U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

November 21, 2022

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Advance Notice of Proposed Rulemaking; Extension of Comment Period, Federal Trade Commission; Trade Regulation Rule on Commercial Surveillance and Data Security *Commercial Surveillance ANPR," R111004* (87 Fed. Reg. 63,738-63,739, October 20, 2022)

Dear Commissioners:

The U.S. Chamber of Commerce ("the Chamber") appreciates the opportunity to comment to the Federal Trade Commission ("FTC" or "Commission") regarding its proposed "Trade Regulation Rule on Commercial Surveillance and Data Security" ("Proposed Rule" or "ANPR").[1]

I. Executive Summary

The Chamber has long advocated for a clear and truly national privacy law that protects all Americans equally,[2] but given open questions (including questions posed in the ANPR) about the limits of the Commission's statutory authority, only Congress can achieve this goal. Anything short of federal legislation would only add to the already complex patchwork of laws and regulations purporting to govern privacy and data security. An economywide comprehensive privacy, algorithmic, and security rule promulgated by FTC raises serious legal concerns.

The data-driven economy provides unparalleled benefits to society. It enables greater affordability of goods and services, empowers small business, enhances public safety, provides more nimble and robust public health responses, and promotes financial inclusion. For the United States to continue to reap the benefits of this data-driven economy and compete against countries that do not share our values in a free-market economy and democracy, there must be trust. Consumers should trust that their data is protected and respected by innovators and companies. Businesses and consumers should trust that the government will provide clear rules and enforcement that prevent nefarious actors from harming consumers. Finally, all citizens must trust that government agencies will honor the Constitution and due process.

[1] 87 Fed. Reg. 51273 *available at* https://www.govinfo.gov/content/pkg/FR-2022-08-22/pdf/2022-17752.pdf.
[2] https://www.uschamber.com/technology/data-privacy/us-chambers-model-data-privacy-legislation.

A trade rule on privacy, security, and algorithms would add a new layer of confusion both for consumers and businesses striving to innovate while remaining compliant, and lead to major negative impacts on the U.S. economy.

The Federal Trade Commission should halt the current rulemaking because: 1) a comprehensive privacy rule and many of the individual proposals in the ANPR exceed FTC's statutory authority; 2) the ANPR itself fails to meet the requirements of Section 18 of the FTC Act; and 3) many of the proposals in the APNR would impede innovation, harm consumers, and negatively impact the ability of businesses—particularly small ones, including minority-, veteran-, and woman-owned companies—to compete.

II. The Proposed Rules Exceed FTC's Authority.

A. The Major Questions Doctrine

The rule contemplated by the ANPR would violate the Supreme Court's "major questions doctrine," because the history and breadth of FTC's asserted authority, as well as the economic and political significance of that asserted authority, are such that Congress would not have delegated it to the FTC absent clear authorization, which the FTC lacks. Federal agencies must operate within their constitutional authority. The Constitution established the principle of separation of powers so that no branch (or agency) of government may act as legislator, judge, and enforcer. An important component of the Constitution's separation of powers is that the power to legislate rests with the legislative branch, which can delegate its policymaking authority to executive agencies only under defined circumstances.

The Supreme Court recently reaffirmed this principle in *West Virginia v. Environmental Protection Agency*, stating that "in certain extraordinary cases, both separation of powers and a practical understanding of legislative intent make [the Court] 'reluctant to read into ambiguous statutory text' the delegation claimed to be lurking there" by federal agencies.[3] The Court instructed that the "history and breadth of the [asserted] authority" can mark a regulation as imposing upon the major questions doctrine, as can the "economic and political significance" of the asserted authority.[4] The Court typically views assertions of extravagant authority over the national economy with skepticism.[5] The Court's analysis makes clear that the ANPR is attempting to resolve major questions without congressional authorization.

1. A Comprehensive Privacy, Security, and Algorithmic Rulemaking Has Major Economic and Political Significance

[3] *West Virginia v. Environmental Protection Agency*, 142 S. Ct. 2587, 2609 (2002) (quoting *Utility Air Regulatory Group v. EPA*, 573 U.S. 302, 324 (2014)).
[4] *Id.* at 2608
[5] *Id*. at 2609.

The regulation of data would significantly impact the U.S. economy. Data is core to the fundamental business decisions of every company in America. Data is also key to the United States' competitiveness and to improving the lives of Americans. The internet economy was estimated to have contributed $2.45 trillion to U.S. GDP.[6] Artificial Intelligence alone will have a $3.7 trillion positive impact on North American GDP by 2030.[7] Small businesses that utilize technology platforms like business software, social media, delivery apps, and payment support the jobs of nearly 100 million Americans and $17.7 trillion in economic value.[8] On a practical level, the data-driven economy is enhancing public safety by stopping violent crime, preventing and detecting fraud, promoting financial inclusion by using expanded datasets, and improving health outcomes.[9]

The text of the ANPR clearly indicates the Commission is contemplating making "rules [that] apply economy-wide" in the context of automated decision-making systems.[10] Given the Commission's own questions in the ANPR and the clear significant and political impact, a comprehensive trade rule regarding data privacy, security, and algorithms would be an extravagant assertion of authority by an independent agency over the national economy.

