UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Commissioner
Noah Joshua Phillips

# Dissenting Statement of Commissioner Noah Joshua Phillips

*Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking*

August 11, 2022

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

National consumer privacy laws pose consequential questions, which is why I have said, repeatedly,[2] that Congress—not the Federal Trade Commission ("FTC" or "Commission")—is where national privacy law should be enacted. I am heartened to see Congress considering just such a law today,[3] and hope this Commission process does nothing to upset that consideration.

---

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

[2] *See, e.g.*, Statement of Commissioner Noah Joshua Phillips Regarding the Report to Congress on Privacy and Security (Oct. 1, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597020/commissioner_phillips_dissent_to_privacy_report_to_congress_updated_final_93021_for_posting.pdf; Sen. Roger Wicker, Rep. Cathy McMorris Rodgers & Noah Phillips, *FTC must leave privacy legislating to Congress*, WASH. EXAM'R (Sept. 29, 2021), https://www.washingtonexaminer.com/opinion/op-eds/ftc-must-leave-privacy-legislating-to-congress; Prepared Oral Statement of Commissioner Noah Joshua Phillips Before the House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce, Hearing on "Transforming the FTC: Legislation to Modernize Consumer Protection" (July 28, 2021), https://www.ftc.gov/system/files/documents/public_statements/1592981/prepared_statement_0728_house_ec_hearing_72821_for_posting.pdf.

[3] *See* Rebecca Klar, *House panel advances landmark federal data privacy bill*, THE HILL (July 20, 2022), https://thehill.com/policy/technology/3567822-house-panel-advances-landmark-federal-data-privacy-bill/; Press Release, House Committee on Energy and Commerce, *House and Senate Leaders Release Bipartisan Discussion*

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

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

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

The ANPR fails to live up to the promise in its name, to give advance notice to the public (and Congress) of what the Commission might propose. The FTC Act requires an ANPR to "contain a brief description of the area of inquiry under consideration, the objective which the Commission seeks to achieve, and possible regulatory alternatives under consideration by the Commission."[4] This ANPR flunks even that basic test. The areas of inquiry are vast and amorphous, and the objectives and regulatory alternatives are just not there. It is impossible to discern from this sprawling document—which meanders in and out of the jurisdiction of the FTC and goes far afield from traditional data privacy and security—the number and scope of rules the Commission envisions.[5] The document stands in stark contrast to the focus that characterizes recent ANPRs issued by the Commission, which addressed far more limited topics like impersonating a government entity or private business, deceptive earnings claims, or the scope of the Telemarketing Sales Rule.[6] I supported each of those.

---

*Draft of Comprehensive Data Privacy Bill* (June 3, 2022), https://energycommerce.house.gov/newsroom/press-releases/house-and-senate-leaders-release-bipartisan-discussion-draft-of.

[4] 15 U.S.C. § 57a(b)(2)(A)(i).

[5] The Commission is not even limiting itself to Section 18 rules that must follow the procedures laid out in Magnuson-Moss Warranty Act, Pub. L. No. 93-637, 88 Stat. 2183. The ANPR notes that it is requesting information on how commercial surveillance harms competition, which could inform competition rulemaking. Other commissioners may believe the Commission may promulgate such rules, including without an ANPR. I do not. *See* Prepared Remarks of Commissioner Noah Joshua Phillips at FTC Non-Compete Clauses in the Workplace Workshop (Jan. 9, 2020), https://www.ftc.gov/system/files/documents/public_statements/1561697/phillips_-_remarks_at_ftc_nca_workshop_1-9-20.pdf.

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

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

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

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

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

---

Telemarketing Sales Rule, 87 FR 33662 (June 3, 2022), https://www.federalregister.gov/documents/2022/06/03/2022-10922/telemarketing-sales-rule.

[7] *See* ANPR for Trade Regulation Rule on Commercial Surveillance and Data Security, _____ FR _____, at [Q.1]. [hereinafter ANPR].

[8] *Id.* at [Q.14]

[9] *Id.* at [Q.26].

[10] *Id.* at [Q.49].

[11] *Id.* at [Q.86].

[12] I am not sure what this means. Should the Commission be obtaining monetary redress for the cost of consumers' therapy? *Id.* at [Q.9]. Where conduct is not deceptive, the FTC Act only permits us to regulate conduct that causes "substantial injury". 15 U.S.C. § 45(n).

[13] ANPR at 24.

[14] *Id.*

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

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

*The ANPR Recasts the FTC as a Legislature*

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

The ANPR's many references to international and state privacy laws signal the majority's view that the scope of the rules passed by the unelected commissioners of an independent agency should be on par with statutes passed by elected legislators. Even as we vote, Congress is

---

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

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

[17] *Id.* at [Qs.24-29].

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

[19] *West Virginia v. EPA*, 597 U.S. ___, 2022 WL 2347278 (June 30, 2022) (slip op. at 20).

[20] 15 U.S.C. § 57a.

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

considering actively legislation concerning the very matters the ANPR purports to address.[22] I sincerely hope that this ill-advised process does not upset that very much needed one.

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

This ANPR, meanwhile, attempts to establish the prevalence necessary to justify broad commercial surveillance rulemaking by citing an amalgam of cases concerning very different business models and conduct.[27] Under Section 18, the agency must show that the unfair acts or practices in question are prevalent, a determination that can only be made if the Commission has previously "issued cease and desist orders regarding such acts or practices," or if it has any other information that "indicates a widespread pattern of unfair or deceptive acts or practices."[28] Where the agency has little (or no) experience, prudence counsels in favor of investigation to explore costs and benefits and to determine illegality. The ANPR aims for regulation without even any experience, to say nothing of court decisions ratifying the application of Section 5 to the business conduct in question. As this process moves forward, the Commission would do well to keep in mind that "[a]gencies have only those powers given to them by Congress, and

---

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

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

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

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

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

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

[28] 15 U.S.C. § 57a(b)(3).

'enabling legislation' is generally not an 'open book to which the agency [may] add pages and change the plot line.'"[29]

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

Consider also the ANPR's discussion of consent, one of the traditional bedrocks of privacy policy. Whether notice and consent is the optimal approach to consumer privacy in every context is worthy of serious debate. Instead of discussing the merits and shortcomings of transparency and choice, the majority simply concludes that "consent may be irrelevant."[33] The ANPR bolsters this view with claims that other privacy regimes are moving away from an emphasis on consent. Really? While there are certainly privacy laws that include data minimization requirements or restrict secondary uses of data, many still allow for consent. For example, the Children's Online Privacy Protection Act of 1998 requires parents to give verified parental consent before a business collects information from a child.[34] The European Union's General Data Protection Regulation ("GDPR") allows businesses to process data if they have the consumer's consent, which must be freely given, specific, informed, and unambiguous.[35]

The ANPR appears skeptical that consumers can be trusted to make their own choices, seeking information on what "commercial surveillance" practices are illegal, "irrespective of whether consumers consent to them."[36] Should the majority be thwarted in its quest to make consent passé, the ANPR contemplates at least having different consent standards for individuals

---

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

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

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

[32] *See* ANPR at [Q.62].

[33] *Id.* at 6.

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

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

[36] *See* ANPR at [Q.76].

"in crisis" or "especially vulnerable to deception."[37] This is paternalistic to say the least: Heaven forfend adults make decisions and permit companies to use their data to serve them targeted ads. But even if you disagree with that view, the point is that a consequential decision to take away that choice from individuals—like many of the decisions that need to be weighed in creating a national privacy law—is best left to Congress. The FTC is not a legislature.

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

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

*The ANPR is FTC Overreach*

The ANPR reaches outside the jurisdiction of the FTC. It seeks to recast the agency as a civil rights enforcer, contemplating policing algorithms for disparate impact without a statutory command.[43] This raises immediate concerns. First, do we have the authority? When Congress

---

[37] *Id.* at [Q.79].

[38] 15 U.S.C. § 6502.

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

[40] 15 U.S.C. § 6502.

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

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

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

seeks to ban discrimination, it says so directly.[44] The FTC Act does not mention discrimination. Second, the civil rights laws Congress has adopted to fight discrimination delineate the bases upon which discrimination is illegal.[45] The FTC Act does not. Third, our antidiscrimination laws cover aspects of commerce where Congress has expressed concern about the impact of discrimination, for example housing, employment, and the extension of credit.[46] The FTC Act applies broadly to any unfair or deceptive act or practice in or affecting commerce. Finally, the FTC Act does not specify whether it is a regime of disparate treatment or disparate impact.

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

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

---

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

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

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

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

[48] *See* ANPR at [Q.60].

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

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

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

---

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

[50] ANPR at [Q.12].

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

[52] *Id.* at [Q.39].

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

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

[55] *Id.* at [Q.62].

[56] *Id.* at [Q.63-64].

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

*The ANPR Gives Short Shrift to Critical Policy Issues within its Scope*

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

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

---

[58] *See* Health Breach Notification Rule, 16 C.F.R. Part 318; Gramm-Leach Bliley Act, Pub. L. No. 106-102, 112 Stat. 1338 (1999); Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505.

[59] *See* ANPR at [Q.10].

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

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

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

*Conclusion*

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

I would have supported an ANPR for a data security rule. I would have been more sympathetic to an ANPR that was focused on consumer privacy as reflected in our long record of enforcement and policy advocacy—say, a rule that, for example, would require transparency or that would, depending on the sensitivity of the information or the purposes for which it was collected, put some limits on the collection and use of consumer information. These ideas would be consistent with, among other things, Commission enforcement experience. I cannot support an ANPR that is the first step in a plan to go beyond the Commission's remit and outside its experience to issue rules that fundamentally alter the internet economy without a clear congressional mandate. That's not "democratizing" the FTC or using all "the tools in the FTC's toolbox." It's a naked power grab. I dissent.