Before the

Federal Trade Commission

Washington, D.C. 20580

Comments of the

Competitive Enterprise Institute

In the Matter of	)	
	)	
Federal Trade Commission	)	Commercial Surveillance ANPR
	)	R1110004
	)	
Advanced Notice of	)	
Proposed Rulemaking in the Matter of	)	
Trade Regulation Rule on Commercial	)	
Surveillance and Data Security	)	

November 21, 2022

Ryan Nabil
Competitive Enterprise Institute
1310 L Street NW, 7th Floor
Washington, D.C. 20005

Introduction

On behalf of the Competitive Enterprise Institute (CEI), I respectfully submit the following comments in response to the Federal Trade Commission's (FTC) advanced notice of proposed rulemaking (ANPR) and request for comment on data security and commercial surveillance practices that harm consumers. Founded in 1984, the Competitive Enterprise Institute is a non-profit research and advocacy organization focusing on regulatory policy from a pro-market perspective. CEI experts research and advocate policies to boost American technological innovation and economic competitiveness through technology policy and regulatory reforms in data privacy, artificial intelligence, and platform regulation, among other issues.

The Competitive Enterprise Institute appreciates the intention of the FTC to improve data privacy and security practices in the United States and the Commission's efforts to solicit public comment on whether new trade regulation rules on commercial surveillance and data security are necessary.[1] CEI has five primary responses to the FTC's ANPR inquiry, which are summarized below.

1) The advanced notice of proposed rulemaking's broad scope exceeds the FTC's statutory authority.

2) Absent Congressional authorization, the Commission should focus on addressing specific privacy-related harms and fraud as provided for by the Federal Trade Commission Act.

3) The FTC should explore regulatory alternatives, such as advisory guidelines and policy statements, instead of mainly relying on formal rulemaking processes.

4) The Commission should ask Congress to create a privacy sandbox, which would allow startups and established companies to offer innovative privacy solutions under a lightened regulatory framework for a limited time. By allowing regulators and the private sector to work closely together, a privacy sandbox could enable the FTC and Congress to better calibrate privacy laws and regulations in keeping with changing technological developments.

5) The FTC should examine international legislative and regulatory developments to help Congress develop a federal privacy framework that can better balance the competing priorities of privacy, data and national security, commercial needs, and innovation.

I. The advanced notice of proposed rulemaking's broad scope exceeds the Federal Trade Commission's statutory authority

The broad scope of the FTC's recent advanced notice of proposed rulemaking exceeds the Commission's statutory authority and is inconsistent with the Commission's recent practice. In the 1970s, the FTC's rulemaking based on a broad conception of "fairness" had few limits. That prompted Congress to step in and curb the Commission's regulatory powers. Since then, FTC rulemaking has traditionally been rooted in identifiable harm, cost-benefit considerations, and economic analysis. That, in turn, has allowed the Commission to play a constructive, impartial role in protecting American consumers and enabling technological innovation.[2]

[1] Federal Trade Commission (FTC), "Trade Regulation Rule on Commercial Surveillance and Data Security," Federal Register, Vol. 87, No. 161 (October 21, 2022), pp. 51273-51298, https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

[2] Berin Szóka, Bilal Sayyed, and Andy Jung, "TechFreedom Delivers Remarks at FTC's Commercial Surveillance and Data Security Public Forum," TechFreedom, September 8, 2022, https://techfreedom.org/techfreedom-delivers-remarks-at-ftcs-commercial-surveillance-and-data-security-public-forum/.

However, the Commission's recent inquiry veers from its usually restrained approach to rulemaking. Instead of focusing on specific privacy issues, the FTC asks a series of 95 overly broad questions—from youth protection and commercial surveillance practices to algorithmic fairness and error—many of which fall beyond the traditional scope of the agency's harm-focused approach.[3] The Commission also asks a series of questions related to "unfair methods of competition rulemaking"—a power that Congress has not vested in the FTC.[4] Many such overly broad questions potentially affect the entire U.S. digital economy and implicate the major questions doctrine. As such, these issues are better addressed by Congress.