2. The Breadth and History of the Asserted Authority Show the ANPR Addresses Major Questions

The breadth of the authority the FTC claims in the ANPR shows that the FTC is asserting authority over major questions. In *West Virginia v. EPA*, the Court rejected the idea that Congress would "implicitly task[]" the EPA "with balancing the many vital considerations of national policy implicated in deciding how Americans will get their energy."[11] Instead, the Court will presume that "[t]he basic and consequential tradeoffs involved in such a choice are ones that Congress would likely have intended for itself."[12] The same is true of the ANPR, which—as discussed above—seeks to regulate a broad range of important questions touching on a wide swath of the American economy. That authority would commit to the FTC the power to make tradeoffs that determine the course of American commerce—the power to "settle or amend major social and economic policy decisions."[13] One example of such a tradeoff is contemplated in Question 52 of the ANPR, which asks whether a new trade rule should require interoperability as well as consumer data access.[14] Such a question requires important debate about whether privacy requirements such as consumer data consent or deletion requirements

[6] https://www.iab.com/news/study-finds-internet-economy-grew-seven-times-faster/
[7] https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf
[8] https://americaninnovators.com/wp-content/uploads/2022/08/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf
[9] https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf
[10] 87 Fed. Reg. at 51284 (Question 60).
[11] *West Virginia*, 142 S. Ct. at 2612.
[12] *Id.* at 2613.
[13] *Id.* (quoting W. Eskridge, *Interpreting Law: A Primer on How To Read Statutes and the Constitution* 288 (2016)).
[14] 87 Fed. Reg. at 51283.

may inhibit the ability of companies to make systems fully interoperable.[15] Congress has in the past made such decisions when it enacted the Health Insurance Portability and Accountability Act and the 21st Century Cures Act, which covered only portions of the nation's healthcare sector. Congress has passed no such law on an economy-wide level.

Likewise, the history of this asserted authority shows that the FTC is attempting to regulate an area long considered to be outside the agency's authority. As the Court noted in *West Virginia v. EPA*, a history of congressional refusal to authorize particular action is evidence that Congress has not authorized that action.[16] That is true of the FTC's claim of authority in the ANPR. As early as 2000, the Federal Trade Commission issued a report, *Privacy Online: Fair Information Practices in the Electronic Marketplace* ("Online Privacy Report"), recommending that "Congress enact legislation that, in conjunction with self-regulatory programs, will ensure adequate protection of consumer privacy online."[17] Congress, despite numerous introduced bills, has yet to pass comprehensive privacy legislation in the two decades since the report. That refusal to mandate comprehensive privacy regulation is a sign that Congress has not yet decided to commit comprehensive privacy regulation to the FTC.

3. Congress Has Not Clearly Authorized a Comprehensive Data and Algorithms Rule

Congress has not clearly authorized a comprehensive data and algorithms trade rule. If an agency has asserted authority to resolve major questions, as the FTC has done in the ANPR, the "agency must point to 'clear congressional authorization' for the power it claims."[18] A "[v]ague statutory grant is not close to the sort of clear authorization required" by the Court's precedents.[19]

The ANPR cannot point to any clear authorization because none exists. Indeed, the FTC has acknowledged as much since at least its 2000 Online Privacy Report. In that report, the FTC stated that "the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web site, or portions of their Web sites, not directed to children."[20] The FTC has not offered any satisfactory explanation of what statutory authorization has occurred since 2000 to justify the Commission's change in position.

---

[15] See also Phillips Dissent at 1 (Dissenting from ANPR because the anticipated rulemaking would "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.").

[16] *West Virginia*, 142 S. Ct. at 2614.

[17] https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf

[18] *West Virginia*, 142 S. Ct. at 2614 (quoting *Utility Air*, 573 U.S. at 324).

[19] *Id.*

[20] *Supra* note 12 at 34.

In fact, the FTC admits today that congressional action is necessary to effectuate what the ANPR seeks to accomplish. Chair Khan notes in her supporting statement of the ANPR that:[21]

> If Congress passes strong federal privacy legislation—as I hope it does—or if there is any other significant change in applicable law, *then the Commission would be able to reassess* the value-add of this effort and whether continuing it is a sound use of resources. The recent steps taken by lawmakers to advance federal privacy legislation are highly encouraging, and our agency stands ready to continue aiding that process through technical assistance or otherwise sharing our staff's expertise. At minimum, the record we will build through issuing this ANPR and seeking public comment can serve as a resource to policymakers across the board as legislative efforts continue.

What is clear is that the Chair of the Commission believes Congress has not clearly instructed the FTC to regulate data privacy; therefore, Congress has not clearly spoken to give authorization for a comprehensive data rule. Congress would not embrace the circular logic of having agencies initiate rulemakings in matters of major economic and political significance to assist in the passage of legislation that would authorize an agency rulemaking.

The existing congressional authorization for limited privacy rules serves only to highlight that no broader authorization exists. Congress has clearly authorized federal agencies to make privacy rules in limited contexts including for children under 13, protected health information, and nonpublic personal information in the financial sector.[22] Congress has never explicitly granted rulemaking authority to the Commission regarding comprehensive data policy.

The Commission cannot rely, as it purports to, on its authority to make rules against "unfair or deceptive acts or practices."[23] Such a term as "unfair and deceptive acts or practices" is the sort of "vague statutory grant" that the Court in *West Virginia* found to be "not close to the sort of clear authorization required."[24] That language does not evidence clear congressional authorization to regulate a matter of national economic and political significance. FTC should be prepared to point to clear congressional authorization beyond its ability to enforce against "unfair and deceptive practices" to justify its authority to finalize a trade rule on privacy and security.

Unlike Congress, independent agencies like the FTC have no accountability to the general public, and that is why it is best left for the legislative branch to give a clear grant of authority. The Commission seeks to use its broad general authority, as opposed to clear specific

[21] 87 Fed. Reg. at 51287 (emphasis added).
[22] Children's Online Privacy Protection Act 15 U.S.C. S 6501 et seq.; Health Insurance Portability and Accountability Act; Gramm-Leach-Bliley Act.
[23] 87 Fed. Reg. at 51278.
[24] *West Virginia*, 142 S. Ct. at 2614.

grants of authority, and for this reason does not satisfy the requirements of the major questions doctrine.

