pdf;* Compl. for Permanent Injunction & Other Relief, *FTC* v. *Equifax, Inc.,* No. 1:19-mi-99999–UNA (N.D. Ga. filed July 22, 2019), *https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf;* First Amended Compl. for Injunctive and Other Relief, *FTC* v. *Wyndham Worldwide Corp.,* No. 2:12–01365 (D. Ariz. filed Aug. 9, 2012), *https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.*

[101] *See, e.g.,* Compl., *In re Residual Pumpkin Entity, LLC,* F.T.C. File No. 1923209 (June 23, 2022), *https://www.ftc.gov/system/files/ftc_gov/pdf/1923209CafePressComplaint.pdf.*

[102] *Id.*

[103] *See, e.g.,* Compl., *In re MoviePass, Inc.,* F.T.C. File No. 192–3000 (Oct. 1, 2021), *https://www.ftc.gov/system/files/documents/cases/1923000_-_moviepass_complaint_final.pdf;* Compl., *In re SkyMed Int'l, Inc.,* F.T.C. File No. 192–3140 (Jan. 26, 2021), *https://www.ftc.gov/system/files/documents/cases/c-4732_skymed_final_complaint.pdf;* Compl., *In re HTC Am., Inc.,* F.T.C. File No. 122–3049 (June 25, 2013), *https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf.*

[104] *See also, e.g.,* Compl., *In re Turn Inc.,* F.T.C. File No. 152–3099 (Apr. 6, 2017) (alleging that Respondent deceptively tracked consumers online and through their mobile applications for advertising purposes even after consumers took steps to opt out of such tracking), *https://www.ftc.gov/system/files/documents/cases/152_3099_c4612_turn_complaint.pdf;* Compl., *In re Epic Marketplace, Inc.,* F.T.C. File No. 112–3182 (Mar. 13, 2013) (alleging the Respondents deceptively collected for advertising purposes information about consumers' interest in sensitive medical and financial and other issues), *https://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315epicmarketplacecmpt.pdf;* Compl., *In re ScanScout, Inc.,* F.T.C. File No. 102–3185 (Dec. 14, 2011) (alleging that Respondent deceptively used flash cookies to collect for advertising purposes the data of consumers who changed their web browser settings to block cookies), *https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutcmpt.pdf;* Compl., *In re Chitika, Inc.,* F.T.C. File No. 102–3087 (June 7, 2011) (alleging that Respondent deceptively tracked consumers online for advertising purposes even after they opted out of online tracking on Respondent's website), *https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110617chitikacmpt.pdf.*

[105] Decision and Order, *In re Support King, LLC,* F.T.C. File No. 192–3003 (Dec. 20, 2021), *https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfoneorder.pdf.*

[106] *See, e.g.,* Decision and Order, *In re Zoom Video Commc'ns, Inc.,* F.T.C. File No. 192–3167 (Jan. 19, 2021), *https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf;* Decision and Order, *In re Tapplock,* F.T.C. File No. 192–3011 (May 18, 2020), *https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockorder.pdf;* Decision and Order, *In re Uber Techs., Inc.,* F.T.C. File No. 152–3054 (Oct. 25, 2018), *https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf.*

[107] Decision and Order, *In re Retina-X Studios,* F.T.C. File No. 172–3118 (Mar. 26, 2020), *https://www.ftc.gov/system/files/documents/cases/1723118retinaxorder_0.pdf;* Decision and Order, *In re PaymentsMD, LLC,* F.T.C. File No. 132–3088 (Jan. 27, 2015), *https://www.ftc.gov/system/files/documents/cases/150206paymentsmddo.pdf.*

[108] *See, e.g.,* Decision and Order, *In re Everalbum, Inc.,* F.T.C. File No. 192–3172 (May 6, 2021), *https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf;* Final Order, *In re Cambridge Analytica, LLC,* F.T.C. File No. 182–3107 (Nov. 25, 2019), *https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_orderpublic.pdf. See generally* Slaughter Algorithms Paper, 23 Yale J. L. & Tech. at 38–41 (discussing algorithmic disgorgement).

[109] *See, e.g.,* Decision and Order, *In re Flo Health, Inc.,* F.T.C. File No. 192–3133 (June 17, 2021), *https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf.*

[110] *See, e.g.,* Decision and Order, *In re Everalbum, Inc.,* F.T.C. File No. 192–3172 (May 6, 2021), *https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf.*

[111] *See, e.g.,* 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;* 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/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions;* Press Release, Fed. Trade Comm'n, LifeLock to Pay $100 Million to Consumers to Settle FTC Charges it Violated 2010 Order (Dec. 17, 2015), *https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated;* Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari internet Browser (Aug. 9, 2012), *https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented;* Press Release, Fed. Trade

Continued

The Commission has also engaged in broader policy work concerning data privacy and security. For example, it has promulgated rules pursuant to the sector-specific statutes enumerated above.[112] It also has published reports and closely monitored existing and emergent practices, including data brokers' activities,[113] ''dark patterns,'' [114] facial recognition,[115] Internet of Things,[116] big data,[117] cross-device tracking,[118] and mobile privacy disclosures.[119] The Commission, furthermore, has invoked its authority under Section 6(b) to require companies to prepare written reports or answer specific questions about their commercial practices.[120]

b. Reasons for Rulemaking

The Commission's extensive enforcement and policy work over the last couple of decades on consumer data privacy and security has raised important questions about the prevalence of harmful commercial surveillance and lax data security practices. This experience suggests that enforcement alone without rulemaking may be insufficient to protect consumers from significant harms. First, the FTC Act limits the remedies that the Commission may impose in enforcement actions on companies for violations of Section 5.[121] Specifically, the statute generally does not allow the Commission to seek civil penalties for first-time violations of that provision.[122] The fact that the Commission does not have authority to seek penalties for first-time violators may insufficiently deter future law violations. This may put firms that are careful to follow the law, including those that implement reasonable privacy-protective measures, at a competitive disadvantage. New trade regulation rules could, by contrast, set clear legal requirements or benchmarks by which to evaluate covered companies. They also would incentivize all companies to invest in compliance more consistently because, pursuant to the FTC Act, the Commission may impose civil penalties for first-time violations of duly promulgated trade regulation rules.[123]

Second, while the Commission can enjoin conduct that violates Section 5, as a matter of law and policy enforcement, such relief may be inadequate in the context of commercial surveillance and lax data security practices. For instance, after a hacker steals personal consumer data from an inadequately secured database, an injunction stopping the conduct and requiring the business to take affirmative steps to improve its security going forward can help prevent future breaches but does not remediate the harm that has already occurred or is likely to occur.[124]

Third, even in those instances in which the Commission can obtain monetary relief for violations of Section 5, such relief may be difficult to apply to some harmful commercial surveillance or lax data security practices that may not cause direct financial injury or, in any given individual case, do not lend themselves to broadly accepted ways of quantifying harm.[125] This is a problem that is underscored by commercial surveillance practices involving automated decision-making systems where the harm to any given individual or small group of individuals might affect other consumers in ways that are opaque or

---

Comm'n, Consumer Data Broker ChoicePoint Failed to Protect Consumers' Personal Data, Left Key Electronic Monitoring Tool Turned Off for Four Months (Oct. 19, 2009), *https://www.ftc.gov/news-events/press-releases/2009/10/consumer-data-broker-choicepoint-failed-protect-consumers.*

[112] *See, e.g.,* 16 CFR part 312 (COPPA Rule); 16 CFR part 314 (GLBA Safeguards Rule). The Commission recently updated the GLBA rules. *See* Press Release, Fed. Trade Comm'n, FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches (Oct. 27, 2021), *https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial.*

[113] *See, e.g.,* Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.*

[114] *See* Fed. Trade Comm'n, *Bringing Dark Patterns to Light: An FTC Workshop* (Apr. 29, 2021), *https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop. See also* Press Release, Fed. Trade Comm'n, FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions (Oct. 28, 2021), *https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap.* The Commission's recent policy statement on ''negative option marketing,'' moreover, takes up overlapping concerns about the ways in which companies dupe consumers into purchasing products or subscriptions by using terms or conditions that enable sellers to interpret a consumer's failure to assertively reject the service or cancel the agreement as consent. *See* Fed. Trade Comm'n, Enforcement Policy Statement Regarding Negative Option Marketing (Oct. 28, 2021), *https://www.ftc.gov/public-statements/2021/10/enforcement-policy-statement-regarding-negative-option-marketing.* Those practices do not always entail the collection and use of consumer data, and do not always count as ''commercial surveillance'' as we mean the term in this ANPR.

[115] *See* Fed. Trade Comm'n, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* (Oct. 2012), *https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.*

[116] *See* Fed. Trade Comm'n, *Internet of Things: Privacy & Security in a Connected World* (Jan. 2015), *https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.*

[117] *See* Fed. Trade Comm'n, *Big Data: A Tool for Inclusion or Exclusion?* (Jan. 2016), *https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.*

[118] *See* Fed. Trade Comm'n, *Cross-Device Tracking: An FTC Staff Report* (Jan. 2017), *https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.*

[119] *See* Fed. Trade Comm'n, *Mobile Privacy Disclosures: Building Trust Through Transparency: FTC Staff Report* (Feb. 2013), *https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.*

[120] *See* 15 U.S.C. 46(b). The Commission's recent report on broadband service providers is an example. Press Release, Fed. Trade Comm'n, FTC Staff Report Finds Many internet Service Providers Collect Troves of Personal Data, Users Have Few Options to Restrict Use (Oct 21, 2021), *https://www.ftc.gov/news-events/press-releases/2021/10/ftc-staff-report-finds-many-internet-service-providers-collect.* The Commission also recently commenced a Section 6(b) inquiry into social media companies. *See* Business Blog, Fed. Trade Comm'n, *FTC issues 6(b) orders to social media and video streaming services* (Dec. 14, 2020), *https://www.ftc.gov/news-events/blogs/business-blog/2020/12/ftc-issues-6b-orders-social-media-video-streaming-services.* Past Section 6(b) inquiries related to data privacy or security issues include those involving mobile security updates and the practices of data brokers. *See* Press Release, FTC Recommends Steps to Improve Mobile Device Security Update Practices (Feb. 28, 2018), *https://www.ftc.gov/news-events/press-releases/2018/02/ftc-recommends-steps-improve-mobile-device-security-update;* Press Release, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information (May 27, 2014), *https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more.*

[121] *See, e.g.,* 15 U.S.C. 53, 57b. *See also* Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC Act's Penalty Offense Authority,* 170 U. Pa. L. Rev. 71 (2021) (arguing that the Commission should provide whole industries notice of practices that the FTC has declared unfair or deceptive in litigated cease-and-desist orders in order to increase deterrence by creating a basis for the Commission to seek civil penalties pursuant to section 5(m)(1)(B) of the FTC Act against those that engage in such practices with knowledge that they are unfair or deceptive).

[122] Typically, in order to obtain civil monetary penalties under the FTC Act, the Commission must find that a respondent has violated a previously entered cease-and-desist order and then must bring a subsequent enforcement action for a violation of that order. *See* 15 U.S.C. 45(*l*).

[123] *See* 15 U.S.C. 45(m).

[124] The Supreme Court recently held, in *AMG Capital Management, LLC* v. *FTC,* 141 S. Ct. 1341 (2021), that Section 13(b) of the FTC Act, 15 U.S.C. 53(b), does not allow the FTC to obtain equitable monetary relief in federal court for violations of Section 5. This has left Section 19, 15 U.S.C. 57b—which requires evidence of fraudulent or dishonest conduct—as the only avenue for the Commission to obtain financial redress for consumers.

[125] *See generally* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms,* 102 B.U. L. Rev. 793 (2022).

hard to discern in the near term,[126] but are potentially no less unfair or deceptive.

Finally, the Commission's limited resources today can make it challenging to investigate and act on the extensive public reporting on data security practices that may violate Section 5, especially given how digitized and networked all aspects of the economy are becoming. A trade regulation rule could provide clarity and predictability about the statute's application to existing and emergent commercial surveillance and data security practices that, given institutional constraints, may be hard to equal or keep up with, case-by-case.[127]

IV. Questions

The commercial surveillance and lax data security practices that this ANPR describes above are only a sample of what the Commission's enforcement actions, news reporting, and published research have revealed. Here, in this Item, the Commission invites public comment on (a) the nature and prevalence of harmful commercial surveillance and lax data security practices, (b) the balance of costs and countervailing benefits of such practices for consumers and competition, as well as the costs and benefits of any given potential trade regulation rule, and (c) proposals for protecting consumers from harmful and prevalent commercial surveillance and lax data security practices.

This ANPR does not identify the full scope of potential approaches the Commission might ultimately undertake by rule or otherwise. It does not delineate a boundary on the issues on which the public may submit comments. Nor does it constrain the actions the Commission might pursue in an NPRM or final rule. The Commission invites comment on all potential rules, including those currently in force in foreign jurisdictions, individual U.S. states, and other legal jurisdictions.[128]

Given the significant interest this proceeding is likely to generate, and in order to facilitate an efficient review of submissions, the Commission encourages but does not require commenters to (1) submit a short Executive Summary of no more than three single-spaced pages at the beginning of all comments, (2) provide supporting material, including empirical data, findings, and analysis in published reports or studies by established news organizations and research institutions, (3) consistent with the questions below, describe the relative benefits and costs of their recommended approach, (4) refer to the numbered question(s) to which the comment is addressed, and (5) tie their recommendations to specific commercial surveillance and lax data security practices.

a. To what extent do commercial surveillance practices or lax security measures harm consumers?

This ANPR has alluded to only a fraction of the potential consumer harms arising from lax data security or commercial surveillance practices, including those concerning physical security, economic injury, psychological harm, reputational injury, and unwanted intrusion.

1. Which practices do companies use to surveil consumers?

2. Which measures do companies use to protect consumer data?

3. Which of these measures or practices are prevalent? Are some practices more prevalent in some sectors than in others?

4. How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?

5. Are there some harms that consumers may not easily discern or identify? Which are they?

6. Are there some harms that consumers may not easily quantify or measure? Which are they?

7. How should the Commission identify and evaluate these commercial surveillance harms or potential harms? On which evidence or measures should the Commission rely to substantiate its claims of harm or risk of harm?

8. Which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions?

9. Has the Commission adequately addressed indirect pecuniary harms, including potential physical harms, psychological harms, reputational injuries, and unwanted intrusions?

10. Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?

11. Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and business models more likely to protect consumers than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?

