United States Senate
WASHINGTON, DC 20510

November 3rd, 2022

Chair Lina Khan
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chair Khan,

We write to express our strong opposition to the Advanced Notice of Proposed Rulemaking (ANPR) for the Trade Regulation Rule on Commercial Surveillance and Data Security published by the Federal Trade Commission (FTC) on 8/22/22.[1] Consumer data privacy and security are complex issues which will require standards that are robust, adaptive, and can balance the interests of consumers with the needs of businesses. We believe that this balance can only be struck within federal legislation that is comprehensive and preemptive, such that the law creates a single national standard. Without federal preemption, any new privacy rules issued by the FTC would only add to the existing 'patchwork' of state privacy laws and create an additional layer of requirements for businesses. Rather than provide clarity to stakeholders, the proposed rulemaking action would only complicate the regulatory landscape in a way that would potentially increase compliance costs for businesses, reduce competition, and create confusion. Regardless of the outcome, the existence of debate in Congress over data privacy legislation indicates that Congress itself is where this debate should occur, not at the FTC. Therefore, the FTC should not exceed its authority to set national standards for data privacy and security and should instead leave that work to Congress.

As of this writing, five states (California, Colorado, Connecticut, Utah, and Virginia) have passed wide-ranging data privacy laws that set rules around how consumer data may be collected, used, and shared. Although these laws contain many similarities, they also vary along dimensions including processing limitations, transparency requirements, and definitions of sensitive data.[2] These differing standards can result in additional compliance costs for businesses, which often stifles innovation. As more states pass data privacy laws, compliance costs will only increase. In a recent report, the Information Technology and Innovation Foundation (ITIF) estimated the cost of a patchwork of state laws, projecting the costs resulting from businesses complying with multiple out-of-state privacy laws to be upwards of $112 billion annually.[3] The effects of these compliance costs would likely be felt disproportionally by small businesses that cannot take advantage of economies of scale to reduce the marginal cost of

[1] Federal Trade Commission. "Trade Regulation Rule on Commercial Surveillance and Data Security." Federal Register, August 22, 2022. https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.
[2] Livley, Taylor Kay. "US State Privacy Legislation Tracker." International Association of Privacy Professionals, August 11, 2022. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[3] Castro, Daniel, Luke Dascoli, and Gillian Diebold. "The Looming Cost of a Patchwork of State Privacy Laws." Information Technology & Innovation Foundation, January 24, 2022. https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

compliance. Of the compliance costs following from out-of-state laws, the ITIF estimates that small businesses would shoulder around $23 billion annually.

By undertaking this rulemaking action, the FTC will only add to the compliance burden facing small businesses. Rules enacted through this process may exist on top of the frameworks currently in state privacy laws. Because it is unclear if the FTC's final rule will fully preempt state legislation in all relevant areas of data use in the economy, the result of the FTC's actions could add another piece to the patchwork of requirements that currently exist. Moreover, these rules would often overlap with components of existing and proposed state laws. In questions 43 and 83 of the ANPR, the FTC asks for feedback on whether rules should impose requirements for purpose limitation and transparency. This is a major component of multiple state laws and leads us to believe that the FTC intends to issue rules which could overlap with them. This overlap could further increase the compliance costs for businesses which already must implement multiple states' standards. As a result of these additional costs, we are concerned that this rulemaking would ultimately reduce competition in digital markets to the detriment of consumers by potentially forcing small businesses to exit the market and creating new barriers for entry. At a time when many are rightly concerned about the concentration of digital markets, this rulemaking would likely only further worsen that problem.

Beyond increasing compliance costs, a more complex regulatory landscape increases uncertainty for businesses and alters perceptions of risk. This too can have negative effects for competition. In an academic study on the effects of the European Union's General Data Protection Regulation (GDPR) on web technology providers, a team of authors found that large web technology firms benefited from regulatory uncertainty following the implementation of the GDPR while smaller providers suffered.[4] The authors suggest that website operators responding to compliance risk may have selected larger web technology firms more likely to 'weather' compliance challenges. A similar outcome may arise in the United States if the rules enacted lead to greater uncertainty and higher perceptions of enforcement risk by firms.

The uncertainty facing businesses would only be compounded where state laws differ or conflict with the FTC's rules. Where state laws differ from each other, any FTC rule would necessarily preference the standards of one law over another. This would place the FTC as the arbiter of state laws by creating a *de facto* national default. In his dissenting opinion on the ANPR, former Commissioner Noah Phillips mirrors this concern, stating that the ANPR, "recasts the FTC as a legislature."[5] In addition, by potentially establishing conflicting rules, this process could lead to situations where businesses would be forced to decide whether to implement state or FTC standards. As more states consider and pass comprehensive data privacy legislation, the potential for these conflicts to arise increases.

Crafting rules for consumer data privacy and security is an important undertaking that must be done with care to balance consumer interests with business needs across the entire United States.

---

[4] Peukert, Christian, Stefan Bechtold, Michail Batikas, and Tobias Kretschmer. "Regulatory Spillovers and Data Governance: Evidence from the GDPR." Marketing Science 41, no. 4 (February 15, 2022): 318–40.
[5] Phillips, Noah Joshua. "Dissenting Statement of Commissioner Noah Joshua Phillips," August 11, 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

We believe that the preemption of state privacy laws is essential to this effort to avoid the costs that would result from a patchwork of privacy laws. As the Supreme Court has recently reinforced, agencies must stay within their statutory grant of power, and should not create rules where they have not been granted authority to do so by Congress.[6] Because the FTC lacks the authority to create preemptive standards, this rulemaking would only add uncertainty and confusion to an already complicated regulatory landscape, increasing compliance costs, reducing competition, and ultimately harming consumers.

In their opinions, all five Commissioners voiced support for federal privacy legislation as the preferred option for creating data privacy standards. In her dissenting opinion, Commissioner Christine Wilson further argues that this ANPR will hinder negotiations on federal privacy legislation currently under consideration in Congress.[7] We agree with her conclusion and further argue that Congress is the only appropriate venue for developing rules for data privacy and security and to set a truly national standard.

For all the above reasons, we urge the FTC to withdraw this ANPR and leave the task of creating data privacy and security rules to the elected officials in Congress.

Sincerely,

Cynthia Lummis
United States Senator

Marco Rubio
United States Senator

Kevin Cramer
United States Senator

[6] *West Virginia v. EPA*, 2022 WL 2347278 (June 30, 2022) (slip op. at 20).
[7] Wilson, Christine. "Dissenting Statement of Commissioner Christine S. Wilson Trade Regulation Rule on Commercial Surveillance and Data Security," August 11, 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Wilson%20Dissent%20ANPRM%20FINAL%2008112022.pdf.

CC:

Commissioner Rebecca Kelly Slaughter
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Commissioner Christine Wilson
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Commissioner Alvaro Bedoya
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580