B. The Proposed Rules Contemplate Replacing the Clear Intent of Congress Regarding Children and Teen's Privacy

Per the Children's Online Privacy Protection Act ("COPPA"), the FTC is charged with overseeing certain privacy protections for children *under 13*.[25] Congress carefully delineated the scope of, and the appropriate age limit for, these protections. Congress also clearly sees any extension of COPPA, including expanding age limit to cover teens, as being within its purview, as demonstrated by the introduction this Congress of the Children and Teens Online Privacy Protection Act (aka COPPA 2.0).[26] Yet, the FTC seems to think it has the unilateral authority to significantly expand COPPA under the guise of Section 5.

The ANPR asks a series of questions that directly contemplate extending COPPA to teens and providing additional privacy protections to both children and teens beyond those Congress authorized (e.g., "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 activities?"; other examples are scattered throughout this Section of the ANPR).[27] These questions suggest that the FTC is contemplating stepping outside the bounds of its clearly defined statutory authority.

III. The ANPR Violates the FTC Act.

In issuing the ANPR, the FTC erred twice in interpreting its rulemaking authority. First, to the extent the ANPR relies on the FTC's Section 18 rulemaking authority with respect to "unfair and deceptive acts and practices," the ANPR fails to comport with the FTC's statutory obligations for those rulemakings. Second, to the extent the ANPR purports to contemplate a rulemaking under Section 6(g) of the FTC Act to address "unfair methods of competition," the FTC lacks rulemaking authority at all.

A. Section 18 Rulemaking Authority

1. The Advanced Notice of Proposed Rulemaking Does Not Meet the Requirements of Section 18 of the FTC Act.

Rather than broadly expanding the Commission's authority, Congress has on several occasions taken steps to rein in the Agency by placing procedural safeguards on its rulemaking

[25] 15 U.S.C. §6501(1).
[26] https:/www.congress.gov/bill/117th-congress/senate-bill/1628/text__;!!CxwJSw!JK3nl1Oewfs9Z060G9jmoPWo0967rzbKENDbJf3WqQCYDqsrYiEqcqMCI2YE2bWVJWrGy5X4aWxqNiunMVksoQyNoA$
[27] 87 Fed. Reg 51282 (Question 14).

authority. Commissioners Noah Phillips and Christine Wilson made the following observation about the restraints placed about the FTC in the 1970s and 80s:[28]

> The Washington Post accused the agency of attempting to serve as the "national nanny." A Senate Report found that the agency's rulemaking efforts were filled with "excessive ambiguity, confusion, and uncertainty." Backlash from the agency's sweeping regulatory efforts culminated in the Federal Trade Commission Improvements Act of 1980, which imposed additional procedural obligations on Section 18 rulemaking efforts. Yet again Congress cabined the agency's discretion—a rebuke to the agency's regulatory enthusiasm that Ernest Gellhorn characterized as "The Wages of Zealotry."

In response to these concerns, Congress enacted and modified Section 18 of the FTC Act to require the Commission to provide the public meaningful notice and input. Congress authorized the FTC to promulgate certain legislative rules under Section 18 of the FTC Act, but that Act also imposed numerous additional procedural requirements that the FTC has so far failed to meet. In the ANPR, the FTC must include "a brief description of the area of inquiry under consideration, the objectives which the Commission seeks to achieve, and possible regulatory alternatives under consideration by the Commission."[29] The FTC may proceed with rulemaking only if it "make[s] a determination that unfair or deceptive acts or practices are prevalent," which requires either that the FTC "has issued cease and desist orders regarding such acts or practices" or that the FTC has information "indicat[ing] a widespread pattern of unfair or deceptive acts or practices."[30]

a. Brevity and Specificity

The ANPR on its face fails to meet the requirements of Section 18. The Act requires that an advanced notice of rulemaking "contain a *brief description* of the area of inquiry under consideration, the objectives which the Commission seeks to achieve, and possible regulatory alternatives under consideration by the Commission."[31] The Commission is later in the rulemaking process required to "define with specificity acts or practices which are unfair and deceptive acts or practices in or affecting commerce."[32]

The ANPR itself violates Section 18 because it provides the public no meaningful way to understand and provide feedback on potential rules. The ANPR states that it focuses on "commercial surveillance," but that description cannot conceivably put the public on notice of the wide range of issues at stake. Indeed, the Commission defines "commercial surveillance" to

---

[28] https://www.ftc.gov/system/files/documents/public_statements/1591702/p210100_wilsonphillips_joint_statement_-_rules_of_practice.pdf at 2-3.

[29] 15 U.S.C. § 57a(b)(2)(A).

[30] 15 U.S.C. § 57a(b)(3).

[31] 15 U.S.C. § 57a(b)(2)(A)(i) (emphasis added).

[32] 15 U.S.C. § 57a(a)(1)(B).

include "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivates of that information."[33] The term "commercial surveillance" is thus a pejorative misnomer that applies to virtually any use of data – regardless of whether such use is unfair or deceptive – that informs business decision making, advertising, customer interactions, privacy, and algorithms. The Commission asks *95* different questions that attempt to cover a range of topics so broad as to touch on every aspect of business use of data, beginning with how businesses collect consumer data and make business decisions using data and whether these practices harm consumers.[34] To make decisions about how to tailor products, services, and advertising for consumers, consumer data is necessary for basic business decisions.