12. Lax data security measures and harmful commercial surveillance injure different kinds of consumers (*e.g.,* young people, workers, franchisees, small businesses, women, victims of stalking or domestic violence, racial minorities, the elderly) in different sectors (*e.g.,* health, finance, employment) or in different segments or ''stacks'' of the internet economy. For example, harms arising from data security breaches in finance or healthcare may be different from those concerning discriminatory advertising on social media which may be different from those involving education technology. How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors? Which commercial surveillance practices, if any, are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them? To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?

b. To what extent do commercial surveillance practices or lax data security measures harm children, including teenagers?

13. The Commission here invites comment on commercial surveillance practices or lax data security measures that affect children, including teenagers. Are there practices or measures to which children or teenagers are particularly vulnerable or susceptible? For instance, are children and teenagers more likely than adults to be manipulated by practices designed to

[126] *See generally* Alicia Solow-Niederman, *Information Privacy and the Inference Economy,* 117 Nw. U. L. Rev. 1, 27–38 (forthcoming 2022; cited with permission from author) (currently available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3921003*).

[127] The Commission is wary of committing now, even preliminarily, to any regulatory approach without public comment given the reported scope of commercial surveillance practices. The FTC Act, however, requires the Commission to identify ''possible regulatory alternatives under consideration'' in this ANPR. 15 U.S.C. 57a(b)(2)(A)(i). Thus, in Item IV below, this ANPR touches on a variety of potential regulatory interventions, including, among others, restrictions on certain practices in certain industries, disclosure, and notice requirements.

[128] The Commission is currently undertaking its regular periodic review of current COPPA enforcement and rules. *See* Fed. Trade Comm'n, Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 FR 35842 (July 25, 2019), *https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online.* Nothing in this ANPR displaces or supersedes that proceeding.

encourage the sharing of personal information?

14. What types of commercial surveillance practices involving children and teens' data are most concerning? For instance, given the reputational harms that teenagers may be characteristically less capable of anticipating than adults, to what extent should new trade regulation rules provide teenagers with an erasure mechanism in a similar way that COPPA provides for children under 13? Which measures beyond those required under COPPA would best protect children, including teenagers, from harmful commercial surveillance practices?

15. In what circumstances, if any, is a company's failure to provide children and teenagers with privacy protections, such as not providing privacy-protective settings by default, an unfair practice, even if the site or service is not targeted to minors? For example, should services that collect information from large numbers of children be required to provide them enhanced privacy protections regardless of whether the services are directed to them? Should services that do not target children and teenagers be required to take steps to determine the age of their users and provide additional protections for minors?

16. Which sites or services, if any, implement child-protective measures or settings even if they do not direct their content to children and teenagers?

17. Do techniques that manipulate consumers into prolonging online activity (*e.g.,* video autoplay, infinite or endless scroll, quantified public popularity) facilitate commercial surveillance of children and teenagers? If so, how? In which circumstances, if any, are a company's use of those techniques on children and teenagers an unfair practice? For example, is it an unfair or deceptive practice when a company uses these techniques despite evidence or research linking them to clinical depression, anxiety, eating disorders, or suicidal ideation among children and teenagers?

18. To what extent should trade regulation rules distinguish between different age groups among children (*e.g.,* 13 to 15, 16 to 17, etc.)?

19. Given the lack of clarity about the workings of commercial surveillance behind the screen or display, is parental consent an efficacious way of ensuring child online privacy? Which other protections or mechanisms, if any, should the Commission consider?

20. How extensive is the business-to-business market for children and teens' data? In this vein, should new trade regulation rules set out clear limits on transferring, sharing, or monetizing children and teens' personal information?

21. Should companies limit their uses of the information that they collect to the specific services for which children and teenagers or their parents sign up? Should new rules set out clear limits on personalized advertising to children and teenagers irrespective of parental consent? If so, on what basis? What harms stem from personalized advertising to children? What, if any, are the prevalent unfair or deceptive practices that result from personalized advertising to children and teenagers?

22. Should new rules impose differing obligations to protect information collected from children depending on the risks of the particular collection practices?

23. How would potential rules that block or otherwise help to stem the spread of child sexual abuse material, including content-matching techniques, otherwise affect consumer privacy?

c. How should the Commission balance costs and benefits?

24. The Commission invites comment on the relative costs and benefits of any current practice, as well as those for any responsive regulation. How should the Commission engage in this balancing in the context of commercial surveillance and data security? Which variables or outcomes should it consider in such an accounting? Which variables or outcomes are salient but hard to quantify as a material cost or benefit? How should the Commission ensure adequate weight is given to costs and benefits that are hard to quantify?

25. What is the right time horizon for evaluating the relative costs and benefits of existing or emergent commercial surveillance and data security practices? What is the right time horizon for evaluating the relative benefits and costs of regulation?

26. To what extent would any given new trade regulation rule on data security or commercial surveillance impede or enhance innovation? To what extent would such rules enhance or impede the development of certain kinds of products, services, and applications over others?

27. Would any given new trade regulation rule on data security or commercial surveillance impede or enhance competition? Would any given rule entrench the potential dominance of one company or set of companies in ways that impede competition? If so, how and to what extent?

28. Should the analysis of cost and benefits differ in the context of information about children? If so, how?

29. What are the benefits or costs of refraining from promulgating new rules on commercial surveillance or data security?

d. How, if at all, should the Commission regulate harmful commercial surveillance or data security practices that are prevalent?

i. Rulemaking Generally

30. Should the Commission pursue a Section 18 rulemaking on commercial surveillance and data security? To what extent are existing legal authorities and extralegal measures, including self-regulation, sufficient? To what extent, if at all, are self-regulatory principles effective?

ii. Data Security

31. Should the Commission commence a Section 18 rulemaking on data security? The Commission specifically seeks comment on how potential new trade regulation rules could require or help incentivize reasonable data security.

32. Should, for example, new rules require businesses to implement administrative, technical, and physical data security measures, including encryption techniques, to protect against risks to the security, confidentiality, or integrity of covered data? If so, which measures? How granular should such measures be? Is there evidence of any impediments to implementing such measures?

33. Should new rules codify the prohibition on deceptive claims about consumer data security, accordingly authorizing the Commission to seek civil penalties for first-time violations?

34. Do the data security requirements under COPPA or the GLBA Safeguards Rule offer any constructive guidance for a more general trade regulation rule on data security across sectors or in other specific sectors?

35. Should the Commission take into account other laws at the state and federal level (*e.g.,* COPPA) that already include data security requirements. If so, how? Should the Commission take into account other governments' requirements as to data security (*e.g.,* GDPR). If so, how?

36. To what extent, if at all, should the Commission require firms to certify that their data practices meet clear security standards? If so, who should set those standards, the FTC or a third-party entity?

iii. Collection, Use, Retention, and Transfer of Consumer Data

37. How do companies collect consumers' biometric information? What kinds of biometric information do companies collect? For what purposes do they collect and use it? Are consumers typically aware of that collection and use? What are the benefits and harms of these practices?

38. Should the Commission consider limiting commercial surveillance practices that use or facilitate the use of facial recognition, fingerprinting, or other biometric technologies? If so, how?

39. To what extent, if at all, should the Commission limit companies that provide any specifically enumerated services (*e.g.,* finance, healthcare, search, or social media) from owning or operating a business that engages in any specific commercial surveillance practices like personalized or targeted advertising? If so, how? What would the relative costs and benefits of such a rule be, given that consumers generally pay zero dollars for services that are financed through advertising?

40. How accurate are the metrics on which internet companies rely to justify the rates that they charge to third-party advertisers? To what extent, if at all, should new rules limit targeted advertising and other commercial surveillance practices beyond the limitations already imposed by civil rights laws? If so, how? To what extent would such rules harm consumers, burden companies, stifle innovation or competition, or chill the distribution of lawful content?

41. To what alternative advertising practices, if any, would companies turn in the event new rules somehow limit first- or third-party targeting?

42. How cost-effective is contextual advertising as compared to targeted advertising?

43. To what extent, if at all, should new trade regulation rules impose limitations on companies' collection, use, and retention of consumer data? Should they, for example, institute data minimization requirements or purpose limitations, *i.e.,* limit companies from collecting, retaining, using, or transferring consumer data beyond a certain predefined point? Or, similarly, should they require companies to collect, retain, use, or transfer consumer data only to the extent necessary to deliver the specific service that a given individual consumer explicitly seeks or those that are compatible with that specific service? If so, how? How should it determine or define which uses are compatible? How, moreover, could the Commission discern which data are relevant to achieving certain purposes and no more?

44. By contrast, should new trade regulation rules restrict the period of time that companies collect or retain consumer data, irrespective of the different purposes to which it puts that data? If so, how should such rules define the relevant period?

45. Pursuant to a purpose limitation rule, how, if at all, should the Commission discern whether data that consumers give for one purpose has been only used for that specified purpose? To what extent, moreover, should the Commission permit use of consumer data that is compatible with, but distinct from, the purpose for which consumers explicitly give their data?

46. Or should new rules impose data minimization or purpose limitations only for certain designated practices or services? Should, for example, the Commission impose limits on data use for essential services such as finance, healthcare, or search—that is, should it restrict companies that provide these services from using, retaining, or transferring consumer data for any other service or commercial endeavor? If so, how?

47. To what extent would data minimization requirements or purpose limitations protect consumer data security?

48. To what extent would data minimization requirements or purpose limitations unduly hamper algorithmic decision-making or other algorithmic learning-based processes or techniques? To what extent would the benefits of a data minimization or purpose limitation rule be out of proportion to the potential harms to consumers and companies of such a rule?

49. How administrable are data minimization requirements or purpose limitations given the scale of commercial surveillance practices, information asymmetries, and the institutional resources such rules would require the Commission to deploy to ensure compliance? What do other jurisdictions have to teach about their relative effectiveness?

50. What would be the effect of data minimization or purpose limitations on consumers' ability to access services or content for which they are not currently charged out of pocket? Conversely, which costs, if any, would consumers bear if the Commission does not impose any such restrictions?

51. To what extent, if at all, should the Commission require firms to certify that their commercial surveillance practices meet clear standards concerning collection, use, retention, transfer, or monetization of consumer data? If promulgated, who should set those standards: the FTC, a third-party organization, or some other entity?

52. To what extent, if at all, do firms that now, by default, enable consumers to block other firms' use of cookies and other persistent identifiers impede competition? To what extent do such measures protect consumer privacy, if at all? Should new trade regulation rules forbid the practice by, for example, requiring a form of interoperability or access to consumer data? Or should they permit or incentivize companies to limit other firms' access to their consumers' data? How would such rules interact with general concerns and potential remedies discussed elsewhere in this ANPR?

iv. Automated Decision-Making Systems

53. How prevalent is algorithmic error? To what extent is algorithmic error inevitable? If it is inevitable, what are the benefits and costs of allowing companies to employ automated decision-making systems in critical areas, such as housing, credit, and employment? To what extent can companies mitigate algorithmic error in the absence of new trade regulation rules?

54. What are the best ways to measure algorithmic error? Is it more pronounced or happening with more frequency in some sectors than others?

55. Does the weight that companies give to the outputs of automated decision-making systems overstate their reliability? If so, does that have the potential to lead to greater consumer harm when there are algorithmic errors?

56. To what extent, if at all, should new rules require companies to take specific steps to prevent algorithmic errors? If so, which steps? To what extent, if at all, should the Commission require firms to evaluate and certify that their reliance on automated decision-making meets clear standards concerning accuracy, validity, reliability, or error? If so, how? Who should set those standards, the FTC or a third-party entity? Or should new rules require businesses to evaluate and certify that the accuracy, validity, or reliability of their commercial surveillance practices are in accordance with their own published business policies?

57. To what extent, if at all, do consumers benefit from automated decision-making systems? Who is most likely to benefit? Who is most likely to be harmed or disadvantaged? To what extent do such practices violate Section 5 of the FTC Act?

58. Could new rules help ensure that firms' automated decision-making practices better protect non-English speaking communities from fraud and abusive data practices? If so, how?

59. If new rules restrict certain automated decision-making practices, which alternatives, if any, would take their place? Would these alternative techniques be less prone to error than the automated decision-making they replace?

60. To what extent, if at all, should new rules forbid or limit the development, design, and use of automated decision-making systems that generate or otherwise facilitate outcomes that violate Section 5 of the FTC Act? Should such rules apply economy-wide or only in some sectors? If the latter, which ones? Should these rules be structured differently depending on the sector? If so, how?

61. What would be the effect of restrictions on automated decision-making in product access, product features, product quality, or pricing? To what alternative forms of pricing would companies turn, if any?

62. Which, if any, legal theories would support limits on the use of automated systems in targeted advertising given potential constitutional or other legal challenges?

63. To what extent, if at all, does the First Amendment bar or not bar the Commission from promulgating or enforcing rules concerning the ways in which companies personalize services or deliver targeted advertisements?

64. To what extent, if at all, does Section 230 of the Communications Act, 47 U.S.C. 230, bar the Commission from promulgating or enforcing rules concerning the ways in which companies use automated decision-making systems to, among other things, personalize services or deliver targeted advertisements?

v. Discrimination Based on Protected Categories

65. How prevalent is algorithmic discrimination based on protected categories such as race, sex, and age? Is such discrimination more pronounced in some sectors than others? If so, which ones?

66. How should the Commission evaluate or measure algorithmic discrimination? How does algorithmic discrimination affect consumers, directly and indirectly? To what extent, if at all, does algorithmic discrimination stifle innovation or competition?

67. How should the Commission address such algorithmic discrimination? Should it consider new trade regulation rules that bar or somehow limit the deployment of any system that produces discrimination, irrespective of the data or processes on which those outcomes are based? If so, which standards should the Commission use to measure or evaluate disparate outcomes? How should the Commission analyze discrimination based on proxies for protected categories? How should the Commission analyze discrimination when more than one protected category is implicated (*e.g.,* pregnant veteran or Black woman)?

68. Should the Commission focus on harms based on protected classes? Should the Commission consider harms to other underserved groups that current law does not recognize as protected from discrimination (*e.g.,* unhoused people or residents of rural communities)?

69. Should the Commission consider new rules on algorithmic discrimination in areas where Congress has already explicitly legislated, such as housing, employment, labor, and consumer finance? Or should the Commission consider such rules addressing all sectors?

70. How, if at all, would restrictions on discrimination by automated decision-making systems based on protected categories affect all consumers?

71. To what extent, if at all, may the Commission rely on its unfairness authority under Section 5 to promulgate antidiscrimination rules? Should it? How, if at all, should antidiscrimination doctrine in other sectors or federal statutes relate to new rules?

72. How can the Commission's expertise and authorities complement those of other civil rights agencies? How might a new rule ensure space for interagency collaboration?

vi. Consumer Consent

73. The Commission invites comment on the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices. Given the reported scale, opacity, and pervasiveness of existing commercial surveillance today, to what extent is consumer consent an effective way of evaluating whether a practice is unfair or deceptive? How should the Commission evaluate its effectiveness?

