1212 New York Ave. NW
Suite 900
Washington D.C. 20005
202-525-5717

Free Markets. Real Solutions.
rstreet.org

October 12, 2022

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington D.C. 20580

Re: Commercial Surveillance ANPR, R111004
Submitted Electronically

The R Street Institute (R Street) respectfully submits these comments in response to the advance notice of proposed rulemaking (ANPR) released Aug. 22, 2022 regarding the Federal Trade Commission's (FTC) potential rules on commercial surveillance and data security.

R Street shares the FTC's view that clarity and additional protections around data privacy and security are needed. We believe that effective data privacy and security rules are important for consumers, industry and national security. Other nations and U.S. states have acted, though the vast majority of Americans are left unprotected.[1]

At the outset, we appreciate the FTC's interest in this area. However, we believe the ANPR is premature and too expansive in scope. This is especially true since Congress is actively considering a comprehensive federal data privacy and security bill that would cover many of the same areas. There are also consequential policy questions that need to be decided, and the FTC's authority to reach into multiple of the areas outlined should be clarified. There are nonetheless actions the FTC can take now in anticipation of this bill and under existing authority.

We are hesitant to answer the specific questions outlined. However, some sections of our comments correspond with outlined questions and are noted as such.

[1] Anokhy Desai, "US State Privacy Legislation Tracker," International Association of Privacy Professionals, Oct. 7, 2022. https://iapp.org/resources/article/us-state-privacy-legislation-tracker.

I. R Street's report on reaching consensus on federal data privacy and security legislation calls for a strong, yet defined role for the FTC.

The R Street Institute's Cyber Team undertook a year-long study of the roadblocks to passing comprehensive federal data privacy and security legislation, which focused on preemption, the role of the FTC and a private right of action.[2] The goal was to identify consensus for federal legislation to address each barrier through engagement with over 120 stakeholders across the ideological spectrum from consumer advocacy to industry groups.

In our analysis, we advocated for the FTC to be the body responsible for data security and privacy instead of a new agency.[3] We acknowledge that unchecked or overly broad authority risks unwieldy regulation that could harm innovation and business, but too little authority risks insufficient protection from privacy harms and rigid protections that cannot adapt to rapidly changing technology.

Therefore, a balance through "guided FTC rulemaking" is essential.[4] This means Congress should establish clear guardrails and definitions around the type of rulemaking authority, targeted areas in which that authority could be applied and the means by which such efforts should be undertaken. Corresponding to **Question 95**, this includes allowing the FTC to update regulatory provisions as defined by Congress that it deems inadequate to address new harms through technological change, but the agency must demonstrate the need to do so through rulemaking procedures. This process would help counter obsolescence in rulemaking. Compliance and increased consumer data security and privacy should be the goal, not the collection of fines or the penalizing of entities—underscoring the importance of guardrails around any rules.

II. The ANPR is expansive and premature in light of congressional attempts to pass comprehensive federal data privacy and security legislation.

Congress has made great progress on a bipartisan, bicameral comprehensive data privacy and security bill with the American Data Privacy and Protection Act (ADPPA) passing out of committee with nearly unanimous consent.[5] This bill may not be perfect in every respect, but we believe it is an attempt to reach a middle ground.[6] Most significantly, this bill shows that Congress is actively considering data

---

[2] Tatyana Bolton et al., "The Path to Reaching Consensus for Federal Data Security and Privacy Legislation," R Street Institute and Harvard Belfer Center for Science and International Affairs, May 26, 2022. https://www.rstreet.org/2022/05/26/the-path-to-reaching-consensus-for-federal-data-security-and-privacy-legislation.

[3] Ibid.

[4] Tatyana Bolton et al., "The Role of the Federal Trade Commission in Federal Data Security and Privacy Legislation," R Street Institute and Harvard Belfer Center for Science and International Affairs, May 31, 2022. https://www.rstreet.org/2022/05/31/the-role-of-the-federal-trade-commission-in-federal-data-security-and-privacy-legislation.

[5] H.R 8152, American Data Privacy and Protection Act, 117th Congress.

[6] Brandon Pugh and Sofia Lesmes, "Marking Up Momentum: What's Next for the ADPPA," R Street Institute, July 21, 2022. https://www.rstreet.org/2022/07/21/marking-up-momentum-whats-next-for-the-adppa.

privacy and security legislation. We believe it is premature for the FTC to act without clear direction from Congress, especially while this legislation is pending a floor vote. In addition, since consequential decisions are at play that would have wide impacts, we believe it is best for Congress to act. The ANPR could further complicate the patchwork of privacy laws and regulations. As such, this section best answers **Questions 29 and 30** of the ANPR.

Congress has deliberately included areas for FTC rulemaking and action in the ADPPA, but the ANPR goes beyond them and does so prematurely without a federal law. For example, the ADPPA empowers the FTC to commence rulemaking for specific aspects of definitions, individual rights, third parties, large data holders, data security and protection of data, and technical compliance programs. The FTC is also empowered to make guidelines in certain areas like for data minimization, privacy by design, and algorithm impact and evaluation. These responsibilities are in addition to the FTC's clear roles in enforcement, public information, reporting, administration and tracking, decision making, victim relief and youth privacy under the ADPPA. While not specific, the ADPPA also provides for an appropriation to carry out the law.