If the FTC has asked broad and sweeping questions about practices, then it will not have a sufficient record to move forward on those topics in an NPRM. The Commission itself seems to recognize this failure of the ANPR, stating that the FTC is "wary of committing now, even preliminarily, to any regulatory approach without public comment given the reported scope of commercial surveillance practices."[35]

In the past, FTC trade rules focused on specific industries and practices like the funeral, ophthalmic, and home insulation labeling rules. By contrast, the current ANPR's scope includes effectively all business decisions that involve consumers. An economywide fishing expedition for which types of data practices should be regulated by the Commission runs afoul of Section 18.

b. Prevalence of Unfair or Deceptive Acts or Practices

To promulgate a trade rule declaring that an act or practice is unfair or deceptive, Section 18 requires that the Commission find that the "unfair or deceptive acts or practices are prevalent."[36] The ANPR fails to identify an unfair or deceptive trade practice at all, and the ANPR further fails to indicate that any unfair or deceptive practice is prevalent.

Unfair or Deceptive Acts or Practices. The Commission puts the proverbial cart before the horse when it asks in Question 3 of the ANPR, which "surveillance practices" are prevalent.[37] Since the FTC has never found that many of the myriad practices discussed in the ANPR are unfair or deceptive (and, in many cases, has found that data collection and uses provide significant benefits to consumers and competition), it is premature and meaningless to ask whether the practices are prevalent. The question suggests that FTC is looking for something to regulate, rather than look to solve a specific identified problem.

[33] 87 Fed. Reg. at 51277.
[34] 87 Fed. Reg. at 51282 (Question 1 and 4).
[35] *Id*. at 51281 n. 127.
[36] 15 U.S.C. S 57a(b)(3).
[37] 87 Fed. Reg. 51282 (Question 3).

It is not enough to show that an act or practice is prevalent, and that it sometimes causes harm. Rather, the specific act or practice must always be unfair or deceptive. Only when that specific act or practice has been shown to violate the FTC Act should the Commission attempt to determine if a rulemaking is warranted because it is prevalent. The practices referenced in the ANPR, such as the collection of data and tailoring of advertising, are not inherently harmful and thus are not inherently unfair or deceptive.

The Commission can determine that an act or practice is "unfair" only if it "*causes or is likely to cause substantial injury to consumers* which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits."[38] The injury could be a small harm to a large number of people or a significant risk of concrete harm but would not include emotional distress or injury.[39] The unfair practice must also affect consumers and not "the public."

Rather than identify widespread patterns of unfair and deceptive acts and practices, the FTC has asked commenters to themselves identify which data practices could be harmful. In addition to that broad call regarding which data practices could be harmful, the ANPR also identifies many legitimate business practices, including limitations on targeted advertising and widespread industry data minimization requirements.

Unfortunately, the ANPR amounts to a fishing expedition, as opposed to focusing on narrow discrete areas of harm. For example, Questions 1 and 4 ask "which practices do companies use to surveil consumers?" and "How, *if at all*, do these commercial surveillance practices harm consumers…"[40] The Commission should identify discrete and concrete harmful conduct and weigh that against countervailing benefits and the ability of consumers to avoid injury.

Prevalence. An act is considered prevalent if the Commission has either issued a cease and desist order regarding such acts or practices or if "any other information available to the Commission indicated a widespread pattern of unfair or deceptive acts or practices."[41] If the FTC has adjudicated very few cases regarding privacy and algorithms, it is unlikely to show that there is a "a widespread pattern" of any unfair or deceptive acts or practices. The Commission cannot rely on broad generalizations and anecdotes to demonstrate prevalence.

B. The FTC Does Not Have Authority to Make Rules Under Its "Unfair Methods of Competition Authority"

The ANPR cites a Petition by Accountable Tech as evidence of the need for the Proposed Rules regarding privacy, security, and algorithms.[42] The Accountable Tech Petition requested

[38] 15 U.S.C. § 45(n) (emphasis added).
[39] FTC Policy Statement on Unfairness *available at* https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness
[40] 87 Fed. Reg. 51281.
[41] 15 U.S.C. § 57a(b)(3).
[42] 87 Fed. Reg. 51287.

that the Commission make rules under its authority to enforce against unfair methods of competition.[43] The current ANPR similarly uses the misnomer that the Accountable Tech Petition uses concerning "surveillance" and in Footnote 47 asserts "[s]uch rules could arise from the Commission's authority to protect against unfair methods of competition."[44]

Any attempt to make rules concerning matters of unfair methods of competition regarding privacy, security, or algorithms would be an unlawful expansion of the authority granted to the FTC by Congress.

The FTC Act's text, structure, and history, as well as recent guidance from the Supreme Court, all point in the same direction: the FTC lacks statutory authority to act on this Proposed Rule as an unfair method of competition. Section 5 of the FTC Act prohibits "unfair methods of competition" (UMC), and Section 6(g) states that the Commission "shall have power ... [f]rom time to time to classify corporations and ... to make rules or regulations for the purpose of carrying out the [Act's] provisions." 15 U.S.C. §§ 45, 46(g). Nothing in the Act's text expressly gives the FTC rulemaking authority to prohibit competitive methods that the FTC deems unfair. Nowhere, for example, does the Act state that the FTC "shall or may" promulgate rules to determine whether certain types of competitive methods are fair or unfair, to supplant state law, or to invalidate entire categories of advertising on competitive grounds. Indeed, such a broad grant of statutory authority under Section 5 would have been extraordinary, as it would have allowed a majority of just three commissioners, independent of and with little guidance from the President or Congress, to dictate commercial practices, and override state laws, across virtually the entire U.S. economy.