74. In which circumstances, if any, is consumer consent likely to be effective? Which factors, if any, determine whether consumer consent is effective?

75. To what extent does current law prohibit commercial surveillance practices, irrespective of whether consumers consent to them?

76. To what extent should new trade regulation rules prohibit certain specific commercial surveillance practices, irrespective of whether consumers consent to them?

77. To what extent should new trade regulation rules require firms to give consumers the choice of whether to be subject to commercial surveillance? To what extent should new trade regulation rules give consumers the choice of withdrawing their duly given prior consent? How demonstrable or substantial must consumer consent be if it is to remain a useful way of evaluating whether a commercial surveillance practice is unfair or deceptive? How should the Commission evaluate whether consumer consent is meaningful enough?

78. What would be the effects on consumers of a rule that required firms to give consumers the choice of being subject to commercial surveillance or withdrawing that consent? When or how often should any given company offer consumers the choice? And for which practices should companies provide these options, if not all?

79. Should the Commission require different consent standards for different consumer groups (*e.g.,* parents of teenagers (as opposed to parents of pre-teens), elderly individuals, individuals in crisis or otherwise especially vulnerable to deception)?

80. Have opt-out choices proved effective in protecting against commercial surveillance? If so, how and in what contexts?

81. Should new trade regulation rules require companies to give consumers the choice of opting out of all or certain limited commercial surveillance practices? If so, for which practices or purposes should the provision of an opt-out choice be required? For example, to what extent should new rules require that consumers have the choice of opting out of all personalized or targeted advertising?

82. How, if at all, should the Commission require companies to recognize or abide by each consumer's respective choice about opting out of commercial surveillance practices—whether it be for all commercial surveillance practices or just some? How would any such rule affect consumers, given that they do not all have the same preference for the amount or kinds of personal information that they share?

vii. Notice, Transparency, and Disclosure

83. To what extent should the Commission consider rules that require companies to make information

available about their commercial surveillance practices? What kinds of information should new trade regulation rules require companies to make available and in what form?

84. In which contexts are transparency or disclosure requirements effective? In which contexts are they less effective?

85. Which, if any, mechanisms should the Commission use to require or incentivize companies to be forthcoming? Which, if any, mechanisms should the Commission use to verify the sufficiency, accuracy, or authenticity of the information that companies provide?

a. What are the mechanisms for opacity?

86. The Commission invites comment on the nature of the opacity of different forms of commercial surveillance practices. On which technological or legal mechanisms do companies rely to shield their commercial surveillance practices from public scrutiny? Intellectual property protections, including trade secrets, for example, limit the involuntary public disclosure of the assets on which companies rely to deliver products, services, content, or advertisements. How should the Commission address, if at all, these potential limitations?

b. Who should administer notice or disclosure requirements?

87. To what extent should the Commission rely on third-party intermediaries (*e.g.,* government officials, journalists, academics, or auditors) to help facilitate new disclosure rules?

88. To what extent, moreover, should the Commission consider the proprietary or competitive interests of covered companies in deciding what role such third-party auditors or researchers should play in administering disclosure requirements?

c. What should companies provide notice of or disclose?

89. To what extent should trade regulation rules, if at all, require companies to explain (1) the data they use, (2) how they collect, retain, disclose, or transfer that data, (3) how they choose to implement any given automated decision-making system or process to analyze or process the data, including the consideration of alternative methods, (4) how they process or use that data to reach a decision, (5) whether they rely on a third-party vendor to make such decisions, (6) the impacts of their commercial surveillance practices, including disparities or other distributional outcomes among consumers, and (7) risk mitigation measures to address potential consumer harms?

90. Disclosures such as these might not be comprehensible to many audiences. Should new rules, if promulgated, require plain-spoken explanations? How effective could such explanations be, no matter how plain? To what extent, if at all, should new rules detail such requirements?

91. Disclosure requirements could vary depending on the nature of the service or potential for harm. A potential new trade regulation rule could, for example, require different kinds of disclosure tools depending on the nature of the data or practices at issue (*e.g.,* collection, retention, or transfer) or the sector (*e.g.,* consumer credit, housing, or work). Or the agency could impose transparency measures that require in-depth accounting (*e.g.,* impact assessments) or evaluation against externally developed standards (*e.g.,* third-party auditing). How, if at all, should the Commission implement and enforce such rules?

92. To what extent should the Commission, if at all, make regular self-reporting, third-party audits or assessments, or self-administered impact assessments about commercial surveillance practices a standing obligation? How frequently, if at all, should the Commission require companies to disclose such materials publicly? If it is not a standing obligation, what should trigger the publication of such materials?

93. To what extent do companies have the capacity to provide any of the above information? Given the potential cost of such disclosure requirements, should trade regulation rules exempt certain companies due to their size or the nature of the consumer data at issue?

viii. Remedies

94. How should the FTC's authority to implement remedies under the Act determine the form or substance of any potential new trade regulation rules on commercial surveillance? Should new rules enumerate specific forms of relief or damages that are not explicit in the FTC Act but that are within the Commission's authority? For example, should a potential new trade regulation rule on commercial surveillance explicitly identify algorithmic disgorgement, a remedy that forbids companies from profiting from unlawful practices related to their use of automated systems, as a potential remedy? Which, if any, other remedial tools should new trade regulation rules on commercial surveillance explicitly identify? Is there a limit to the Commission's authority to implement remedies by regulation?

ix. Obsolescence

95. The Commission is alert to the potential obsolescence of any rulemaking. As important as targeted advertising is to today's internet economy, for example, it is possible that its role may wane. Companies and other stakeholders are exploring new business models.[129] Such changes would have notable collateral consequences for companies that have come to rely on the third-party advertising model, including and especially news publishing. These developments in online advertising marketplace are just one example. How should the Commission account for changes in business models in advertising as well as other commercial surveillance practices?

V. Comment Submissions

You can file a comment online or on paper. For the Commission to consider your comment, it must receive it on or before October 21, 2022. Write ''Commercial Surveillance ANPR, R111004'' on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website. The Commission strongly encourages you to submit your comments online through the *https://www.regulations.gov* website. To ensure the Commission considers your online comment, please follow the instructions on the web-based form.

If you file your comment on paper, write ''Commercial Surveillance ANPR, R111004'' on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC–5610 (Annex B), Washington, DC 20580.

Because your comment will be placed on the public record, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not contain sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number or foreign country equivalent; passport number; financial

[129] *See, e.g.,* Brian X. Chen, *The Battle for Digital Privacy Is Reshaping the internet,* N.Y. Times (Sept. 16, 2021), *https://www.nytimes.com/2021/09/16/technology/digital-privacy.html.*

account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any ''[t]rade secret or any commercial or financial information which . . . is privileged or confidential''—as provided in Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled ''Confidential,'' and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted publicly at *https://www.regulations.gov*-as legally required by FTC Rule 4.9(b)—we cannot redact or remove your comment, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC website to read this document and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments it receives on or before October 21, 2022. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy.*

VI. The Public Forum

The Commission will hold a public forum on Thursday, September 8, 2022, from 2 p.m. until 7:30 p.m. eastern time. In light of the ongoing COVID–19 pandemic, the forum will be held virtually, and members of the public are encouraged to attend virtually by visiting *https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum.* The public forum will address in greater depth the topics that are the subject of this document as well as the rulemaking process with a goal of facilitating broad public participation in response to this ANPR and any future rulemaking proceedings the Commission undertakes. A complete agenda will be posted at the aforementioned website and announced in a press release at a future date. Individuals or entities that would like to participate in the public forum by offering two-minute public remarks, should email *Sept8testimony@ftc.gov.* Please note that this email is only for requests to participate in the public forum and is not a means of submitting comments in response to this ANPR. Please see Item V above for instructions on submitting public comments.

Forum panelists will be selected by FTC staff, and public remarks are first come, first serve. The Commission will place a recording of the proceeding on the public record. Requests to participate in the public remarks must be received on or before August 31, 2022. Individuals or entities selected to participate will be notified on or before September 2, 2022. Because disclosing sources of funding promotes transparency, ensures objectivity, and maintains the public's trust, prospective participants, if chosen, will be required to disclose the source of any support they received in connection with participation at the forum. This funding information will be included in the published biographies as part of the forum record.

By direction of the Commission.

Joel Christie,

Acting Secretary.

Note: The following statements will not appear in the Code of Federal Regulations:

Statement of Chair Lina M. Khan

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 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 potentially unlawful practices may be prevalent, with case-by-case enforcement failing to adequately deter lawbreaking or remedy the resulting harms.

[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.*

[4] *See* Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, __FR__§ 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.*

Indeed, a significant majority of Americans today feel 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 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 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.

[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.'').

The fact that current data practices can have such consequential effects heightens both the importance of wielding the full set of tools 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 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 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 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 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 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

[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.*

[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 section IV(b) Q.21; ANPR at section IV(d) Q.43; ANPR at section IV(d) Q.48.

[15] ANPR at section IV(d) Q.76.

we best ensure that any rules we pursue can be easily and efficiently administered and that these rules do not rest on determinations we are not well positioned to make or commitments 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 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]

• Workplace surveillance: Reports suggest 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.

Statement of Commissioner Rebecca Kelly Slaughter

Three years ago, I gave a speech outlining: why I believed that case-by-case enforcement in the space of data abuses was not effective; how I hoped to see Congress pass a long-overdue federal privacy law; and that, until such a law is signed, the Commission should use its authority under Section 18 to initiate a rulemaking process.[1] I am delighted that Congress appears to be making substantial and unprecedented progress toward a meaningful privacy law, which I am eager to see pass.[2] Nonetheless, given the uncertainty of the legislative process and the time a Section 18 rulemaking necessarily takes, the Commission should not wait any longer than it already has to develop a public record that could support enforceable rules. So I am equally delighted that we are now beginning the Section 18 process by issuing this advance notice of proposed rulemaking (''ANPR'') on commercial surveillance and data security.[3]

It is indisputable that the Federal Trade Commission has expertise in regulating this sector; it is widely recognized as the nation's premier ''privacy enforcer.'' [4] I commend agency staff for their dogged application of our nearly 100-year-old consumer-protection statute (and handful of sector-specific privacy laws) to build that reputation.

Historically, much of that work operated through the straightforward application of those basic consumer-protection principles to privacy. The FTC ensured that companies told users what they were doing with the users' data, insisted that they secure users' consent, and policed companies' promises. But case-by-case enforcement has not systemically deterred unlawful behavior in this market. As our own reports make clear, the prevailing notice-and-choice regime has failed to protect users,[5] and the modes by which sensitive information can be discovered,

[16] ANPR at section IV(d) Q.49.

[17] ANPR at section IV(a) Q.11.

[18] ANPR at section 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 section 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-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 section 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 sections 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.*

[1] *See* Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law,* Silicon Flatirons-University of Colorado Law School (Sept. 6, 2019), *https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf.*

[2] *See* Rebecca Klar, *House Panel Advances Landmark Federal Data Privacy Bill,* The Hill (July 20, 2022), *https://thehill.com/policy/technology/3567822-house-panel-advances-landmark-federal-data-privacy-bill/.*

[3] Fed. Trade Comm'n, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 FR (forthcoming 2022) [hereinafter ''ANPR''].

[4] When Congress passed the Children's Online Privacy Protection Act (''COPPA'') in 1998 it assigned sector-specific privacy enforcement and rulemaking powers to the FTC on top of our UDAP authority. Bills being debated in both House and Senate Commerce Committees build on our ''comparative expertise'' in this field and seek to streamline and enhance our privacy enforcement and rulemaking processes. *See West Virginia* v. *EPA,* 142 S. Ct. 2587, 2613 (2022) ('''When an agency has no comparative expertise' in making certain policy judgments, we have said, 'Congress presumably would not' task it with doing so.'' (quoting *Kisor* v. *Wilkie,* 139 S. Ct. 2400, 2417 (2019))).

[5] An FTC staff 6(b) study on ISP privacy uncovered that companies routinely bury important disclosures in endless terms-of-service and that choice, even when purportedly offered, is ''illusory.'' Fed. Trade Comm'n, *A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major internet Service Providers* 27 (Oct. 21, 2021), *https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-youexamining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.*

derived, and disclosed have only grown in number and complexity.[6]

Data abuses such as surreptitious biometric or location tracking,[7] unaccountable and discriminatory algorithmic decision-making,[8] or lax data security practices [9] have been either caused by, exacerbated by, or are in service of nearly unfettered commercial data collection, retention, use, and sharing. It is up to the Commission to use the tools Congress explicitly gave us, however rusty we are at wielding them, to prevent these unlawful practices. That is why I have consistently, for years, called for the Commission to begin the process to consider clear, bright-line rules against unfair or deceptive data practices pursuant to our Section 18 authority.[10]

Section 18 rulemaking's virtue lies in being open, iterative, and public. By the same token it is, by congressional design, laborious and time-consuming. But we intend to follow the record where it leads and, if appropriate, issue Trade Regulation Rules to proscribe unlawful conduct. The Commission has proactively taken steps to use this authority as Congress directed. During my time as Acting Chair, we created a Rulemaking Group within the Office of General Counsel, which has already been indispensable in building the agency's capacity during this process.[11] Working with that Group, the Commission updated our Rules of Practice to enhance transparency and shed self-imposed roadblocks to avoid unnecessary and costly delay in these proceedings.[12]

As happy as I am to see us finally take this first step of opening this record, it is not something I take lightly. An initiative like this entails some risk, though I believe further inaction does as well. I have heard arguments, including from my fellow Commissioners, that conducting a rulemaking in the data space is inappropriate, either because Congress is currently debating privacy legislation or even because the topic is simply too consequential or the issues too vast for the Commission to appropriately address. In this statement, I challenge some of these assumptions and then raise some of the issues in which I am especially interested.

On Timing

The best time to initiate this lengthy process was years ago, but the second-best time is now. Effective nationwide rules governing the collection and use of data are long overdue. As the nation's principal consumer-protection agency, we have a responsibility to act.

Restoring Effective Deterrence

The question of effective enforcement is central to this proceeding. Case-by-case enforcement, while once considered a prudent expression of our statutory authority, has not proved effective at deterring illegal conduct in the data space. Trade Regulation Rules can help remedy this problem by providing clear and specific guidance about what conduct the law proscribes and attaching financial consequences to violations of the law.