The FTC could argue that it intends to use the ANPR findings to inform Congress of a sound approach for a federal data privacy framework, but that does not appear to be the case. For example, in the ANPR, the FTC solicits public comment on biometrics, data minimization, and other data protection-related issues that Congress has extensively discussed in multiple legislative sessions and hearings, especially in the context of the recently proposed American Data Protection and Privacy Act (ADPPA).[5]

Given Congress' already extensive consideration of these issues, the benefit to lawmakers from the FTC repeating such questions is limited. Instead, the broad range of questions and the FTC's recent efforts to expand its privacy jurisdiction makes it likely that this ANPR is the first procedural step in the Commission's efforts to redefine and shape the future of data privacy law without Congressional authorization.[6]

The ANPR's timing also suggests a disconnect between Congress and the FTC and the Commission's lack of willingness to work with lawmakers on privacy-related issues. There is a growing need for federal privacy legislation that preempts proliferating state-level privacy laws. Against this backdrop, the American Data Protection and Privacy Act was introduced in the House of Representatives in June 2022.[7] Despite the bipartisan support for the proposed law, it featured many flaws. For example, the draft legislation's long list of exemptions would limit its preemption powers for state privacy statutes.[8] However, instead of voicing such concerns and working with Congress to improve the legislation, the FTC appears more intent on making unilateral privacy rulings as a regulator.

Moreover, the Commission's recent actions suggest it is willing to act beyond its statutory authority. For example, the proposed ADPPA specifies areas over which the FTC could exercise rulemaking and enforcement authority, including the definition of data security, individual rights, and the rights of third parties. The draft bill also proposes granting the FTC authority to craft regulatory guidelines in areas such as privacy by design, data minimization, and algorithm auditing. However, instead of acting within this narrow role under the ADPPA, the Commission seeks to expand its regulatory powers using an overly broad interpretation of its statutory authority.[9] Instead, the FTC should work with Congress to clarify

---

[3] Szóka, Sayyed, and Jung.
[4] Senators Cynthia Lummis, Marco Rubio, and Kevin Cramer, Letter to Federal Trade Commission Chair Lina Khan on Commercial Surveillance and Data Security, November 3, 2022, https://senatorkevincramer.app.box.com/s/e35b6picvfivkhxzmcchh2omuxqavx56.
[5] Brandon Pugh and Chris Riley, R Street Institute Comments on FTC's ANPR on Commercial Surveillance and Data Security, Federal Trade Commission, R111004, October 12, 2022, https://www.rstreet.org/2022/10/24/r-street-institute-comments-on-ftcs-anpr-on-commercial-surveillance-and-data-security/.
[6] Ibid.
[7] H.R. 8152 – American Data Privacy and Protection Act, 117th Congress, 2nd Session, https://www.congress.gov/bill/117th-congress/house-bill/8152/text.
[8] Ryan Nabil, "The American Data Privacy and Protection Act Fails to Streamline Privacy Laws Nationwide and Promote Technological Innovation," *Competitive Enterprise Institute Blog*, June 15, 2022, https://cei.org/blog/the-american-data-privacy-and-protection-act-fails-to-streamline-privacy-laws-nationwide-and-promote-technological-innovation/.
[9] Pugh and Riley.

which additional responsibilities the Commission might need to carry out its role as a privacy regulator going forward.

Ultimately, the more the FTC tries to extend its regulatory authority in data privacy, the more likely it is that such actions will be met with legal challenges. To withstand legal challenges, the FTC must show that Section 18 of the FTC Act grants the Commission the legal authority to make privacy laws. While the Commission has statutory authority to pass regulations relating to unfair and deceptive practices, the Federal Trade Commission Act did not grant the agency the authority to issue rules on account of "fair methods" of competition. The FTC will also need to demonstrate that its rulemaking addresses data practices that lead to substantial injury to consumers, are not counterweighed by potential benefits, and are not reasonably avoidable by consumers.[10] Rulemaking on many privacy issues that the Commission is considering in this ANPR will likely fail this test.

The Commission's actions could also lead to regulatory confusion. Unilateral FTC privacy rulings—coupled with the proliferation of state privacy laws—would make it more challenging to create a unified federal privacy framework and worsen the increasingly confusing patchwork of privacy rules across the nation.

Furthermore, the overly broad questions in the ANPR affect practically all sectors of the U.S. economy. As such, these issues invoke the major questions doctrine, which holds that policy matters of "vast economic and political significance" should not be decided by agencies without statutory authority but by Congress.[11] The Supreme Court's recent ruling in *West Virginia v. EPA* makes it likely that courts will strike down the FTC's attempt to impose privacy rules that impact the entire U.S. digital economy without Congressional authorization.[12] Such a development will delay the creation of a unified federal privacy framework and erode the FTC's reputation as a neutral arbiter—which is all the more critical because of its possible future role as a Congressionally mandated privacy regulator.