The FTC Act's structure confirms that the FTC lacks UMC rulemaking authority. In sharp contrast to the text's silence on such authority, Congress expressly granted the FTC authority to promulgate other rules. For example, statutes such as the Children's Online Privacy Protection Act and Telemarketing and Consumer Fraud and Abuse Prevention Act expressly grant the FTC the authority to engage in notice and comment rulemaking to enforce their provisions.[45] Congress also provided the FTC explicit rulemaking authority for unfair and deceptive acts and practices through the Magnuson-Moss Warranty – Federal Trade Commission Improvement Act of 1975. In these statutes, Congress clearly defined the scope of its delegation to the FTC, either in terms of a proposed rule's substantive scope or its procedural path, or both. The fact that Congress failed to set forth any guidance or guardrails for UMC rulemaking authority strongly suggests that no such authority exists.

Moreover, the FTC Act fails to provide for any sanctions for violations of rules promulgated pursuant to Section 6. Again, this omission strongly suggests that Congress never intended to give the FTC substantive, binding UMC rulemaking authority at all. As the American

[43] 86 Fed. Reg. 73206.
[44] 87 Fed. Reg. 51287.
[45] *See* Jeffrey Lubbers, *It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1789, 1991-92 (Nov. 2015).

Bar Association explained, the Act's "fail[ure] to provide any sanctions for violating any rule adopted pursuant to Section 6(g) . . . strongly suggest[s] that Congress did not intend to give the agency substantive rulemaking powers when it passed the Federal Trade Commission Act."[46]

Perhaps recognizing these textual and structural shortfalls, as a matter of history, the FTC has hesitated to assert that it has UMC rulemaking authority. Until 1962, and for almost half a century since the enactment of Magnuson-Moss in 1975, the FTC never attempted to promulgate a UMC rule. The time period since 1975 spans eight Presidential administrations, from both major political parties, and FTC chairs and commissioners with widely differing philosophies and priorities. Indeed, even prior to 1975, only once had the FTC's authority to conduct rulemaking under Section 6(g) been tested in court. In *National Petroleum Refiners Association v. FTC,* 482 F.2d 672 (D.C. Cir. 1973), the FTC promulgated a rule defining the failure to post octane rating numbers on gasoline pumps at service stations as "an unfair method of competition and an unfair or deceptive act or practice." The D.C. Circuit found that Section 6(g) conferred such authority, which led Congress to enact Magnuson-Moss. Critically, Magnuson-Moss expressly confers rulemaking authority for unfair and deceptive acts and practices, but not unfair methods of competition. Since that time, the FTC has never claimed UMC rulemaking authority. That silence speaks volumes.

Recent court decisions confirm that the FTC cannot assert broad authority without an express grant from Congress. In *AMG Capital Management v. FTC*, 141 S. Ct. 1341 (2021), the Supreme Court unanimously rejected the FTC's claim that it could assert broad remedial powers without an express grant of authority from Congress. In its decision, the Court stressed that the Commission must operate within the express confines of the statutory language: "to read those words [in Section 13(b)] as allowing what they do not say, namely, as allowing the Commission to dispense with administrative proceedings to obtain monetary relief as well, is to read the words as going well beyond the provision's subject matter." For decades now, the Supreme Court has made clear that an agency's authority extends only so far as the relevant statute's express language. As the Court has explained, "Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes." *Whitman v. Am. Trucking Associations*, 531 U.S. 457, 468 (2001). Applying these principles, Section 6(g) is best understood as granting the FTC ministerial, not legislative authority, to specify how it will carry out its adjudicative, investigative, and informative functions.

IV. The ANPR Would Harm Businesses and Innovation.

A. A Burdensome Privacy Patchwork

[46] ABA, *Comments of the Antitrust Law Section of the American Bar Association in Connection with the Federal Trade Commission Workshop on "Non-Competes in the Workplace: Examining Antitrust and Consumer Protection Issues"* at 54.

A comprehensive privacy, security, and algorithmic rule would exacerbate an already complex patchwork of state privacy laws. Five states—California, Virginia, Colorado, Connecticut, and Utah—have all passed comprehensive laws that all have substantial differences in requirements. Because the FTC's authorities under Section 5 likely would not be preemptive, a new national rule would add a new layer of regulation that would further confuse consumers and make compliance even more difficult for companies, particularly small businesses. Eighty percent of small business owners credit the use of technology platforms that employ data as enabling them to compete with larger firms.[47] These platforms have enabled small businesses to grow their number of employees, sales, and revenue through more targeted advertising, payment systems, and workflow management. Eighty percent of small businesses also agree that limiting their access to data would harm their business operations. [48]

Adding a new national layer of regulation to a state patchwork would disproportionately impact small businesses, as they would not have the same resources for compliance as larger firms. According to a report by ITI, a 50-state patchwork of laws could cost the economy one trillion dollars over ten years, with small businesses alone taking a $200 billion hit.[49] Even if the Commission were to apply a different set of rules to larger companies, small businesses report that they would no longer be able to access the tools they need to reduce costs to compete with larger competitors.[50] The Commission must consider the cost of additional complexity and confusion as it assesses whether to move forward with proposed regulations.

B. The Commission Must Follow Section 5 of the FTC Act by Considering the Benefits of the Data-Driven Economy.

In determining whether a practice or act is unlawfully unfair, the Commission must show that the "act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers and *not outweighed by countervailing benefits to consumers of to competition*."[51] The data-driven economy has enabled greater affordability and availability of products and services across the entire economy. If regulations restrict or eliminate the use of data, many of those online services will move behind a pay wall which will have a disparate impact on lower socioeconomic levels and smaller businesses.