In contrast to acting under Congress's narrower view for the FTC, the ANPR sets forth 95 questions on a wide range of issues from biometrics to targeted advertising. The rules' themes can even extend beyond this, since the ANPR states that it does not identify the full scope of potential approaches the FTC might undertake by a rule. If passed, final rules would impact many industries and multiple technologies—all without further congressional action. We acknowledge the FTC's existing authority to commence rulemaking under the FTC Act over certain areas, but we believe this scope goes far beyond what Congress has authorized and is significantly beyond clarifying existing authorities.

We recognize that the ANPR is not yet a proposal of final rules, but its breadth belies claims that the purpose is inquisitive in nature. If the ANPR focused on a narrower set of questions, like those highlighted by Commissioner Alvaro Bedoya, it would be easier to see the exercise as developing a useful record of information and collective understanding that could inform either future FTC proceedings or Congress's continued legislative plans.[7] Instead, the ANPR's relitigation of long-discussed data protection matters with normative merits that have been discussed in congressional proceedings (and many, many other places) for several years makes this appear not as an inquiry, but rather the FTC's first procedural step to shape the future themselves, directly, without waiting on or deferring to Congress.

The ANPR does not appear to be much different from what Justice Neil Gorsuch stated in a different context: agencies using "regulations as substitutes for laws."[8] For example, we share Commissioner Noah Phillips' belief that the ANPR contemplates even reaching to "common business practices [the FTC has]

---

[7] Office of Commissioner Alvaro M. Bedoya, "Statement of Commissioner Alvaro M. Bedoya," Federal Trade Commission, Aug. 11, 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/Bedoya%20ANPR%20Statement%2008112022.pdf.

[8] *West Virginia et al. v. Environmental Protection Agency et al.*, Supreme Court, June 30, 2022, p. 19. https://www.supremecourt.gov/opinions/21pdf/20-1530_n758.pdf.

never before even asserted are illegal."[9] In addition, Commissioner Rebecca Slaughter constructively lays out the substantive and procedural obstacles before the FTC in considering such broad rulemaking: 1) prohibitions can only apply to practices that are unfair or deceptive under the law, each of which involves a three step test; 2) the practices must not be theoretical but must in fact be "prevalent;" and 3) a rulemaking process cannot expand the FTC's authority beyond what it can adjudicate case-by-case today using existing Section 5 authority.[10] R Street's concern is that the questions raised in this ANPR and its implicit potential rules far exceed these guardrails.

However, we do not believe this means that the FTC needs to wait for Congress to act either. Data security is one area where the FTC could provide greater clarity, as explained below. In addition, the FTC should be preparing for possible federal legislation and supporting Congress with technical advice during the drafting and debating stages. While the exact details of that are not known, it is almost certain that the FTC will take on a greater enforcement role.

Lastly, we believe the broad nature of the ANPR should be pared back to focus on a narrower scope of areas that would allow for a deeper and more targeted study. This would better align with the FTC's stated goal of developing a public record to "help sharpen the Commission's enforcement work and may inform reform by Congress or other policymakers …"[11] Should the FTC be guided by congressional legislation to adopt broader rules than this, the agency would have procedural opportunity in a future notice of proposed rulemaking to expand appropriately, as directed. But with such a broad scope in an initial ANPR process, it is not clear what the FTC actually plans to do. And the voluminous burden of information production without clear focus will disproportionately affect nonprofit organizations and small businesses attempting to contribute to the FTC's record, as they are far less well-resourced than larger entities.

III. Data security is an area where greater clarity and focus would be beneficial.

Given the Cyber team's deep focus on data security and privacy, we would also like to provide high-level information applicable to the data security series of questions (**Questions 31-36**).[12]

---

[9] Office of Commissioner Noah Joshua Phillips, "Dissenting Statement of Commissioner Noah Joshua Phillips," Federal Trade Commission, Aug. 11, 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

[10] Office of Commissioner Rebecca Kelly Slaughter, "Statement of Commissioner Rebecca Kelly Slaughter," Federal Trade Commission, Aug. 11, 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/RKS%20ANPR%20Statement%2008112022.pdf.