II. The Commission's efforts should focus on specific harms as provided by existing law

Under its current leadership, the FTC increasingly seeks to use fairness grounds to expand the Commission's regulatory powers and upend privacy law. As noted earlier, an overly broad interpretation of the Commission's statutory authority will likely be met with legal challenges. Instead, the FTC should focus its efforts on addressing instances of specific harms and fraud, where agency guidelines and rulemaking could provide needed clarity to data governance principles.[13]

Under the Federal Trade Commission Act, the Commission's privacy powers are limited to specific instances, such as practices that involve consumer harm, injury, or fraud. While Congress may appoint the FTC as a data privacy regulator and impose proper checks and balances for enforcement actions, the Commission does not yet have the legislative authority to act as the country's privacy regulator.[14]

One area in which the FTC could play a constructive role is data security. By working closely with other regulatory agencies and the private sector, the Commission could play a significant role in enabling the

[10] 15 U.S.C. § 45(n); Jeffrey Westling and Joshua Levine, Comments of Jeffrey Westling and Joshua Levine in the Matter of Commercial Surveillance ANPRM, Federal Trade Commission, R1110004, October 26, 2022, https://www.americanactionforum.org/comments-for-record/commercial-surveillance-anprm/.
[11] Kate R. Bowers, "The Major Questions Doctrine," *Congressional Research Service*, updated November 2, 2022, https://crsreports.congress.gov/product/pdf/IF/IF12077.
[12] Westling and Levine.
[13] Ibid. Pugh and Riley.
[14] Westling and Levine.

private sector to better protect user data. The number of data breaches and other data security issues has increased in recent years, with some data breaches related to lax cybersecurity practices. Cyberattacks from both non-state actors and foreign state-sponsored groups have also increased. As a result, there is a growing need for more robust privacy and cybersecurity guidelines to help the private sector better protect user data against such emerging threats. [15]

The FTC could also take steps to prevent improper access to consumer and business data. That is especially important due to growing concerns that private companies could share sensitive user information with foreign government-affiliated organizations without users' knowledge. The Commission could help ensure that U.S.-domiciled user data are not improperly shared with U.S. and foreign government entities.[16] To that end, the FTC could review relevant data practices, issue policy statements, initiate formal rulemaking processes, and take regulatory action in coordination with other agencies.

III. The FTC should explore alternative methods to address specific privacy issues

As the Commission focuses on privacy cases with provable harm, it should use a more comprehensive range of policy tools instead of relying mainly on rulemaking for three reasons.

First, the FTC is legally obligated to consider such alternative means even in cases of specific harm.[17]

Second, the lengthy rulemaking processes often struggle to keep up with technological developments, which happen quickly. Some policy tools, such as advisory policy statements, are swifter and more adaptable and can help the FTC become more flexible in responding effectively to consumers' and businesses' different needs. For example, developing a platform for sharing best cybersecurity practices and issuing policy statements could help companies develop internal privacy guidelines to protect against cyber threats. [18]

Third, litigation can help create a body of case law that companies could look to for guidance regarding rapidly developing fields such as cybersecurity.

IV. The FTC should work with Congress to create a privacy sandbox

Creating a regulatory sandbox for data protection and privacy would help U.S. policymakers and companies better navigate the rapidly changing technology and data privacy landscape. As new technologies change ways of doing business, there is a growing need for a flexible regulatory approach toward data governance. That is where a regulatory sandbox can help by allowing companies to offer innovative products and enabling closer interaction between regulators and companies.

A company could apply to join a privacy sandbox to offer an innovative product or service—for example, a messaging app that uses quantum-proof encryption techniques—that might not exist in the U.S. market. By joining the sandbox, the company receives regulatory guidance and exemption from specific regulations. As innovative startups and companies offer new products through the sandbox, it has the potential to help improve data security and privacy for consumers and businesses alike.

[15] Pugh and Riley.
[16] Ibid.
[17] Westling and Levine.
[18] Szóka, Sayyed, and Jung.

Meanwhile, by working with innovative companies, policymakers can better understand emerging technologies and the entities they seek to regulate and craft more flexible, business-friendly rules that reflect the most recent technological developments and business practices.