1. Marketing and Advertising

---

[47] https://americaninnovators.com/wp-content/uploads/2022/08/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf.
[48] *Id*.
[49] https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/
[50] https://www.uschamber.com/technology/small-business-owners-credit-technology-platforms-as-a-lifeline-for-their-business
[51] 15 U.S.C. S 45(n) (emphasis added). https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf

The ANPR asks several times about whether the Commission should regulate personalized advertising or even ban certain companies from engaging in the practice.[52] Not only do these questions unfairly presuppose that targeted advertising harms consumers, the ANPR fails to acknowledge the benefits that personalized advertising provides. As noted *supra*, small businesses benefit from the use of personalized advertising because they can optimize their resources by personalizing advertising to likely customers.

The Commission itself has recognized that personalized online advertising benefits consumers by "funding online content and services" available to consumers,[53] providing "personalized advertisements that many consumers value," and reducing unwanted advertising.[54] In fact, 77 percent of Americans prefer online advertisements that are tailored to their interests and more Americans oppose banning this type of practice than do not.[55]

---

[52] 87 Fed. Reg. 51283

[53] https://www.ftc.gov/system/files/documents/reports/brief-primer-economics-targeted-advertising/economic_issues_paper_-_economics_of_targeted_advertising.pdf; Prepared Statement of the FTC on Do Not Track Before the House of Representatives Committee on Energy and Commerce (Dec. 2, 2010) at 12, 17, https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-do-not-track/101202donottrack.pdf. *See also* Where's the Remote? Maintaining Consumer Control in the Age of Behavioral Advertising, Remarks of FTC Chairman Jon Leibowitz at the National Cable & Telecommunications Association (May 12, 2010) at 1-2, https://www.ftc.gov/sites/default/files/documents/public_statements/wheres-remote-maintaining-consumer-control-age-behavioral-advertising/100512nctaspeech.pdf (Targeted ads are "good for the Internet, where online advertising helps support the free content everyone enjoys and expects."); Prepared Statement of the FTC on Emerging Threats in the Online Advertising Industry Before the Senate Committee on Homeland Security and Governmental Affairs (May 15, 2014) at 1,

[54] *See, e.g.*, Where's the Remote? Maintaining Consumer Control in the Age of Behavioral Advertising, Remarks of FTC Chairman Jon Leibowitz at the National Cable & Telecommunications Association (May 12, 2010) at 1-2, https://www.ftc.gov/sites/default/files/documents/public_statements/wheres-remote-maintaining-consumer-control-age-behavioral-advertising/100512nctaspeech.pdf (Targeted ads "are usually good for consumers, who don't have to waste their time slogging through pitches for products they would never buy."); Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009) at 9-10, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf ("Online behavioral advertising may provide valuable benefits to consumers in the form of…personalization that many consumers appear to value, and a potential reduction in unwanted advertising."); Prepared Statement of the FTC on Behavioral Advertising Before the Senate Committee on Commerce, Science, and Transportation (Jul. 9, 2008) at 3-4, https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-behavioral-advertising/p085400behavioralad.pdf ("[B]y providing advertisements that are likely to be of interest to the consumer, behavioral advertising also may reduce the number of unwanted, and potentially unwelcome, advertisements consumers receive online." (citing Larry Ponemon, "FTC Presentation on Cookies and Consumer Permissions," presented at the FTC's Town Hall "Behavioral Advertising: Tracking, Targeting, and Technology" (Nov. 1, 2007))). Dr. Ponemon found that "about 55 percent of [survey] respondents believe that an online ad that targets their individual preference or interest improves or greatly improves their experience." https://www.ftc.gov/sites/default/files/documents/public_events/ehavioral-advertising-tracking-targeting-and-technology/71101wor.pdf at 143.

[55] https://americaninnovators.com/wp-content/uploads/2022/07/CTEC-Impact-of-Tech-on-US-Small-Business-American-Public-Views-7.28.pdf

It is violative of Section 5 for the Commission to presuppose that personalized advertising is *per se* harmful to consumers.

2. Operational Uses of Data

The ANPR asks whether trade rules should impose data minimization or purpose limitation requirements.[56] Such a requirement would effectively require the Commission to second guess the gathering of data necessary for fundamental business operations as well as research and other publicly beneficial uses. Furthermore, such a general requirement is also unwarranted because there are significant benefits to consumers and competition from the secondary use of data. Given the tradeoffs required and the significant economic impact of such a rule, it is only appropriate for the legislative branch to make such a determination.

FTC is not in the position to make judgments about these tradeoffs, given its limited authority. State legislation which has undergone debate has led to exceptions that reflect the need for societally beneficial uses of data. For example, data that may not necessarily be needed for a direct transaction may be useful in assisting a company to detect fraudulent activity and protect a consumer. Such secondary data has also been used to stop criminals engaged in violent activities, enable artificial intelligence systems to operate more accurately, and determine environmental factors that could impact an individual's healthcare outcome and tailor care.[57] Data was also used with supercomputing resources to determine effectiveness and track the spread of COVID-19.[58]

There are also considerable tradeoffs required when it comes to regulating the use of data. For example, sensitive data related to race or gender of an individual may be necessary to determine whether private or public sector services are being provided equitably. The Commission could also inadvertently bar collection or use of data that may make compliance impossible if the agency also imposes interoperability requirements. Additionally, if the FTC were to impose rules regarding publicly available information, the Commission may violate First Amendment protected activity. For this reason, the Commission should wait on Congress to debate and make the necessary tradeoffs for an issue of great economic significance and public welfare.

