BILLING CODE: 6750-01-P

FEDERAL TRADE COMMISSION

16 CFR Part 464

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 (1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.

DATES: Comments must be received on or before [60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. 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.

[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/.

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

---

[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).

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

---

[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.

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] Many privacy notices that acknowledge such risks are reportedly not readable to the average consumer.[22] Many consumers do not have the

---

[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 (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).

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.

---

[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).

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

---

[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-

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 forms and mechanisms for discrimination based on statutorily protected categories,[38] including in critical

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.").

[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).

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]

---

[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).

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

[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").

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 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

[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-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.).

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.

---

[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.

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]

---

[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).

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 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

[70] 15 U.S.C. 57a(b)(3).
[71] *Id.*
[72] 15 U.S.C. 45(n).

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

[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] Pub. L. No. 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.

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];

[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.

- 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];

[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 (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.

- 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];

---

[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.

- 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

---

[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*

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]

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

---

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 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.

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]

---

[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.

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

[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).

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 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]

---

[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).

[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.

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,

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.

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 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?

[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.

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 [60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. 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 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 [60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. 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 web site 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.

April J. Tabor, *Secretary*.