As of this writing, there is no privacy sandbox in the United States, but the Consumer Financial Protection Bureau and several states run financial technology sandbox programs.[19] Likewise, as envisaged in the draft Artificial Intelligence Act legislation of the European Union, EU members such as Spain are setting up regulatory sandboxes to promote AI innovation.[20] The FTC should examine such programs to understand how a U.S. privacy sandbox could be designed and implemented.

Creating a privacy sandbox raises many jurisdictional issues that Congress must address. Therefore, the legal framework for a sandbox would be best established within the context of a comprehensive federal privacy law. However, the FTC's current statutory role as a privacy regulator is limited. Therefore, Congress will ultimately need to establish the legal framework for a privacy sandbox and clarify whether the FTC, another regulator, or a group of regulators will oversee the sandbox program. Moreover, a potential sandbox participant could be subject to the overlapping jurisdiction of multiple regulators—such as the Consumer Financial Protection Bureau, the Federal Communications Commission, and the Federal Trade Commission—for proposed business activity within the sandbox. Congress will need to set rules for interagency coordination in such cases and clear limitations on the power of each agency.

V. The FTC should examine international legislative and regulatory developments to help Congress develop a balanced federal privacy framework

The FTC should develop a mechanism to study major privacy regimes worldwide to understand how different privacy rules affect consumers and businesses and how similar rules might impact the U.S. economy. The United States, unlike many other developed countries, does not have a comprehensive national privacy law. In the absence of federal privacy law, the growing number of state-level privacy statutes risks creating a fragmented U.S. digital economy. To prevent this confusing regulatory patchwork, Congress needs to pass data privacy legislation and create a unified national privacy framework.[21]

Other countries' national privacy laws can provide a comparative advantage for the United States. Studying them could help U.S. policymakers better understand different approaches to data governance and their impact on privacy and innovation, as well as weigh the regulatory costs associated with different requirements against their potential innovation benefits. Privacy regimes the FTC should examine include

[19] Ryan Nabil, "How Regulatory Sandbox Programs Can Promote Technological Innovation and Consumer Welfare: Insights from Federal and State Experience," *OnPoint* No. 281, Competitive Enterprise Institute, August 17, 2022, https://cei.org/studies/how-regulatory-sandbox-programs-can-promote-technological-innovation-and-consumer-welfare/.

[20] As of this writing, the European Union is in the process of finalizing the text of the AI Act. The final text will need to be approved by the EU's Telecommunications Council at the upcoming December 6 meeting and then passed into EU law by the European Parliament along with the Council of the EU. Ben Wodecki, "EU AI Act Edges Closer to Passage," *AI Business*, November 21, 2022, https://aibusiness.com/responsible-ai/eu-ai-act-edges-closer-to-passage. European Commission, "First regulatory sandbox on Artificial Intelligence presented," Digibyte, June 27, 2022, https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented. The Future Society, "TFS champions Regulatory Sandboxes in the EU AI Act," The AI Initiative, June 28, 2022, https://thefuturesociety.org/2022/06/28/tfs-champions-regulatory-sandboxes-in-the-eu-ai-act/.

[21] Ryan Nabil, "Congress can prevent an over-regulated US digital economy. Here's how," *The Hill*, June 8, 2022, https://thehill.com/opinion/technology/3515282-congress-can-prevent-an-over-regulated-us-digital-economy-heres-how/.

those of the European Union, United Kingdom, Australia, Canada, Japan, South Korea, and other comparable jurisdictions.

A mechanism to evaluate international privacy developments can also advise Congress on how to update federal privacy law if necessary. Since the FTC's powers as a privacy regulator remain limited, the Commission should work with lawmakers to develop a national privacy framework that balances the competing priorities of privacy, data and national security, commercial needs, and innovation.

Such a privacy law should delineate the FTC's expanded responsibilities as a privacy regulator and set limits to its statutory authority. The Commission should recognize such restrictions and operate strictly within the limitations such a law would specify.

Conclusion

The Federal Trade Commission has a vital role in preventing data misuse and online harm in America's growing digital economy. Ultimately, the United States needs a federal privacy framework that preempts the growing patchwork of state-level privacy laws. Such a framework will affect all areas of the U.S. economy. Therefore, that is an issue for Congress—not the FTC—to decide. When Congress creates such a framework, the Commission should enforce privacy rules within the statutory bounds of that framework. Until then, the FTC should refrain from privacy rulemaking except in cases of explicit harm to consumers and businesses.

Respectfully submitted,

Ryan Nabil
Research Fellow
Competitive Enterprise Institute