V. Congress Should Pass Protective, Preemptive Data-Security/Cybersecurity Legislation: Policymakers Need to Safeguard Industry Defenders

A. The ANPR's Casual Use of the Phrase 'Lax Security' Is Dismissive of Businesses That Invest in Strong Cybersecurity

[56] 87 Fed. Reg. 51283
[57] https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf.
[58] https://americaninnovators.com/wp-content/uploads/2020/10/CTEC_TechUpgrade_Data_.pdf

In its ANPR, the FTC majority significantly misses the mark in contemplating forward-looking data-security/cybersecurity (referred to jointly as cybersecurity) policy. Not only does the FTC lack and legislative mandate to regulate on the basis of cyber security, but the ANPR runs counter to some emerging trends in cybersecurity policymaking, including deepening public-private collaboration, harmonizing regulations, and safeguarding industry defenders.

The ANPR's casual and repetitive use of the phrase "lax security" is unwarranted. For several years, federal, state, and local governments and the business community have embraced a partnership model to defend U.S. critical infrastructure—the majority of which is owned and operated by the private sector—from nation-state and criminal cyberattacks. This approach has been generally successful. Many focus on the unfortunate cyber incidents that occur, while too few focus on the countless cyberattacks that have been avoided.[59]

The ANPR is also dismissive of businesses that invest heavily in their cybersecurity programs. Absent from most cybersecurity policy discussions is the fact that private entities with mature cybersecurity programs receive comparatively limited government support or actionable information to contest foreign malicious cyber activity. Notable exceptions include law enforcement and the Cybersecurity and Infrastructure Security Agency (CISA).

The ANPR does not consider substantive ways in which a business could work with the federal government so that national security agencies can disrupt the campaigns of threat actors on a more persistent basis. Many in industry are eager to pursue collaborative relationships between industry and national security agencies to degrade or disrupt malicious cyber activity against the U.S.—not more government mandates especially from agencies that are not charged with a cyber security mandate.

B. The Current Regulatory Model Is Unjust and Unsustainable

The ANPR asks whether the FTC should write new rules to "require or help incentivize reasonable data security."[60] The Chamber believes that the ANPR would largely exacerbate the status quo, such as the Safeguards Rule. In commenting on the Safeguards Rule in in August 2019 and February 2022, the Chamber stressed its longstanding interest in fostering a dynamic approach to cybersecurity governance. We urged the FTC and other policymaking bodies to partner with businesses to streamline the growing collection of state, federal, and international cybersecurity regulations.

In 2019, the Chamber said that the Safeguards Rule should not be expanded to include additional requirements governing covered financial institutions' information security programs. (The FTC based its decision to amend the Safeguards Rule to include more specific

[59] See the Chamber's September 16, 2022, letter to the Senate on legislation related to systemically important enterprises.
https://www.uschamber.com/security/cybersecurity/coalition-letter-on-cyber-amendment-to-h-r-7900-the-fy23-national-defense-authorization-act

[60] 87 Fed. Reg. 51284 (see questions 31–36).

security requirements on a comparatively limited subset of comments received in 2016.) The Chamber stressed that it would be opposed to an updated Safeguards Rule that does not grant strong legal liability and regulatory protections to covered entities.[61]

It is frequently overlooked that industry is the main force shouldering the protection and resilience of U.S. information systems against cyberattacks initiated by predatory nation-state hackers and other illicit groups. The current regulatory model is both unjust and unsustainable, as the following 4 themes—fairness, correctness, mismatch, and fragmentation—argue. It is past time for capable businesses to get legal credit when they meet certain security standards, including regarding enterprise risk management and internet-of-things (IoT) devices.[62]

1. **Fairness.** Businesses contend with relentless, state-sponsored cyberattacks but **lack effective government protection.** Justice—or a basic sense of fairness—recommends legal liability protections for businesses.

2. **Correctness.** In the context of the ANPR, new FTC rules would amount to a regulatory free lunch. If the FTC believes that new cybersecurity rules would deliver the security benefits that the ANPR suggests, then the agency should confidently call on Congress to pair existing/any new rules with legal liability protections. Policymakers should stand behind the perceived correctness of their rules. Anything short of clear legal liability protections for covered entities would call into question the assumption that the cybersecurity requirements are appropriately risk-based and technically sound.

3. **Mismatch.** There is an overwhelming numeric mismatch between agencies that are tasked with regulating the business community and agencies that are empowered to disrupt the campaigns of threat actors on a more persistent basis. For example, consider the role of law enforcement. The FBI and the Secret Service are just 2 federal entities—in comparison with the Cybersecurity Forum for Independent and Executive Branch Regulators (the Cyber Forum), which is comprised of 17 departments and agencies—that push back on malicious actors.[63]

---

[61] See the Chamber's August 2, 2019, comment letter to the FTC. https://www.regulations.gov/comment/FTC-2019-0019-0033

[62] See the Chamber's October 18, 2021, comment letter to the Federal Communications Commission (FCC) on the agency's notice of inquiry regarding ways to strengthen IoT cybersecurity. https://www.fcc.gov/ecfs/file/download/211018_Comments_IoT%20Cybersecurity%20SecureEquipment_FCC.pdf?folder=10182049018274

[63] The federal Cyber Forum includes the following agencies: the Coast Guard, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, CISA, the Department of Health and Human Services, the Department of Homeland Security, the Department of Treasury, FCC, the Federal Energy Regulatory Commission, the Federal Housing Finance Agency, the Federal Reserve Bank, FTC, the Food and Drug Administration, the National Institute of Standards and Technology, the Nuclear Regulatory Commission, the Office of the Comptroller of the Currency, and the Securities Exchange Commission.