Providing a financial penalty for first-time lawbreaking is now, in the wake of the loss of our Section 13(b) authority, a particular necessity. Last year, the Supreme Court ruled that we can no longer seek monetary relief in federal court for violations of the FTC Act under our 13(b) authority.[13] I have testified in Congress that the loss of this authority is devastating for consumers who now face a significantly steeper uphill battle to be made whole after suffering a financial injury stemming from illegal conduct.[14] But the loss of 13(b) also hampers our ability to deter unlawful conduct in the first place. In its absence, and without a statutory fix, first-time violators of the FTC Act are unlikely to face monetary consequences for their unlawful practices.[15] Trade Regulation Rules enforced under

[6] *See* Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data,* Fed. Trade Comm'n (July 11, 2022), *https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use* (''Smartphones, connected cars, wearable fitness trackers, ''smart home'' products, and even the browser you're reading this on are capable of directly observing or deriving sensitive information about users.'').

[7] *See, e.g., Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission,* FTC (June 22, 2016), *https://www.ftc.gov/newsevents/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.*

[8] *See, e.g.,* Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI* (Apr. 19, 2021), *https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.*

[9] *See, e.g.,* Press Release, *FTC Finalizes Action Against CafePress for Covering Up Data Breach, Lax Security* (June 24, 2022), *https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-finalizes-action-against-cafepress-covering-data-breach-lax-security-0.*

[10] *See, e.g.,* Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law,* Silicon Flatirons-University of Colorado Law School, (Sept. 6, 2019) *https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf; Remarks of Commissioner Rebecca Kelly Slaughter on Algorithms and Economic Justice,* UCLA School of Law (Jan. 24, 2020), *https://www.ftc.gov/system/files/documents/public_statements/1564883/remarks_of_commissioner_rebecca_kelly_slaughter_on_algorithmic_and_economic_justice_01-24-2020.pdf; Opening Statement of Commissioner Rebecca Kelly Slaughter,* United States Senate Committee on Commerce, Science, and Transportation Hearing on Oversight of the Federal Trade Commission (Aug. 5, 2020), *https://www.ftc.gov/system/files/documents/public_statements/1578979/opening_statement_of_commissioner_rebecca_slaughter_senate_commerce_oversight_hearing.pdf; FTC Data Privacy Enforcement: A Time of Change,* N.Y.U. School of Law (Oct. 16, 2020), *https://www.ftc.gov/system/files/documents/public_statements/1581786/slaughter_-_remarks_on_ftc_data_privacy_enforcement_-_a_time_of_change.pdf; Protecting Consumer Privacy in a Time of Crisis,* Future of Privacy Forum, (Feb. 10, 2021) *https://www.ftc.gov/system/files/documents/public_statements/1587283/fpf_opening_remarks_210_.pdf; Keynote Remarks of FTC Acting Chairwoman Rebecca Kelly Slaughter,* Consumer Federation of America's Virtual Consumer Assembly (May 4, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1589607/keynote-remarks-acting-chairwoman-rebecca-kelly-slaughte-cfa-virtual-consumer-assembly.pdf;* Rebecca Kelly Slaughter, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission,* Yale J. L. & Tech. (Aug. 2021), *https://yjolt.org/sites/default/files/23_yale_j.l._tech._special_issue_1.pdf; Statement of Rebecca Kelly Slaughter Regarding the Report to Congress on Privacy and Security* (Oct. 1, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1597012/rks_statement_on_privacy_report_final.pdf; Disputing the Dogmas of Surveillance Advertising,* National Advertising Division (Oct. 1, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1597050/commissioner_slaughter_national_advertising_division_10-1-2021_keynote_address.pdf; Wait But Why? Rethinking Assumptions About Surveillance Advertising,* IAPP Privacy Security Risk Keynote (Oct. 22, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1597998/iapp_psr_2021_102221_final2.pdf; NTIA Listening Session on Privacy, Equity, and Civil Rights Keynote Address of Commissioner Rebecca Kelly Slaughter,* NTIA, (Dec. 14, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1599831/slaughter-ntia-keynote.pdf.*

[11] Press Release, *FTC Acting Chairwoman Slaughter Announces New Rulemaking Group* (Mar. 25, 2021), *https://www.ftc.gov/news-events/news/press-releases/2021/03/ftc-acting-chairwoman-slaughter-announces-new-rulemaking-group.*

[12] Statement of Commissioner Rebecca Kelly Slaughter joined by Chair Lina Khan and Commissioner Rohit Chopra Regarding the Adoption of Revised Section 18 Rulemaking Procedures (July 1, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1591522/joint_rules_of_practice_statement_final_7121_1131am.pdf.*

[13] *AMG Cap. Mgmt., LLC* v. *FTC,* 141 S. Ct. 1341, 1347 (2021).

[14] Rebecca Kelly Slaughter, *Opening Statement of Acting Chairwoman Rebecca Kelly Slaughter [on] The Urgent Need to Fix Section 13(b) of the FTC Act,* United States House Committee on Energy and Commerce

Subcommittee on Consumer Protection and Commerce (Apr. 27, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1589456/opening_statement_april_27_house_13b_hearing_427.pdf.*

[15] *See* ANPR at 23 (''For instance, after a hacker steals personal consumer data from an inadequately secured database, an injunction stopping the conduct and requiring the business to take affirmative steps to improve its security going forward can help prevent future breaches but does not remediate the harm that has already occurred or is likely to occur.'').

Section 19 can enable such consequences.[16]

Rulemaking in the Time of ADPPA

For years, Congress has nibbled around the edges of comprehensive federal privacy legislation; it is now engaged in the advanced stages of consideration of such legislation. All members of the Commission have repeatedly called on Congress to act in this space. I have advocated for legislation that sets clear rules regarding data minimization, use restrictions, and secondary uses; that gives us the ability to seek civil penalties for law violations; that gives us flexible APA rulemaking authority so we can act swiftly to address new conduct; and most importantly gives the agency the resources to meaningfully enforce the law.

The House may be the closest it has been in years to seeing legislation like this reach the finish line.[17] I not only welcome it—I prefer Congressional action to strengthen our authority. But I know from personal experience that the road for a bill to become a law is not a straight or easy one.[18] In the absence of that legislation, and while Congress deliberates, we cannot sit idly by or press pause indefinitely on doing our jobs to the best of our ability. As I mentioned above, I believe that we have a duty to use the authorities Congress has already given us to prevent and address these unfair or deceptive practices how we best see fit.

I am certain that action by the Federal Trade Commission will not clip the wings of Congressional ambition. Our work here is complementary to Congress' efforts.[19] The bills supported by the leaders of both Commerce Committees empower the FTC to be a more effective privacy regulator,[20] as will the record we develop pursuant to this ANPR. Section 18 rulemaking, even more so than more common APA rulemaking, gives members of the public the opportunity to be active participants in the policy process. The open record will allow us to hear from ordinary people about the data economy harms they have experienced. We can begin to flex our regulatory muscle by evaluating which of those harms meet the statutory prohibitions on unfair or deceptive conduct and which of those are prevalent in the market. The study, public commentary, and dialogue this proceeding will launch can meaningfully inform any superseding rulemaking Congress eventually directs us to take as well as the Congressional debate should the current legislative progress stall.

Our Authority and the Scope of This Proceeding

Some have balked at this ANPR as overly ambitious for an agency that has not previously issued rules in this area, or as coloring outside the lines of our statute in the topics it addresses, especially in light of the Supreme Court decision in *West Virginia* v. *EPA.* But our authority is as unambiguous as it is limited, and so our regulatory ambit is rightfully constrained—the questions we ask in the ANPR and the rules we are empowered to issue may be consequential, but they do not implicate the ''major questions doctrine.'' [21]

Section 18 Rulemaking

In its grant of Section 18 rulemaking authority to the Commission in 1975 under the Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Congress explicitly empowered the FTC to ''define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce . . . .'' [22] Those terms, and therefore our delegated authority, are not defined by ''modest words,'' ''vague terms,'' ''subtle devices,'' or ''oblique or elliptical language.'' [23] Determining what acts ''in commerce'' are unfair or deceptive is central to our statutory mission and their meaning is prescribed by our statutes and nearly 100 years of judicial interpretation.

It is worth reiterating these standards, both as a matter of legal principle and as a note for those participating in this process. A ''deceptive'' act is one that (1) makes a ''representation, omission, or practice that is likely to mislead the consumer'' (2) who is ''acting reasonably in the circumstances'' and (3) is ''material,'' meaning it would ''affect the consumer's conduct or decision with regard to a product or service.'' [24]

Congress updated the FTC Act in 1994, adopting into statute the Commission's policy statement on ''unfairness.'' An act may be ''unfair'' and in violation of the FTC Act if that act (1) ''causes or is likely to cause substantial injury to consumers,'' (2) ''is not reasonably avoidable by consumers themselves,'' and (3) is not ''not outweighed by countervailing benefits to consumers or to competition.'' [25]

Even after finding that a practice is unfair or deceptive we face an additional hurdle to issuing a Notice of proposed rulemaking leading to a possible Trade Regulation Rule. We may issue proposed rules to prevent unfair or deceptive practices only if we find that such practices are ''prevalent.'' We can find a practice prevalent if the FTC has ''issued cease and desist orders regarding such acts or practices,'' or we can determine prevalence through ''any other information available to the Commission'' that ''indicates a widespread pattern of unfair or deceptive acts or practices.'' [26]

We cannot invent the law here. I want to underscore this. In this rulemaking we can address only unfair or deceptive practices that we could have otherwise found unlawful in the ordinary enforcement of our Section 5 authority on a case-by-case basis. But the purpose of Section 18 rulemaking is not merely to memorialize unlawful activity that we have already fully adjudicated.[27]

---

[16] In the course of removing our 13(b) equitable monetary relief authority, the Supreme Court admonished the Commission to stop complaining about the ''cumbersome'' Section 19 process and either use our authority in earnest, ask Congress for a fix, or both. *AMG Cap. Mgmt.,* 141 S. Ct. at 1352 (''Nothing we say today, however, prohibits the Commission from using its authority under § 5 and § 19 to obtain restitution on behalf of consumers. If the Commission believes that authority too cumbersome or otherwise inadequate, it is, of course, free to ask Congress to grant it further remedial authority.'').

[17] Gilad Eldman, *Don't Look Now, but Congress Might Pass an Actually Good Privacy Bill,* Wired (July 21, 2022), *https://www.wired.com/story/american-data-privacy-protection-act-adppa/.*

[18] *See* Margaret Harding McGill, *Online Privacy Bill Faces Daunting Roadblocks,* Axios (Aug. 4, 2022), *https://www.axios.com/2022/08/04/online-privacy-bill-roadblocks-congress.*

[19] A group of nine Senators wrote that these are ''parallel'' efforts and encouraged the Commission to ''take advantage of every took in its toolkit to protect consumers' privacy.'' Notably, a majority of these members have either introduced or cosponsored FTC-empowering privacy legislation. Senators Booker, Blumenthal, Coons, Luján, Markey, Klobuchar, Schatz, Warren, and Wyden, *2021.09.20 FTC Privacy Rulemaking* (Sept. 20, 2021), *https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf.*

[20] *See, e.g.,* American Data Privacy and Protection Act, H.R.8152, 117th Congress (2022); *See* Consumer Online Privacy Rights Act, S.3195, 117th Congress (2021).

[21] *West Virginia,* 142 S. Ct. at 2614 (2022) (''Given these circumstances [of a novel claim of authority by an agency] . . . the Government must—under the major questions doctrine—point to 'clear congressional authorization' to regulate in that manner.''). The FTC is exercising here, however, its central authority: to define unfair or deceptive acts or practices, as it has done in enforcement matters for nearly 100 years under Section 5 and in rulemaking under Section 18 for nearly 50.

[22] 15 U.S.C. 57a(a)(1)(B).

[23] *West Virginia,* 142 S. Ct. at 2609 (internal quotation marks omitted).

[24] FTC Policy Statement on Deception (Oct. 14, 1983), *appended to In re Cliffdale Assocs., Inc.,* 103 F.T.C. 110, 174 (1984), *https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.*

[25] 15 U.S.C. 45(n).

[26] 15 U.S.C. 57a(b)(3).

[27] In fact, we have a different statute for that process: our penalty offense authority. *See* Fed.

The ANPR allows us to look at harms systematically and address the root of that unlawful activity. The limiting principle for the scope of conduct we may regulate is the contours of the law itself: acts that are both deceptive or unfair *and* prevalent.

Scope of the ANPR

The scope of the ANPR is reflective of the broad set of issues that arise from unfettered commercial data collection and use. That a public inquiry into this market asks a wide range of questions—inquiring about issues like collection and consent, algorithms, ad-delivery, demographic data, engagement, and the ecosystem's effects on kids and teens—should not be surprising. This is broadly the same scope of issues the Commission is currently examining in our social media and video streaming study initiated under Chair Simons in 2020.[28]

I believe it is appropriate ask those questions, and more, in this ANPR. I expect that the record will alert us, and Congress, to widespread harms that may otherwise have not reached our attention. Some of those harms may be better addressed under our other sector-specific privacy authorities or under our competition authority. A holistic look at the data economy allows us to better understand the interplay between our consumer protection and competition missions and, should we get to that stage, propose better and more effective rules.

Are data abuse rules different?

Some have argued that this exercise of our rulemaking authority is permissible to address some unfair or deceptive practices in some other sector of the market but not this one.[29] The rules the agency has historically issued already touch hundreds of millions of Americans' lives. FTC rules cover business conduct in funerals,[30] the marketing of new opportunities to consumers,[31] the eyeglasses market,[32] and unfair credit practices.[33] These rules cover sectors with hundreds of billions in economic output. The Franchise Rule,[34] for example, helps govern the business conduct of a sector that employs over 8 million people and contributes over 3% to the country's GDP.[35] This is all to say that the ''bigness'' of an industry, or the potential significance of rulemaking in that industry, should have little bearing on the legal question about the scope of our authority.[36] As a policy matter, ''bigness,'' if anything, should compel extra scrutiny of business practices on our part, not a free pass, kid gloves, or a punt to Congress. Though their products and services touch all our lives, technology companies are not exempt from generally applicable laws. If we have the authority to police their business practices by case-by-case enforcement to protect the public from potentially unfair or deceptive practices, and we do, then we have the authority to examine how *ex ante* rules may also govern those practices.

Issues of Particular Interest

I want to encourage public participation in this comment period, especially from the voices we hear from less at the Commission. Having information in the record from a diverse set of communities and commenters will strengthen the record and help lay a firm foundation for potential agency action. I encourage the public to engage with all the issues we have teed up in the ANPR and to think about how commercial surveillance and abusive data practices affect them not only as consumers of products and services but also as workers, small business owners, and potential competitors to dominant firms.[37] I'm eager to see and evaluate the record in its entirety, but there are some issues I have had a particular interest in during my time at the Commission. I've highlighted some of them below.

Minimization and Purpose and Use Specifications

I have spoken at length about my interest in ideas around data minimization.[38] The ANPR asks several questions related to the concept, and I am eager to see comments about potentially unlawful practices in this area, the state of data collection in the industry, and how that relates to user expectations of the products or services on offer.[39]

Civil Rights, Vulnerable Populations, and Discriminatory Algorithms

Data abuses are a civil rights issue, and commercial surveillance can be especially harmful from a civil rights and equity perspective. The FTC's own reports have explored these issues for years.[40] The FTC's mission to protect consumers from unfair or deceptive practices in commerce must include examining how commercial practices affect the marginalized and vulnerable. Discrimination based on protected-class status is obviously unfair in the colloquial sense and may sometimes be unfair in Section 5 terms as well.[41] As I have written, failure to closely scrutinize the impact of data-driven decision-making tools can create discriminatory outcomes.[42] The ANPR

Trade Comm'n, *Notices of Penalty Offenses, https://www.ftc.gov/enforcement/penalty-offenses.*

[28] *See* Lesley Fair, *FTC issues 6(b) orders to social media and video streaming services* (Dec. 14, 2020), *https://www.ftc.gov/business-guidance/blog/2020/12/ftc-issues-6b-orders-social-media-and-video-streaming-services.*

[29] *See* Jordan Crenshaw, *Congress Should Write Privacy Rules, Not the FTC,* U.S. Chamber of Commerce (Sept. 17, 2021), *https://www.uschamber.com/technology/data-privacy/congress-should-write-privacy-rules-not-the-ftc.*

[30] 16 CFR part 453.

[31] 16 CFR part 437.

[32] 16 CFR part 456.

[33] 16 CFR part 444.

[34] 16 CFR part 436.

[35] *See* Int'l Francise Ass'n, *2022 Franchising Economic Outlook* (Feb. 15, 2022) *https://www.franchise.org/franchise-information/franchise-business-outlook/2022franchising-economic-outlook.*

[36] *West Virginia,* 142 S. Ct. at 2628 (Kagan, J., dissenting) (''A key reason Congress makes broad delegations . . . is so an agency can respond, appropriately and commensurately, to new and big problems. Congress knows what it doesn't and can't know when it drafts a statute; and Congress therefore gives an expert agency the power to address issues—even significant ones—as and when they arise.'').

[37] People are far more than simply consumers of products and services. Effective consumer protection has to think about people as workers and potential entrepreneurs too. *See* Statement of Commissioner Rebecca Kelly Slaughter Regarding Advance Notice of Proposed Rulemaking on the Use of Earnings Claims (Feb. 17, 2022), *https://www.ftc.gov/system/files/ftc_gov/pdf/RKS%20Earnings%20Claim%20Statement.pdf.*

[38] *See* Rebecca Kelly Slaughter, *Keynote Closing Remarks of Commissioner Rebecca Slaughter at IAPP 2021,* IAPP (Oct. 22, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597998/iapp_psr_2021_102221_final2.pdf.

[39] See ANPR at 31.

[40] See Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues, (Jan. 2016), *https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusionunderstanding-issues/160106big-data-rpt.pdf. See also* Fed. Trade Comm'n, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major internet Service Providers* (Oct. 21, 2021), *https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-youexamining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.*

[41] Commercial practices that discriminate against people based on their immutable characteristics neatly fit into Section 5's prohibitions. They may cause or be likely to cause substantial injury to consumers, may not be reasonably avoidable by those consumers, and may not be outweighed by benefits to consumers or competition. *See* 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.*

[42] See Rebecca Kelly Slaughter, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission,* Yale J. L. & Tech. (Aug. 2021), *https://yjolt.org/sites/default/files/23_yale_j.l._tech._special_issue_1.pdf.*

asks several questions about the prevalence of such practices, the extent of our authority in this area, and how the FTC, working with other enforcement agencies, may ameliorate those potential harms.[43]

Kids and Teens

As I remarked at COPPA's 20th anniversary, our experience enforcing the Children's Online Privacy Protection Act (''COPPA'') surely has lessons for any potential rulemaking.[44] What can the statutory scheme in COPPA tell us about how to structure potential rules? As a parent, I also have concerns for children as they pass outside the COPPA safety zone of under-13 years old. Are there harms we should examine that affect young teenagers in particular?[45]

Conclusion

The path the Commission is heading down by opening this rulemaking process is not an easy one. But it is a necessary one. The worst outcome, as I said three years ago, is not that we get started and then Congress passes a law; it is that we never get started and Congress never passes a law. People have made it clear that they find this status quo unacceptable.[46] Consumers and businesses alike deserve to know, with real clarity, how our Section 5 authority applies in the data economy. Using the tools we have available benefits the whole of the Commission's mission; well-supported rules could facilitate competition, improve respect for and compliance with the law, and relieve our enforcement burdens.

I have an open mind about this process and no certainty about where our inquiry will lead or what rules the record will support, as I believe is my obligation. But I do know that it is past time for us to begin asking these questions and to follow the facts and evidence where they lead us. I expect that the Commission will take this opportunity to think deeply about people's experiences in this market and about how to ensure that the benefits of progress are not built on an exploitative foundation. Clear rules have the potential for making the data economy more fair and more equitable for consumers, workers, businesses, and potential competitors alike.

I am grateful to the Commission staff for their extensive work leading up to the issuance of this ANPR,[47] as well as to the Chair for her leadership in pushing this project across the starting line, and to my fellow Commissioners for their thoughtful engagement with the document. Both the Chair and Commissioner Bedoya brought their expertise and vision to this endeavor, which is reflected throughout the final product. And, although I do not agree with my dissenting colleagues Commissioners Phillips and Wilson, I very much appreciate their constructive engagement, which has helped improve not only my own thinking but also the substance of the ANPR. I look forward to continued dialogue with all of them.

Statement of Commissioner Alvaro M. Bedoya

Our nation is the world's unquestioned leader on technology. We are the world's unquestioned leader in the data economy. And yet we are almost alone in our lack of meaningful protections for this infrastructure. We lack a modern data security law. We lack a baseline consumer privacy rule. We lack civil rights protections suitable for the digital age. This is a landscape ripe for abuse.

Now it is time to act. Today, we are beginning the hard work of considering new rules to protect people from unfair or deceptive commercial surveillance and data security practices.

My friend Commissioner Phillips argues that this advance notice of proposed rulemaking (''ANPR'') ''recast[s] the Commission as a legislature,'' and ''reaches outside the jurisdiction of the FTC.''[1] I respectfully disagree. Today, we're just asking questions, exactly as Congress has directed us to do.[2] At this *most* preliminary step, breadth is a feature, not a bug. We need a diverse range of public comments to help us discern whether and how to proceed with notices of proposed rulemaking. There is much more process to come.

In 1975, Congress passed the Magnuson-Moss Warranty—Federal Trade Commission Improvement Act (the ''Magnuson-Moss Act'').[3] That Act made explicit the Commission's authority to prescribe rules prohibiting unfair or deceptive trade practices. It also set out steps for doing so, including providing informal oral hearings with a limited right of cross examination, which were consistent with best practices of that time.[4] In the decade following its passage, the Magnuson-Moss Act was viewed as ''substantially increasing the agency's rulemaking powers.''[5]

Together with Congress's modest amendments to this process in 1980[6] and 1994,[7] federal law now gives us a clear roadmap for this work.[8] We will follow it to the letter.

The bipartisan American Data Privacy and Protection Act (ADPPA) is the strongest privacy bill that has ever been this close to passing. I hope it does pass. I hope it passes soon. What Chairman Frank Pallone, Ranking Member Cathy McMorris Rodgers, Senator Roger

[43] See ANPR at 36.

[44] See Rebecca Kelly Slaughter, *COPPA at 20: Protecting Children's Privacy in the New Digital Era,* Georgetown Univ. Law Ctr., (Oct. 24, 2018) *https://www.ftc.gov/system/files/documents/public_statements/1417811/opening_remarks_of_commissioner_slaughter_georgetown_law_coppa_at_20_event.pdf.*

[45] See ANPR at 27.

[46] See Lee Raine, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns,* Pew Research Center (Mar. 27, 2018), *https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns* (''Some 80% of social media users said they were concerned about advertisers and businesses accessing the data they share on social media platforms, and 64% said the government should do more to regulate advertisers.''); Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* Pew Research 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* (''Some 81% of the public say that the potential risks they face because of data collection by companies outweigh the benefits. . .''). These are not just theoretical concerns: The lack of effective data protection is harming the vitality of the tech sector. *See* Andrew Perrin, *Half of Americans have decided not to use a product or service because of privacy concerns,* Pew Research Center (Apr. 14, 2020), *https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/.*

[47] I would like to particularly acknowledge the hard work of Olivier Sylvain, Rashida Richardson, Gaurav Laroia, Janice Kopec, Austin King, Aaron Rieke, Bobbi Spector, Audrey Austin, Kristin Cohen, Mark Eichorn, Jim Trilling, and Peder Magee. And I would be remiss if I did not recognize the extraordinary contributions of Kurt Walters, who, as a law clerk in my office in summer 2019, began the process of debunking myths around Section 18 rulemaking, resulting in his law review article that is cited by several of my colleagues. *See* 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), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875970.*

[1] Dissenting Statement of Commissioner Noah Joshua Phillips, *Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking* (Aug. 11, 2022).

[2] Federal Trade Commission Improvements Act of 1980, Public Law 96–252, 94 Stat. 374.

[3] Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Public Law 93–637, 88 Stat. 2183 (1975).

[4] *Id.* at sec. 202 (adding § 18(c) of the FTC Act).

[5] Kurt Walters, *Reassessing the Mythology of Magnuson-Moss: A Call to Revive Section 18 Rulemaking at the FTC,* 16 Harvard L. & Pol'y Rev. (forthcoming 2022) (manuscript at 13), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875970.*

[6] Public Law 96–252, 94 Stat. 374 (1980).

[7] Federal Trade Commission Act Amendments of 1994, Public Law 103–312, Sections 3, 5, 108 Stat. 1691, 1691–92.

[8] 15 U.S.C. 57a (2018).

Wicker and their colleagues have accomplished is formidable and promising. This ANPR will not interfere with that effort. I want to be clear: Should the ADPPA pass, I will not vote for any rule that overlaps with it. There are no grounds to point to this process as reason to delay passage of that legislation.

Turning finally to the substance of the ANPR itself: It is a priority for me that the Commission, throughout this rulemaking process, stays focused on the needs of people who are most at risk of being left behind by new technology in the modern economy.[9] So while I will be interested in answers to all of our questions, I am keenly interested to learn about:

1. Emerging discrimination issues (Questions 65–72), especially from civil rights experts and affected communities. I agree with Commissioner Slaughter and Chair Khan that our unfairness authority is a powerful tool for combatting discrimination.[10] It *clearly* is.[11] Given significant gaps in federal antidiscrimination laws, especially related to internet platforms and technology companies,[12] I believe the Commission must act to protect people's civil rights.

2. The mental health of kids and teens (Question 17), especially from youth development experts and psychologists. A growing body of evidence suggests that teenagers, particularly teenage girls, who spend more than two or three hours daily on social media, suffer from increased rates of depression, anxiety, and thoughts of suicide and self-harm.[13] This is a nuanced issue, and peer-reviewed research is still developing.[14] But this nuance does not diminish the urgency of this work, and in fact heightens our need for comments on it. I appreciate especially the partnership of Commissioner Wilson in this area.

3. How to protect non-English speaking communities from fraud and other abusive data practices (Question 58), especially from affinity groups, internet platforms, and experts in fraud prevention practices. We know that many non-English language communities are disproportionately targeted in the offline world, and I am worried the story is even worse online. I'd like to hear more about how new rules might encourage more effective enforcement by both the Commission and private firms against scams and fraud.

4. How to protect against unfair or deceptive practices related to biometrics (Questions 37–38). A new generation of remote biometric technology is transforming our ability to move in public with some semblance of privacy. I'd welcome proposals for how rules may address and prevent abuse and harmful invasions of privacy.

I want to recognize Commissioner Slaughter for her early vision on this rulemaking process,[15] Chair Khan for her leadership in moving this effort forward, and all the agency staff who worked on it. Although my Republican colleagues are voting against this ANPR, I want them and the public to know I'll still seek their input throughout the process that follows.

I am most grateful to the members of the public, civil society, and small businesses community who will take the time to comment on this ANPR. We need your input. We will read it carefully and with interest.

Dissenting Statement of Commissioner Noah Joshua Phillips

Legislating comprehensive national rules for consumer data privacy and security is a complicated undertaking. Any law our nation adopts will have vast economic significance. It will impact many thousands of companies, millions of citizens, and billions upon billions of dollars in commerce. It will involve real trade-offs between, for example, innovation, jobs, and economic growth on the one hand and protection from privacy harms on the other. (It will also require some level of social consensus about which harms the law can and should address.) Like most regulations, comprehensive rules for data privacy and security will likely displace some amount of competition. Reducing the ability of companies to use data about consumers, which today facilitates the provision of free services, may result in higher prices—an effect that policymakers would be remiss not to consider in our current inflationary environment.[1]

National consumer privacy laws pose consequential questions, which is why I have said, repeatedly,[2] that Congress—

[9] Alvaro M. Bedoya, *Remarks of Commissioner Alvaro M. Bedoya at the National Association of Attorneys General Presidential Summit* (Aug. 9, 2022), *https://www.ftc.gov/news-events/news/speeches/remarks-commissioner-alvaro-m-bedoya-national-association-attorneys-general-presidential-summit.*

[10] *See* Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter, *Matter of Napleton Automotive Group* (Mar. 31, 2022), *https://www.ftc.gov/system/files/ftc_gov/pdf/Statement%20of%20Chair%20Lina%20M.%20Khan%20Joined%20by%20RKS%20in%20re%20Napleton_Finalized.pdf* (''[W]e take this as an opportunity to offer how the Commission should evaluate under its unfairness authority any discrimination that is found to be based on disparate treatment or have a disparate impact.''); Rebecca Kelly Slaughter, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission* (Aug. 2021), *https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf.*

[11] When a business substantially injures a person *because of who they are,* and that injury is not reasonably avoidable or outweighed by a countervailing benefit, that business has acted unlawfully. *See* Federal Trade Commission, *Policy Statement on Unfairness* (Dec. 17, 1980), *https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness* (''[t]o justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.'').

[12] For example, Title VII of the Civil Rights Act of 1964 covers employers and employment agencies, but does not directly address hiring technology vendors, digital sourcing platforms, and other companies that intermediate people's access to employment opportunity. *See* Title VII of the Civil Rights Act of 1964, 42 U.S.C. 2000e–2. Similarly, the Equal Credit Opportunity Act (ECOA) primarily covers ''creditors.'' *See* ECOA, 15 U.S.C. 1691(a) (2014). This scope creates similar coverage questions, including in financial markets related to hiring education. *See, e.g.,* Stephen Hayes & Kali Schellenberg, *Discrimination is ''Unfair'': Interpreting UDA(A)P to Prohibit Discrimination,* Student Borrower Protection Center (Apr. 2021), at 11, *https://protectborrowers.org/wp-content/uploads/2021/04/Discrimination_is_Unfair.pdf.*

[13] Jean M. Twenge et al., *Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time,* 6 Clinical Psychological Science 1, 3, 10 (Jan. 2018), *https://doi.org/10.1177/2167702617723376;* Hugues Sampasa-Kanyiga & Rosamund Lewis, *Frequent use of social networking sites is associated with poor psychological functioning among children and adolescents,* 18(7) Cyberpsychology, Behavior, and Social Networking 380 (Jul. 2015), *https://www.researchgate.net/publication/280059931_Frequent_Use_of_Social_Networking_Sites_Is_Associated_with_Poor_Psychological_Functioning_Among_Children_and_Adolescents.*

[14] *See, e.g.,* Amy Orban & Andrew K. Przybylski, *The association between adolescent well-being and digital technology use,* 3 Nature Human Behaviour 173 (Feb. 2019), *https://www.nature.com/articles/s41562-018-0506-1* (criticizing Twenge et al. at *supra* note 13).

[15] *See, e.g.,* Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law,* Silicon Flatirons-University of Colorado Law School (Sept. 6, 2019), *https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf* (''I believe the time has come to consider a Mag-Moss data-protection rule.'').

[1] German Lopez, *Inflation's 40-Year High,* N.Y. Times (Apr. 13, 2022), *https://www.nytimes.com/2022/04/13/briefing/inflation-forty-year-high-gas-prices.html.*

[2] *See, e.g.,* Statement of Commissioner Noah Joshua Phillips Regarding the Report to Congress on Privacy and Security (Oct. 1, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1597020/commissioner_phillips_dissent_to_privacy_report_to_congress_updated_final_93021_for_posting.pdf;* Sen. Roger Wicker, Rep. Cathy McMorris Rodgers & Noah Phillips, *FTC must leave privacy legislating to Congress,* Wash. Exam'r (Sept. 29, 2021), *https://www.washingtonexaminer.com/opinion/op-eds/ftc-must-leave-privacy-legislating-to-congress;* Prepared Oral Statement of Commissioner Noah Joshua Phillips Before the House Committee on Energy and Commerce Subcommittee on Consumer Protection

Continued

not the Federal Trade Commission (''FTC'' or ''Commission'')—is where national privacy law should be enacted. I am heartened to see Congress considering just such a law today,[3] and hope this Commission process does nothing to upset that consideration.

So I don't think we should do this. But if you're going to do it, do it right. The Commercial Surveillance and Data Security advance notice of proposed rulemaking (''ANPR'') issued today by a majority of commissioners provides no notice whatsoever of the scope and parameters of what rule or rules might follow; thereby, undermining the public input and congressional notification processes. It is the wrong approach to rulemaking for privacy and data security.

What the ANPR does accomplish is to recast the Commission as a legislature, with virtually limitless rulemaking authority where personal data are concerned. It contemplates banning or regulating conduct the Commission has never once identified as unfair or deceptive. That is a dramatic departure even from recent Commission rulemaking practice. The ANPR also contemplates taking the agency outside its bailiwick. At the same time, the ANPR virtually ignores the privacy and data security concerns that have animated our enforcement regime for decades. A cavalcade of regulations may be on the way, but their number and substance are a mystery.

The ANPR Fails To Provide Notice of Anything and Will Not Elicit a Coherent Record

The ANPR fails to live up to the promise in its name, to give advance notice to the public (and Congress) of what the Commission might propose. The FTC Act requires an ANPR to ''contain a brief description of the area of inquiry under consideration, the objective which the Commission seeks to achieve, and possible regulatory alternatives under consideration by the Commission.'' [4] This ANPR flunks even that basic test. 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.[5] The document stands in stark contrast to the focus that characterizes recent ANPRs issued by the Commission, which addressed far more limited topics like impersonating a government entity or private business, deceptive earnings claims, or the scope of the Telemarketing Sales Rule.[6] I supported each of those.

A well-crafted ANPR is calibrated to develop a thorough record. But this ANPR addresses too many topics to be coherent. It requests information ranging from what practices companies currently use to ''surveil consumers'' [7] to whether there should be a rule granting teens an ''erasure mechanism,'' [8] what extent any new commercial surveillance rule would impede or enhance innovation,[9] the administrability of any data minimization or purpose limitation requirements,[10] the ''nature of the opacity of different forms of commercial surveillance practices,'' [11] and whether the Commission has ''adequately addressed indirect pecuniary harms, including . . . psychological harms.'' [12]

The ANPR provides no clue what rules the FTC might ultimately adopt. In fact, the Commission expressly states that the ANPR does not identify the full scope of approaches it could undertake, does not delineate a boundary on issues on which the public can comment, and in no way constrains the actions it might take in an NPRM or final rule.[13] This scattershot approach creates two obvious problems: stakeholders cannot discern how to engage meaningfully and provide comment, and the lack of focus for their comments will give the Commission a corollary ability to proceed in any direction it chooses. I earnestly cannot see how this document furthers an effort to fashion discrete and durable privacy and data security rules.

The ANPR poses some 95 questions about the myriad topics it purports to address, but many simply fail to provide the detail necessary for commenters to prepare constructive responses. Take the ANPR's blanket request for cost-benefit analyses:

> [T]he Commission invites public comment on (a) the nature and prevalence of harmful commercial surveillance and lax data security practices, (b) the balance of costs and countervailing benefits of such practices for consumers and competition, as well as the costs and benefits of any given potential trade regulation rule, and (c) proposals for protecting consumers from harmful and prevalent commercial surveillance and lax data security practices.[14]

This question asks the public to comment on the costs and benefits of any business practice and any possible regulation involving ''commercial surveillance,'' a term defined so broadly (and with such foreboding [15]) that it captures any collection or use of consumer data.[16] It goes on to ask commenters how the Commission should evaluate the answers, as if the FTC Act does not provide a framework for fashioning such regulations (it does) and the Commission does not know how to apply it (I hope we do).[17]

These kinds of questions are not conducive to stakeholders submitting data and analysis that can be compared and considered in the context of a

---

and Commerce, Hearing on ''Transforming the FTC: Legislation to Modernize Consumer Protection'' (July 28, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1592981/prepared_statement_0728_house_ec_hearing_72821_for_posting.pdf.*

[3] *See* Rebecca Klar, *House panel advances landmark federal data privacy bill,* The Hill (July 20, 2022), *https://thehill.com/policy/technology/3567822-house-panel-advances-landmark-federal-data-privacy-bill/;* Press Release, House Committee on Energy and Commerce, *House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill* (June 3, 2022), *https://energycommerce.house.gov/newsroom/press-releases/house-and-senate-leaders-release-bipartisan-discussion-draft-of.*

[4] 15 U.S.C. 57a(b)(2)(A)(i).

[5] The Commission is not even limiting itself to Section 18 rules that must follow the procedures laid out in Magnuson-Moss Warranty Act, Public Law 93–637, 88 Stat. 2183. The ANPR notes that it is requesting information on how commercial surveillance harms competition, which could inform competition rulemaking. Other commissioners may believe the Commission may promulgate such rules, including without an ANPR. I do not. *See* Prepared Remarks of Commissioner Noah Joshua Phillips at FTC Non-Compete Clauses in the Workplace Workshop (Jan. 9, 2020), *https://www.ftc.gov/system/files/documents/public_statements/1561697/phillips_-_remarks_at_ftc_nca_workshop_1-9-20.pdf.*

[6] *See* Trade Regulation Rule on Impersonation of Government and Businesses, 86 FR 72901 (Dec. 23, 2021), *https://www.federalregister.gov/documents/2021/12/23/2021-27731/trade-regulation-rule-on-impersonation-of-government-and-businesses;* Deceptive or Unfair Earnings Claims, 87 FR 13951 (Mar. 11, 2022), *https://www.federalregister.gov/documents/2022/03/11/2022-04679/deceptive-or-unfair-earnings-claims;* Telemarketing Sales Rule, 87 FR 33662 (June 3, 2022), *https://www.federalregister.gov/documents/2022/06/03/2022-10922/telemarketing-sales-rule.*

[7] *See* section IV, Q.1 of this document, ANPR for Trade Regulation Rule on Commercial Surveillance and Data Security. [hereinafter ANPR].

[8] *Id.* at section IV, Q.14.

[9] *Id.* at section IV, Q.26.

[10] *Id.* at section IV, Q.49.

[11] *Id.* at section IV, Q.86.

[12] I am not sure what this means. Should the Commission be obtaining monetary redress for the cost of consumers' therapy? *Id.* at section IV, Q.9.

Where conduct is not deceptive, the FTC Act only permits us to regulate conduct that causes ''substantial injury''. 15 U.S.C. 45(n).

[13] ANPR at 24.

[14] *Id.*

[15] In adopting this academic pejorative, the ANPR trades a serious attempt to understand business practices it would regulate for the chance to liken untold companies large and small to J. Edgar Hoover's COINTELPRO.

[16] ''For the purposes of this ANPR 'commercial surveillance' refers to the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information.'' ANPR at 13.

[17] *Id.* at section IV, Qs.24–29.

specific rule. The Commission would be more likely to receive helpful data if it asked commenters for the costs and benefits of some defined kind of conduct, or a particular rule to regulate it—say, information collected by exercise apps, or a rule limiting the use of third-party analytics by those apps.[18] Without specific questions about business practices and potential regulations, the Commission cannot hope for tailored responses providing a full picture of particular practices. Determining the appropriateness and scope of any subsequent proposed rule will prove difficult.

The ANPR Recasts the FTC as a Legislature

The ANPR kickstarts the circumvention of the legislative process and the imposition upon the populace of the policy preferences of a majority of unelected FTC commissioners. The Supreme Court recently noted ''a particular and recurring problem [of] agencies asserting highly consequential power beyond what Congress could reasonably be understood to have granted.'' [19] Apparently, the FTC is next up to the plate. Our Section 18 authority to regulate ''unfair or deceptive acts or practices'' [20] goes only so far; and the ANPR contemplates reaching well beyond, including to common business practices we have never before even asserted are illegal. Reading the FTC Act to provide the Commission with the ''sweeping and consequential authority'' [21] to mandate changes across huge swaths of the economy will test the limits of our congressional delegation.

The ANPR's many references to international and state privacy laws signal the majority's view that the scope of the rules passed by the unelected commissioners of an independent agency should be on par with statutes passed by elected legislators. Even as we vote, Congress is considering actively legislation concerning the very matters the ANPR purports to address.[22] I sincerely hope that this ill-advised process does not upset that very much needed one.

The ANPR colors well outside the lines of conduct that has been the subject of many (or, in a number of prominent cases, any) [23] enforcement actions, where real world experience provides a guide.[24] Unlike our December 2021 ANPR targeting fraudsters that impersonate the government, for example, the Commission does not have 20 years of cases covering the same conduct.[25] The Auto Rule NPRM issued last month also targeted conduct that was the basis of repeated Commission enforcement.[26]

This ANPR, meanwhile, attempts to establish the prevalence necessary to justify broad commercial surveillance rulemaking by citing an amalgam of cases concerning very different business models and conduct.[27] Under Section 18, the agency must show that the unfair acts or practices in question are prevalent, a determination that can only be made if the Commission has previously ''issued cease and desist orders regarding such acts or practices,'' or if it has any other information that ''indicates a widespread pattern of unfair or deceptive acts or practices.'' [28] Where the agency has little (or no) experience, prudence counsels in favor of investigation to explore costs and benefits and to determine illegality. The ANPR aims for regulation without even any experience, to say nothing of court decisions ratifying the application of Section 5 to the business conduct in question. As this process moves forward, the Commission would do well to keep in mind that ''[a]gencies have only those powers given to them by Congress, and 'enabling legislation' is generally not an 'open book to which the agency [may] add pages and change the plot line.''' [29]

Take, for example, the ANPR's treatment of ''personalized'' or ''targeted'' advertising.[30] The majority seems open to banning—ahem, ''limiting''— targeted advertising. Limiting or banning targeted advertising will be a heavy lift for many reasons, not the least of which is that we have never brought a case alleging that targeted advertising is unfair. The Commission has brought cases where companies deceptively collected, used, or shared personal data for purposes including targeted advertising, but that is not the same.[31] Perhaps in recognition of these potential difficulties, the ANPR requests ideas on what potential legal theories might support limits on the use of automated systems in targeted advertising.[32]

Consider also the ANPR's discussion of consent, one of the traditional bedrocks of privacy policy. Whether notice and consent is the optimal approach to consumer privacy in every context is worthy of serious debate. Instead of discussing the merits and shortcomings of transparency and choice, the majority simply concludes that ''consent may be irrelevant.'' [33] The ANPR bolsters this view with claims that other privacy regimes are moving away from an emphasis on consent. Really? While there are certainly privacy laws that include data

[18] *Cf. In the matter of Flo Health, Inc.,* FTC File No. 1923133 (2021), *https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc* (Flo Health violated Section 5 by sharing consumer health information with data analytics providers, despite promising consumers that it would keep the data private).

[19] *West Virginia* v. *EPA,* 2022 WL 2347278 (June 30, 2022) (slip op. at 20).

[20] 15 U.S.C. 57a.

[21] *West Virginia* v. *EPA,* 2022 WL 2347278, at 17.

[22] 168 Cong. Rec. D823 (daily ed. July 20, 2022). *Cf. West Virginia* v. *EPA,* 2022 WL 2347278 at 20 (stating that the EPA's discovery of power to restructure the energy market ''allowed it to adopt a regulatory program that Congress had conspicuously and repeatedly declined to enact itself.'').

[23] Observers have, in the past, taken the FTC to task for trying to create ''law'' through settlements it reaches following investigations with private parties. *See, e.g.,* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law,* 101 Iowa L. Rev. 955 (2016). That is a real concern. But those criticisms seem quaint in retrospect, as this ANPR contemplates banning or regulating conduct that hasn't even been the subject of enforcement.

[24] For example, while the Commission has explored facial recognition and automated decision-making in workshops and reports, it has never found that the use of facial recognition technology or automated decision-making themselves to be unfair. Despite this conspicuous lack of enforcement actions, if questions such as 38 or 60 of this ANPR are any indication, the Commission might rush straight to limiting or prohibiting their use. *See* ANPR at section IV, Q.38 and Q.60.

[25] The absence of this record itself undermines one of the traditional arguments for rules, *i.e.,* that enforcement efforts have not proven sufficient. *See, e.g.,* Trade Regulation Rule on Impersonation of Government and Businesses, 86 FR 72901 (Dec. 23, 2021), *https://www.federalregister.gov/documents/2021/12/23/2021-27731/trade-regulation-rule-on-impersonation-of-government-and-businesses.*

[26] Motor Vehicle Dealers Trade Regulation Rule, 87 FR 42012 (July 13, 2022), *https://www.federalregister.gov/documents/2022/07/13/2022-14214/motor-vehicle-dealers-trade-regulation-rule.*

[27] *See, e.g., In re Craig Brittain,* FTC File No. 1323120 (2015), *https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3120-craig-brittain-matter* (company solicited ''revenge'' porn and charged consumers to take down images); *U.S.* v. *AppFolio, Inc.,* Civ. Action No. 1:20-cv-03563 (D.D.C. 2020), *https://www.ftc.gov/legal-library/browse/cases-proceedings/1923016-appfolio-inc* (consumer reporting agency failed to implement reasonable procedures to ensure maximum possible accuracy of its tenant screening reports).

[28] 15 U.S.C. 57a(b)(3).

[29] *West Virginia* v. *EPA,* 2022 WL 2347278 at 19, (quoting E. Gellhorn & P. Verkuil, *Controlling Chevron-Based Delegations,* 20 Cardozo L. Rev. 909, 1011 (1999)).

[30] I recognize that all advertising is ''targeted'', why—for example—readers of Car & Driver in the pre-digital era saw ads for cars, driving gloves, and floor mats. In this dissent, I use the phrase ''targeted advertising'' to describe the ubiquitous conduct at issue in the ANPR, *i.e.,* advertising served on the web and through apps based on data collected about people.

[31] *See, e.g., U.S.* v. *OpenX Technologies, Inc.,* Civ. Action No. 2:21-cv-09693 (C.D. Cal. 2021), *https://www.ftc.gov/enforcement/cases-proceedings/1923019/openx-technologies-inc; In the Matter of Goldenshores Technologies, LLC, and Erik M. Geidl,* FTC File No. 1323087 (2014), *https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3087-goldenshores-technologies-llc-erik-m-geidl-matter.*

[32] *See* ANPR section IV, Q.62.

[33] *Id.* at 6.

minimization requirements or restrict secondary uses of data, many still allow for consent. For example, the Children's Online Privacy Protection Act of 1998 requires parents to give verified parental consent before a business collects information from a child.[34] The European Union's General Data Protection Regulation (''GDPR'') allows businesses to process data if they have the consumer's consent, which must be freely given, specific, informed, and unambiguous.[35]

The ANPR appears skeptical that consumers can be trusted to make their own choices, seeking information on what ''commercial surveillance'' practices are illegal, ''irrespective of whether consumers consent to them.'' [36] Should the majority be thwarted in its quest to make consent passé, the ANPR contemplates at least having different consent standards for individuals ''in crisis'' or ''especially vulnerable to deception.'' [37] This is paternalistic to say the least: Heaven forfend adults make decisions and permit companies to use their data to serve them targeted ads. But even if you disagree with that view, the point is that a consequential decision to take away that choice from individuals—like many of the decisions that need to be weighed in creating a national privacy law—is best left to Congress. The FTC is not a legislature.

The ANPR also contemplates rewriting the Children's Online Privacy Protection Act (''COPPA'').[38] Consistent with its dismissal of consent as a legal basis for collecting data, its discussion of children and teens is hostile to the idea that parents can consent to the collection, use, or sharing of data about their children.[39] In enacting COPPA, with its explicit provision for verifiable parental consent, Congress determined that parents can make decisions about the collection and sharing of their children's personal data.[40] The FTC cannot and should not attempt to overrule Congress through rulemaking—or parents, who routinely have to make all sorts of decisions about our children.

To be fair, the ANPR raises the important issue of whether there should be more rules that protect the privacy of teenagers. COPPA only covers children under thirteen, and there are plenty of data privacy and security issues that impact youth ages 13 to 16 online. But here the ANPR is out of order. Just days ago, the Senate Commerce Committee considered legislation to amend COPPA, including to extend protections to minors up to age 16.[41] Congress is working on these answers. And, lest we forget, *so are we.* The privacy of children was a central concern of the social media 6(b)s, a project we have not yet completed.[42] The Commission also has had ongoing for years a review of the COPPA Rule. The Commission received over 170,000 comments upon it, the most of any request for input issued in the history of the agency. This ANPR threatens to supersede that process. We should first complete our homework on those projects before starting over the process of writing new rules.

The ANPR is FTC Overreach

The ANPR reaches outside the jurisdiction of the FTC. It seeks to recast the agency as a civil rights enforcer, contemplating policing algorithms for disparate impact without a statutory command.[43] This raises immediate concerns. First, do we have the authority? When Congress seeks to ban discrimination, it says so directly.[44] The FTC Act does not mention discrimination. Second, the civil rights laws Congress has adopted to fight discrimination delineate the bases upon which discrimination is illegal.[45] The FTC Act does not. Third, our antidiscrimination laws cover aspects of commerce where Congress has expressed concern about the impact of discrimination, for example housing, employment, and the extension of credit.[46] The FTC Act applies broadly to any unfair or deceptive act or practice in or affecting commerce. Finally, the FTC Act does not specify whether it is a regime of disparate treatment or disparate impact.

When determining what conduct violates an antidiscrimination law, all of these questions are critical. The FTC Act, which is not such a law, answers none of them. All of that raises the prospect of interpreting the FTC Act to bar disparate impact, including on bases that most would regard as perfectly reasonable or at the very least benign. So, for example, an algorithm resulting in ads for concert tickets being shown more often to music lovers would constitute illegal discrimination against those who are not music lovers. So might a dating app that uses an algorithm to help users find people of the same faith. Under the theory presupposed in the ANPR, such conduct would be illegal.

The ANPR seeks comment on whether the Commission might bar or limit the deployment of any system that produces disparate outcomes, irrespective of the data or processes on which the outcomes were based. (Is this what people mean when they say ''algorithmic justice''? [47]) This could very well mean barring or limiting any technology that uses algorithms to make decisions that apply to people. The ANPR requests comment on whether the FTC should ''forbid or limit the development, design, and use of automated decision-making systems that generate or otherwise facilitate outcomes that violate Section 5.'' [48] In other words, the Commission wonders if it should put the kibosh on the development of artificial intelligence. Stopping American innovation in its tracks seems to me neither to reflect the law nor to be sound public policy.

The Chair's statement suggests that, through this process, we can and should regulate the relations between

[34] Children's Online Privacy Protection Rule, 16 CFR 312.5, *https://www.govinfo.gov/content/pkg/CFR-2012-title16-vol1/pdf/CFR-2012-title16-vol1-sec312-5.pdf.*

[35] *See* Complete Guide to GDPR Compliance, *https://gdpr.eu/gdpr-consent-requirement/?cn-reloaded=1.*

[36] *See* ANPR at section IV, Q.76.

[37] *Id.* at section IV, Q.79.

[38] 15 U.S.C. 6502.

[39] I suppose there is some logic to the majority's view that if you can't consent to personalized advertising for yourself, then you can't consent for your children either. I disagree with both conclusions.

[40] 15 U.S.C. 6502.

[41] *See* Cristiano Lima, *Senate panel advances bills to boost children's safety online,* Wash. Post (July 27, 2022), *https://www.washingtonpost.com/technology/2022/07/27/senate-child-safety-bill/.*

[42] *See* Lesley Fair, FTC issues 6(b) orders to social media and video streaming services, Fed. Trade Comm'n Business Blog (Dec. 14, 2020), *https://www.ftc.gov/business-guidance/blog/2020/12/ftc-issues-6b-orders-social-media-and-video-streaming-services.*

[43] Illegal discrimination is pernicious, which is why we have statutes and agencies that protect consumers from being wrongly denied employment, housing, or credit due to a protected characteristic.

[44] *See, e.g.,* The Fair Housing Act, 42 U.S.C. 3601 *et seq.,* which prohibits discrimination in housing because of race, religion, sex, national origin, familial status or disability. The Age Discrimination in Employment Act, 29 U.S.C. 621 *et seq.,* prohibits employment discrimination against individuals aged 40 years or older.

[45] For example, Title VII of the Civil Rights Act of 1964, Public Law 88–352, prohibits employment discrimination ''because of such individual's race, color, religion, sex, or national origin.'' The Americans with Disabilities Act, 42 U.S.C. 12101, prohibits discrimination against people with disabilities in employment, transportation, public accommodations, communications, and access to state and local governments' programs and services.

[46] The FTC does enforce the Equal Credit Opportunity Act (''ECOA''), an antidiscrimination law covering the extension of credit. ECOA bars discrimination ''with respect to any aspect of a credit transaction'' on the basis of race, color, religion, national origin, sex, marital status, age, or because of receipt of public assistance. 15 U.S.C. 1691 *et seq.*

[47] Charles C.W. Cooke, *'Algorithmic Justice',* Nat'l Rev. (Apr. 26, 2022), *https://www.nationalreview.com/corner/algorithmic-justice/.*

[48] *See* ANPR at section IV, Q.60.

employers and employees where data are concerned.[49] The only related question in the ANPR asks ''[h]ow, if at all, should potential new trade regulation rules address harms to different consumers across different sectors.'' [50] That question does not seem designed to obtain the information that would be necessary to regulate employers' use of data concerning their employees, so perhaps the concept is off the table right out of the gate. But if not, I disagree with the premise that the FTC Act confers upon us jurisdiction to regulate any aspect of the employer-employee relationship that happens to involve data.[51]

But wait, there's more. The Commission is also apparently considering prohibiting social media, search, or other companies from owning or operating any business that engages in activities such as personalized advertising.[52] The ANPR seeks comment on whether we should limit finance, healthcare, and search services from cross-selling commercial products.[53] It contemplates requiring companies to disclose their intellectual property and trade secrets.[54] How any of these naked restraints on competition fall within our ken of policing ''unfair or deceptive acts or practices'' is completely unclear.

My preference would be that before we draft an ANPR, we be clear about the scope of our legal authority and that our proposal would be guided by those limitations. The ANPR looks instead like a mechanism to fish for legal theories that might justify outlandish regulatory ambition outside our jurisdiction and move far beyond where Commission enforcement has tread. Any ideas of how we might have the authority to ban targeted advertising? [55] Are we constrained by the First Amendment or Section 230 of the Communications Decency Act? [56] The ANPR is open to all creative ideas.[57]

The ANPR Gives Short Shrift to Critical Policy Issues Within its Scope

The ANPR lavishes attention on areas that have not been a focus of our enforcement and policy work, but shortchanges data security, one area ripe for FTC rulemaking. Over the past 20 years, the Commission has brought around 80 data security cases, hosted workshops, and done significant outreach to the business community on the topic of data security. A data security rule could protect consumers from the harms stemming from data breaches and provide businesses with greater clarity about their obligation to protect personal data. It could incentivize better data security by increasing the cost of bad security. I would welcome such a rulemaking if fashioned well. Instead of focusing on this important area, the ANPR gives data security short shrift. Six questions. That's it. A data security ANPR would surely have been more than six questions, a good indication that this ANPR is just not enough to make a data security rule. For example, our ANPR on impersonation fraud asked 13 questions about a far narrower topic. This is a missed opportunity to develop the record needed for a rule requiring companies to implement data security safeguards to protect consumers' personal data.

Perhaps the most shocking aspect of this ANPR is not what it contains, but what it leaves out: privacy. Missing from this document is any meaningful discussion about whether there should be different rules based on the sensitivity of data, a traditional area of privacy concern reflected in particular federal laws, which provide greater protection for data considered more sensitive, like health data, financial data, and data collected from children.[58] Almost as an afterthought, the ANPR asks ''which kinds of data'' might be subject to any potential rules, but there is no attempt at real engagement on the topic.[59] There is no question asking how ''sensitive data'' should be defined. The ANPR seeks information about whether the Commission should put restrictions on fingerprinting,[60] but is incurious about whether a rule should treat medical history and a social security number differently than an IP address or zip code.[61] ANPR questions focused on treating data differently based on sectors rather than on the sensitivity of the data itself fail to recognize that health data is collected and held across multiple sectors. One of the first steps in any serious attempt to develop a baseline privacy standard should be to determine what information is sensitive and might justify higher levels of protection.

In another departure from most privacy frameworks, the ANPR includes little discussion of how a rule should incorporate important principles like access, correction, deletion, and portability. The majority is so focused on justifying limiting or banning conduct now apparently disfavored that they spare no thought for how best to empower consumers. If you were hoping that the FTC would use its expertise and experience to develop rules that would give consumers greater transparency and control over their personal data, you must be very disappointed.

Conclusion

When adopting regulations, clarity is a virtue. But the only thing clear in the ANPR is a rather dystopic view of modern commerce. This document will certainly spark some spirited conversations, but the point of an ANPR is not simply to pose provocative questions. This is not an academic symposium. It is the first step in a rulemaking process, and the law entitles the public to some sense of where the FTC is going.

I would have supported an ANPR for a data security rule. I would have been more sympathetic to an ANPR that was focused on consumer privacy as reflected in our long record of enforcement and policy advocacy—say, a rule that, for example, would require transparency or that would, depending

[49] Statement of Chair Lina M. Khan Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking (Aug. 11, 2022).

[50] ANPR at section IV, Q.12.

[51] The Chair's statement cites to the *Amazon Flex* case to support the notion that the Commission has authority to regulate the relationship between employers and employees. But that settled enforcement action concerned independent contractors. *See In the matter of Amazon.com, Inc. and Amazon Logistics, Inc.,* FTC File No. 1923123 (2021), *https://www.ftc.gov/legal-library/browse/cases-proceedings/1923123-amazon-flex.* While this Commissioner is no expert in labor and employment law, my understanding is that the distinction between independent contractors and employees is fundamental.

[52] *Id.* at section IV, Q.39.

[53] *Id.* at [Q.46].

[54] China probably approves. *Id.* at section IV, Q.86.

[55] *Id.* at section IV, Q.62.

[56] *Id.* at section IV, Q.63–64.

[57] Law enforcement agencies should stay within the clearly delineated bounds of the law. There are no points for creativity.

[58] *See* Health Breach Notification Rule, 16 CFR part 318; Gramm-Leach Bliley Act, Public Law 106–102, 112 Stat. 1338 (1999); Fair Credit Reporting Act, 15 U.S.C. 1681–1681x; Children's Online Privacy Protection Act, 15 U.S.C. 6501–6505.

[59] *See* ANPR at section IV, Q.10.

[60] While fingerprints would likely constitute sensitive data under a privacy rule, I will be interested to learn how fingerprinting itself is an unfair or deceptive practice under Section 5.

[61] The decision not to ask about how to define sensitive data is particularly odd given the agency's recent statements vowing to aggressively pursue cases involving the use and sharing of ''location, health, and other sensitive information.'' If the goal is to forbid the sharing of location data, in particular location data relating to reproductive health, a rule defining sensitive data would seem invaluable to that project. *See* Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data,* Fed. Trade Comm'n Business Blog (July 11, 2022), *https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use.*

on the sensitivity of the information or the purposes for which it was collected, put some limits on the collection and use of consumer information. These ideas would be consistent with, among other things, Commission enforcement experience. I cannot support an ANPR that is the first step in a plan to go beyond the Commission's remit and outside its experience to issue rules that fundamentally alter the internet economy without a clear congressional mandate. That's not ''democratizing'' the FTC or using all ''the tools in the FTC's toolbox.'' It's a naked power grab. I dissent.

Dissenting Statement of Commissioner Christine S. Wilson

Throughout my tenure as an FTC Commissioner, I have encouraged Congress to pass comprehensive privacy legislation.[1] While I have great faith in markets to produce the best results for consumers, Econ 101 teaches that the prerequisites of healthy competition are sometimes absent. Markets do not operate efficiently, for example, when consumers do not have complete and accurate information about the characteristics of the products and services they are evaluating.[2] Neither do markets operate efficiently when the costs and benefits of a product are not fully borne by its producer and consumers—in other words, when a product creates what economists call externalities.[3] Both of these shortcomings are on display in the areas of privacy and data security. In the language of economists, both information asymmetries and the presence of externalities lead to inefficient outcomes with respect to privacy and data security.

Federal privacy legislation would provide transparency to consumers regarding the full scope of data collection, and how collected data are used, shared, sold, and otherwise monetized. In addition, a comprehensive privacy law would give businesses much-needed clarity and certainty regarding the rules of the road in this important area, particularly given the patchwork of state laws that is emerging. And Congressional action would help fill the emerging gaps in sector-specific approaches created by evolving technologies and emerging demands for information. Perhaps most importantly, a national privacy law would help curb violations of our civil liberties.[4]

While I have long been concerned about data collection and usage, the events of 2020 laid bare new dangers and served only to deepen my concerns. During that tumultuous year, I wrote and spoke on several occasions regarding pressing privacy and civil liberties issues.[5] In the face of continued Congressional inaction, I became willing to *consider* whether the Commission should undertake a Section 18 rulemaking to address privacy and data security. But even then, I emphasized that an FTC rulemaking would be vastly inferior to federal privacy legislation.[6] And I continue to believe that Congressional action is the best course.

I am heartened that Congress is now considering a bipartisan, bicameral bill that employs a sound, comprehensive, and nuanced approach to consumer privacy and data security. The American Data Privacy and Protection Act (ADPPA) rightly has earned broad acclaim in the House Committee on Energy and Commerce and the Subcommittee on Consumer Protection and Commerce, and is moving to a floor vote in the House.[7] I am grateful to Ranking Member Roger Wicker, Chairman Frank Pallone, Chair Jan Schakowsky, Ranking Member Cathy McMorris Rodgers, and Ranking Member Gus Bilirakis for their thoughtful work, and I hope to see this bill become a law. The momentum of ADPPA plays a significant role in my ''no'' vote on the advance notice of proposed rulemaking (ANPRM) announced today. I am gravely concerned that opponents of the bill will use the ANPRM as an excuse to derail the ADPPA.

While the potential to derail the ADPPA plays a large role in my decision to dissent, I have several other misgivings about proceeding with the ANPRM. First, in July 2021, the Commission made changes to the Section 18 Rules of Practice that decrease opportunities for public input and vest significant authority for the rulemaking proceedings solely with the Chair.[8] Second, the Commission is authorized to issue a notice of proposed rulemaking when it ''has reason to believe that the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent.'' [9] Many practices discussed in this ANPRM are presented as clearly deceptive or unfair despite the fact that they stretch far beyond practices with which we are familiar, given our extensive law enforcement experience. Indeed, the ANPRM wanders far afield of areas for which we have clear evidence of a widespread pattern of unfair or deceptive practices. Third, regulatory [10] and enforcement [11] overreach increasingly has drawn sharp criticism from courts. Recent Supreme Court decisions indicate FTC rulemaking overreach likely will not

[1] *See* Oral Statement of Commissioner Christine S. Wilson as Prepared for Delivery Before the U.S. House Energy and Commerce Subcommittee on Consumer Protection and Commerce (July 28, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1592954/2021-07-28_commr_wilson_house_ec_opening_statement_final.pdf;* Oral Statement of Commissioner Christine S. Wilson Before the U.S. Senate Committee on Commerce, Science and Transportation (Apr. 20, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1589180/opening_statement_final_for_postingrevd.pdf;* Oral Statement of Commissioner Christine S. Wilson Before the U.S. Senate Committee on Commerce, Science and Transportation (Aug. 5, 2020), *https://www.commerce.senate.gov/services/files/25112CF8-991F-422C-8951-25895C9DE11D;* Oral Statement of Commissioner Christine S. Wilson as Prepared for Delivery Before the U.S. House Energy and Commerce Subcommittee on Consumer Protection and Commerce (May 8, 2019), *https://www.ftc.gov/system/files/documents/public_statements/1519254/commissioner_wilson_may_2019_ec_opening.pdf.*

[2] Robert Pindyck & Daniel Rubinfeld, Microeconomics 625–626 (8th ed. 2017).

[3] *Id.* at 626.

[4] *See* Christine Wilson, Op-Ed, Coronavirus Demands a Privacy Law, Wall St. J., May 13 2020, available at *https://www.wsj.com/articles/congress-needs-to-pass-a-coronavirus-privacy-law-11589410686;* Christine S. Wilson, Privacy and Public/Private Partnerships in a Pandemic, Keynote Remarks Privacy + Security Forum (May 7, 2020), *https://www.ftc.gov/system/files/documents/public_statements/1574938/wilson_-_remarks_at_privacy_security_academy_5-7-20.pdf;* Christine Wilson, Privacy in the Time of Covid-19, Truth On The Market (Apr. 15, 2020), *https://truthonthemarket.com/author/christinewilsonicle/.*

[5] *Id.*

[6] Oral Statement of Commissioner Christine S. Wilson as Prepared for Delivery Before the U.S. House Energy and Commerce Subcommittee on Consumer Protection and Commerce (July 28, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1592954/2021-07-28_commr_wilson_house_ec_opening_statement_final.pdf.*

[7] Press Release, Bipartisan E&C Leaders Hail Committee Passage of the American Data Privacy and Protection Act (Jul. 20, 2022), *https://energycommerce.house.gov/newsroom/press-releases/bipartisan-ec-leaders-hail-committee-passage-of-the-american-data-privacy.*

[8] *See* Dissenting Statement of Commissioners Christine S. Wilson and Noah Joshua Phillips Regarding the Commission Statement on the Adoption of Revised Section 18 Rulemaking Procedures (July 9, 2021), *https://www.ftc.gov/system/files/documents/public_statements/1591702/p210100_wilsonphillips_joint_statement_-_rules_of_practice.pdf* (detailing the changes to the Rules and concerns that the changes ''fast-track regulation at the expense of public input, objectivity, and a full evidentiary record.'').

[9] 15 U.S.C. 57a(b)(3).

[10] *West Virginia* v. *EPA,* 2022 WL 2347278 (June 30, 2022) (striking down EPA regulations as outside of the agency's Congressionally mandated authority).

[11] *AMG Capital Management, LLC* v. *FTC,* 141 S. Ct. 1341 (2021) (finding that the FTC exceeded its law enforcement authority under Section 13(b) of the FTC Act).

fare well when subjected to judicial review. And fourth, Chair Khan's public statements [12] give me no basis to believe that she will seek to ensure that proposed rule provisions fit within the Congressionally circumscribed jurisdiction of the FTC. Neither has Chair Khan given me reason to believe that she harbors any concerns about harms that will befall the agency (and ultimately consumers) as a consequence of her overreach.

While baseline privacy legislation is important, I am pleased that Congress also is considering legislation that would provide heightened privacy protections for children.[13] Recent research reveals that platforms use granular data to track children's online behavior, serve highly curated feeds that increase engagement, and (in some instances) push kids towards harmful content.[14] More broadly, the research reveals a ''catastrophic wave of mood disorders (anxiety and depression) and related behaviors (self-harm and suicide)'' among minors, and particularly teenage girls, who spend a significant amount of time on social media daily.[15] The Kids Online Safety Act makes particularly noteworthy contributions, and I applaud Senators Richard Blumenthal and Marsha Blackburn on their work.

I appreciate that my newest colleague, Commissioner Alvaro Bedoya, brings to the Commission deep experience in the field of privacy and data security and shares my concerns about protecting children online.[16] I look forward to working with him, FTC staff, and our fellow Commissioners to take constructive steps in this area, including advancing key research, heightening awareness, bringing enforcement actions, and concluding the Commission's ongoing review of the Children's Online Privacy Protection Act.

[FR Doc. 2022–17752 Filed 8–19–22; 8:45 am]

BILLING CODE 6750–01–P

[12] *See, e.g.,* Koenig, Bryan, *FTC's Khan More Worried About Inaction Than Blowback,* Law360 (Apr. 22, 2022), *https://www.law360.com/articles/1486611/ftc-s-khan-more-worried-about-inaction-than-blowback;* Scola, Nancy, *Lina Khan Isn't Worried About Going Too Far,* NY Magazine (Oct. 27, 2021), *https://nymag.com/intelligencer/article/lina-khan-ftc-profile.html.*

[13] Kids Online Safety Act, S.3663, 117th Congress (2021–22), *https://www.congress.gov/bill/117th-congress/senate-bill/3663/text;Children* and Teens' Online Privacy Protection Act, S.1628, 117th Congress (2021–22), *https://www.congress.gov/bill/117th-congress/senate-bill/1628/text; see also* Cristiano Lima, *Senate panel advances bills to boost children's safety online,* Wash. Post (Jul. 27, 2022), *https://www.washingtonpost.com/technology/2022/07/27/senate-child-safety-bill/.*

[14] *See, e.g.,* Testimony of Jonathan Haidt, Teen Mental Health is Plummeting, and Social Media is a Major Contributing Cause, Before the Senate Judiciary Committee, Subcommittee on Technology, Privacy, and the Law (May 4, 2022), *https://www.judiciary.senate.gov/imo/media/doc/Haidt%20Testimony.pdf.*

[15] *Id.*

[16] I have given several speeches discussing these concerns. *See* Christine S. Wilson, The FTC's Role in Supporting Online Safety (Nov. 21, 2019), *https://www.ftc.gov/system/files/documents/public_statements/1557684/commissioner_wilson_remarks_at_the_family_online_safety_institute_11-21-19.pdf;* Christine S. Wilson, Opening Remarks at FTC Workshop: The Future of the COPPA Rule (Oct. 7, 2019), *https://www.ftc.gov/system/files/documents/public_statements/1547693/wilson__ftc_coppa_workshop_opening_remarks_10-7-19.pdf; see also* Christine S. Wilson, Remarks at Global Antitrust Institute, FTC v. *Facebook (Dec. 11, 2019), https://www.ftc.gov/system/files/documents/public_statements/1557534/commissioner_wilson_remarks_at_global_antitrust_institute_12112019.pdf* (discussing, inter alia, my work with staff to secure the provisions of the settlement that provide heightened review for products targeted to minors).

DEPARTMENT OF LABOR

Employee Benefits Security Administration

29 CFR Part 2570

RIN 1210–AC05

Reopening of Comment Period and Hearing Regarding Proposed Amendment to Procedures Governing the Filing and Processing of Prohibited Transaction Exemption Applications

AGENCY: Employee Benefits Security Administration.

ACTION: Hearing announcement and reopening of the comment period.

SUMMARY: The Department of Labor's Employee Benefits Security Administration (EBSA) will hold a virtual public hearing regarding the proposed amendment to its prohibited transaction exemption filing and processing procedures. EBSA welcomes requests from the general public to testify at the hearing.

As discussed in the **DATES** section below, the Department of Labor (the Department) also is reopening the comment period regarding the proposed amendment to its prohibited transaction exemption filing and processing procedures.

DATES: The public hearing will be held on September 15, 2022, and (if necessary) September 16, 2022, via WebEx beginning at 9 a.m. EDT. Requests to testify at the hearing should be submitted to the Department on or before September 8, 2022. The Department will reopen the comment period for the proposed amendment on September 15, 2022. The Department will publish a **Federal Register** notice announcing that the hearing transcript is available on EBSA's web page and when the reopened comment period closes.

ADDRESSES: Please submit all comments and requests to testify concerning the proposed rule to the Office of Exemption Determinations through the Federal eRulemaking Portal at *www.regulations.gov* using Docket ID number EBSA–2022–0003. Instructions are provided at the end of this notice.

FOR FURTHER INFORMATION CONTACT: Brian Shiker, Office of Exemption Determinations, EBSA, by phone at (202) 693–8552 (not a toll-free number) or email *shiker.brian@dol.gov.*

SUPPLEMENTARY INFORMATION:

Background

This spring, the Department published a proposed amendment (the Rule) that would update its existing procedures governing the filing and processing of applications for administrative exemptions from the prohibited transaction provisions of the Employee Retirement Income Security Act, the Internal Revenue Code, and the Federal Employees' Retirement System Act. The Rule was published in the **Federal Register** (87 FR 14722) on March 15, 2022.

The Department received 29 comment letters on the Rule before the public comment period ended on May 29, 2022. After consideration of the comments, including a written request for a public hearing, the Department has decided to hold a virtual public hearing to provide an opportunity for all interested parties to testify on material factual information regarding the Rule.

The hearing will be held via WebEx on September 15, 2022, and (if necessary) September 16, 2022, beginning at 9 a.m. EDT. It will be transcribed. Registration information to access and view the hearing will be available on EBSA's website: *www.dol.gov/agencies/ebsa.*

Instructions for Submitting Requests To Testify

Individuals and organizations interested in testifying at the public hearing must submit a written request to testify and a summary of their testimony by September 8, 2022. Requests to testify must include:

(1) the name, title, organization, address, email address, and telephone number of the individual who would testify;

(2) if applicable, the name of the organization(s) whose views would be represented;