[11] Federal Trade Commission, "*Trade Regulation Rule on Commercial Surveillance and Data Security*," Advanced Notice of Proposed Rulemaking, Docket No. 2022-0053, Aug. 22, 2022. https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

[12] Tatyana Bolton et al., "What does the newest U.S. privacy bill mean for cybersecurity?", International Association of Privacy Professionals, June 17, 2022. https://iapp.org/news/a/what-does-the-newest-u-s-privacy-bill-mean-for-cybersecurity; Tatyana Bolton et al., "Congress Needs to Start Caring About Our Privacy as Much as China Does," *R Street Policy Study* No. 232, June 14,

Data security is critical to data privacy. This is especially true given that access to personal information online increased by 150 percent from 2019 to 2021.[13] Not only is the amount of data constantly expanding, but security and privacy threats are increasing. There were a record number of data breaches in 2021—68 percent more than in 2020.[14] These numbers alone are concerning, but the scope and visibility of recent incidents highlights the problem.[15]

To add to this, data continues to be under risk from foreign threats, like China, who do not hesitate to collect it for intelligence or competition purposes—leaving Americans with a vague understanding of where their data is and how protected it is against malicious actors.[16] In a practical sense, this means ingraining data security standards into data processes to ensure both its security and privacy. However, it is difficult to understand what data security standards entail and how they are or should be defined.

The FTC could aid Congress and industry by outlining a standard of reasonableness for data security, which also benefits consumers and national security. However, any action on data security should be constrained and not used as an attempt to get broader measures through. The FTC should first carefully examine existing data security rules at the state, federal and international levels, including those targeting specific industries to help avoid conflicting provisions and unnecessary duplication and to compile best practices.[17]

According to Commissioner Phillips, data security is "one area ripe for FTC rulemaking."[18] A helpful addition would be for the FTC to streamline its data security rules, rather than use a case-by-case approach that can lead to uncertainty on what is needed to comply. This would serve as a way to put the public and industry on notice for what acts are needed and are reasonable, which could result in broader security compliance, more efficient enforcement for violations and enhanced data protection overall.

2021.
https://www.rstreet.org/2021/06/14/congress-needs-to-start-caring-about-our-privacy-as-much-as-china-does.

[13] "DeleteMe 2021 PII Marketplace Report," DeleteMe, January 2022. p. 3.
https://joindeleteme.com/wp-content/uploads/2022/01/2021-DeleteMe-PII-Marketplace-Report.pdf.

[14] "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Identity Theft Resource Center, Jan. 24, 2022.
https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[15] Aaron Drapkin, "Data Breaches That Have Happened in 2022 So Far," *Tech.co,* Oct. 11, 2022.
https://tech.co/news/data-breaches-2022-so-far.

[16] Brandon J. Pugh, "Lessons for America from China's Massive Data Breach," *RealClearPolicy,* July 19, 2022.
https://www.realclearpolicy.com/articles/2022/07/19/lessons_for_america_from_chinas_massive_data_breach_843154.html.

[17] "FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches," Federal Trade Commission, Oct. 27, 2021.
https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data.

[18] Office of Commissioner Noah Joshua Phillips.
https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

This would especially be true in the case of the ADPPA passing, and the law and FTC rules should subsequently complement each other, even though the ADPPA largely defers to the FTC on data security.

Consider breach notification requirements. Up to now, the Commission has issued a mixture of guidance and documentation that argues for the implication of a requirement for companies to notify their customers in case of a data breach—but uncertainty still looms large in the process.[19]

There are a vast number of considerations that warrant individual attention. These include what specific measures are necessary; incentives to implement security measures; how entities can be assisted in their security journey; the role of other federal agencies like the Cybersecurity and Infrastructure Security Agency; how privacy programs interact with security programs; how existing security frameworks are impacted or can serve as a resource, like those of the National Institute of Standards and Technology; additional components in privacy notices pertaining to security like transfers to select foreign nations; and how the measures can be assessed and/or monitored. After all, administrative, technical and physical safeguards are all important aspects to security, but what is covered can range widely. For example, implementing multi-factor authentication alone, while a great first step, is far from an advanced zero trust architecture. We recommend a more granular analysis on data security, including targeted questions and feedback from a wide range of industries and security experts. To its credit, the FTC has placed attention on security in the past.[20]

While security baselines are helpful, there should be flexibility and special considerations based on the specific data and entity type because one size does not fit all. On the data side, the type, amount, sensitivity and use are important. On the entity side, the size and type, cost and resources, and feasibility of implementation are key. For example, a small local business generally does not need the same security measures as a massive company engaged in data collection. Similarly, not all companies will have the capability to enact the same security measures. This might require exemption of certain types of entities and/or relaxed rules.

Conclusion

We deeply support efforts to increase data privacy and security. While we may disagree with the approach and scope of the ANPR, we are happy to be a resource on specific issues that arise, especially relating to data security. Data privacy and security are important for consumers, industry and national security.

---

[19] Team CTO and the Division of Privacy and Identity Protection, "Security Beyond Prevention: The Importance of Effective Breach Disclosures," Federal Trade Commission, May 20, 2022. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/05/security-beyond-prevention-importance-effective-breach-disclosures.

[20] Office of Commissioner Noah Joshua Phillips. https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

Respectfully submitted,

Brandon J. Pugh
Senior Fellow, Cybersecurity & Emerging Threats

Chris Riley
Senior Fellow, Internet Governance

R Street Institute
1212 New York Ave. NW
Suite 900
Washington, D.C. 20005

Contact: bpugh@rstreet.org