There is a clear surplus of agency regulators vis-à-vis agency defenders. This mismatch has profound implications for U.S. security. Regulatory agencies are free to pass judgment on businesses that are cybercrime victims; yet these businesses are often unsupported against international criminal gangs and purveyors of ransomware.

4. **Fragmentation.** The ANPR appears to reject the growing consensus that agencies need to work together, in collaboration with industry, to achieve greater consistency in cybersecurity requirements. Today, there is considerable fragmentation across agency jurisdictions and sectors. If the FTC were to implement new cybersecurity rules, it would add to the regulatory morass and buck the emerging trend toward regulatory harmonization.[64] What is more, fragmented approaches to cybersecurity lead to duplicative and/or confusing security requirements, splinter organizations' risk management budgets.

C. Safeguard Industry Defenders

The Chamber believes that Congress must pass a federal, preemptive law that would authorize legal liability and regulatory protections for private entities that conform with industry-recognized programs, agency regulations, as well as new laws and requirements. Such a law would have the virtues of giving policymakers, the business community, and consumers more of what they need—enhanced security and resilience. At the same time, businesses need policymakers to better balance federal regulation with legal liability and related protections, consider the growing private sector costs of defending against nation states, and harmonize and promote U.S. policies at home and internationally.

This balanced legislation can be summarized in three words: program, protection, and preemption.

1. **Program.** If the FTC is interested in incentivizing reasonable cybersecurity, it should push Congress to write cybersecurity legislation that recognizes businesses' use of existing standards, guidelines, and frameworks to meet a law's and/or a regulation's requirements.

   In exchange, businesses would qualify for congressionally crafted protections and other inducements to invest in and meet heightened cybersecurity requirements.

---

https://www.meritalk.com/articles/fcc-chair-rosenworcel-to-lead-relaunched-interagency-cyber-forum
https://www.fcc.gov/document/chair-rosenworcel-remarks-cybersecurity-forum-principals-meeting

[64] The national cyber director's (NCD's) October 2021 strategic statement places much emphasis on cybersecurity cooperation and coordination across the many public, private, and international stakeholders in the ecosystem. The White House, Office of the National Cyber Director, *A Strategic Intent Statement for the Office of the National Cyber Director*, October 2021, p. 7.
https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf

Where applicable, legislation should offer private parties a menu of appropriate standards, guidelines, and/or frameworks to select from, facilitating choice and the buy-in of parties that may be subject to various regulatory requirements or expectations.

Programs should also establish reciprocity requirements in order to harmonize laws, regulations, and other obligations. Congressionally created programs should be flexible—such as scalable to a business' size and budget, and risk-based—thus targeting industry's resources at legitimate threats and harms.

2. **Protection.** Cyberspace remains the only domain where private companies are expected to defend themselves against nation states and/or their proxies. The Chamber believes that this security gap justifies blending cybersecurity requirements—existing or new—with regulatory and legal protections. These safeguards would benefit organizations that take constructive steps to elevate cybersecurity. Depending on the nature of a cybersecurity program, legal liability protections should range from an affirmative defense (sometimes referred to as a safe harbor) against lawsuits to more comprehensive protections (e.g., private entities that are certified by third parties and/or regulated by government agencies should be immunized from lawsuits) against litigation generated by a cyberattack.

   Policymaking usually involves making tradeoffs. Yet the ANPR would enable the FTC to pass judgment on businesses' cybersecurity practices while doing almost nothing to mitigate their costs in defending against foreign powers and their proxies.

3. **Preemption.** As new cybersecurity laws continue to be enacted domestically and internationally, businesses are forced to navigate a crowded patchwork of obligations. Adopting risk-based legislation while establishing clear and consistent federal guidelines would ensure that both regulators and regulated entities can direct scarce resources at significant cybersecurity risks. Congress should expressly preempt state cybersecurity laws to provide national uniformity and align duplicative and often conflicting compliance burdens. Greater business certainty would drive investments in better cybersecurity risk management and adherence to laws and requirements.

A serious shortcoming of the ANPR and the federal privacy legislation is that neither one correctly protects capable businesses nor truly preempts state laws. To borrow from FTC Commissioner Noah Phillips, if policymakers are going to keep cybersecurity in a rulemaking or legislation, then they should "do it right."[65]

[65] 87 Fed. Reg. 51294.

VI. Conclusion

Data is fundamental to the 21st century whether it be allowing small businesses to compete during a time of COVID-19 lockdowns and inflation, enabling companies to design equity into their products, or more quickly get vaccines safely to market. Although the business community recognizes that data can be misused by nefarious actors or cause individual harm to consumers, practices like data analytics, targeted advertising, and algorithmic decision-marking are not *per se* harmful to consumers.

Given the complexities involved and the scope of the FTC's ANPR, the Commission should halt its rulemaking and wait for Congress to speak clearly to a matter of vast economic and political significance and allow the legislative branch to debate the necessary policy tradeoffs that must be decided in a truly preemptive national privacy law. Otherwise, the rulemaking will lead to confusion for businesses by exacerbating a growing and burdensome patchwork of privacy, security, and algorithmic laws. Such a rulemaking would have a disproportionate impact on small business and hinder societally beneficial uses of data.

At a time when the nation is experiencing rampant inflation, supply chain issues, and competition with nations not sharing our democratic values, the Commission should respect due process and separation of powers and work to limit the burdens on responsible data-driven innovation.

The Chamber looks forward to your response. Please contact jcrenshaw@uschamber.com if you have any questions.

Sincerely,

Jordan Crenshaw
Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce