

November 21, 2022

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

Re: Commercial Surveillance ANPR, R111004

Dear Ms. Tabor:

This letter is submitted on behalf of Business Roundtable, an organization of chief executive officers of America's leading companies. Business Roundtable member companies operate across all sectors of the domestic and global economy, directly employ 20 million people, and reach virtually every American consumer. Our companies—from technology, communications, retail, financial services, health, public safety and security, manufacturing, hospitality, insurance and others—rely on data and data-driven processes and solutions every day to deliver, improve, and market innovative products and services across the United States and around the world. Consumer trust and confidence are essential elements of our businesses and our relationship with our customers. We appreciate the opportunity to comment on the Advanced Notice of Proposed Rulemaking ("ANPR") issued by the Federal Trade Commission (the "Commission" or "FTC") on August 11, 2022,¹ regarding a possible rulemaking pursuant to the Commission's authority under Section 18 of the FTC Act² related to data acquisition, sharing, and security, broadly defined in the ANPR as "commercial surveillance."

Introduction

Business Roundtable member companies take data privacy and security very seriously. Our companies also understand that many American consumers may not feel in control of their personal data and how it is collected, used, shared, and protected. With this in mind, and consistent with consumer expectations, responsible business practices, and existing law, our member companies already undertake significant efforts to limit the collection, use, and sharing of consumer data, and to protect the security of such data. For example, our member companies maintain robust data privacy and security compliance programs, implement internal

¹ FTC, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022).

² 15 U.S.C. § 57a.

and external privacy policies, provide consumers with meaningful notice and opportunities for consent, and train employees to emphasize the importance of keeping our customers' data confidential and secure. In addition, Business Roundtable member companies are at the forefront of responsible innovation, developing and implementing best practices regarding how new technologies such as artificial intelligence (AI) should be utilized by businesses.³

To be clear, Business Roundtable strongly supports a national framework for data privacy and security and has been active in advocacy surrounding this issue.⁴ A national consumer privacy law enacted by Congress would harmonize requirements to address specific harms and threats.

However, we are concerned that the ANPR is predicated on several sweeping and mistaken conclusions about industry practices that serve as the rationale for establishing restrictions on the collection, use, and sharing of consumer data. These restrictions, as currently conceived, would deprive consumers of the substantial benefits afforded by current data collection and processing.

For the following reasons, Business Roundtable urges the Commission to either refrain from this rulemaking entirely or significantly limit the rulemaking to cover only those deceptive practices that Section 5 of the FTC Act currently prohibits. Any rulemaking that attempts to go beyond the Commission's Section 5 authority before Congress adopts a comprehensive federal privacy law will not withstand judicial scrutiny. Without the clarity that only federal legislation can provide, an FTC rule in this area – *even one that the courts ultimately strike down* – will sow confusion and cause businesses to shy away from data-driven solutions that benefit consumers.

- I. **Increased Fragmentation:** U.S. companies already face a patchwork of privacy requirements that differ, and often conflict, across states, industries and agency jurisdictions. A Commission rulemaking in the absence of greater statutory clarity will further confuse and complicate this fragmented legal regime.
- II. **Preferability of Legislation:** As each member of the Commission has acknowledged, it would be far preferable for a comprehensive national privacy framework to come from Congress. This would not only provide a single, nationwide standard, but also would avoid simply layering a Commission rulemaking on top of the increasing number of state privacy laws and pre-existing sector-specific federal requirements. It would be in the interest of American consumers to enjoy a consistent set of rights throughout the United States.

³ Business Roundtable, Roadmap for Responsible AI (Jan. 26, 2022), <https://www.businessroundtable.org/policy-perspectives/technology/ai>.

⁴ Business Roundtable, Framework for National Privacy Legislation (Dec. 6, 2018), <https://www.businessroundtable.org/policy-perspectives/technology/privacy>.

- III. **Section 18 Compliance:** It is not clear whether the agency's broad rulemaking effort can comply with Section 18's substantive requirements that the Commission identify specific practices that satisfy the definition of "unfairness," and establish its reason to believe those practices are "prevalent." To date, the Commission's enforcement work has largely involved deceptive practices, which are distinct and generally would not support the much more expansive requirements related to, for example, data minimization or obviating the importance of consumer consent.
- IV. **Reduced Consumer Benefits:** Any process toward eventual restrictions on "commercial surveillance" risks unintended consequences that could bar products and services that consumers value. For example:
- Financial services firms and their customers rely on superior data-enabled fraud detection tools that help prevent millions of unauthorized transactions every year. The accuracy of fraud tools is data-driven, which is why such tools have been granted exemptions under the Gramm-Leach-Bliley Act ("GLBA").
 - Health care innovations that improve patient outcomes are enabled through data collection and exchange consistent with prevailing restrictions under the Health Information Portability and Accountability Act ("HIPAA").
 - Energy companies collect and analyze data to assist consumers and enterprises in optimizing energy efficiency and reducing carbon footprints.
 - Retail firms use customer data to manage customer loyalty and rewards programs, and to ensure that inventories track changing customer demand.

For decades, the FTC's greatest strength has been its consistency, rigor, and evidence-based approach—challenging unlawful conduct, and then letting the market sift out what consumers want from the products and services they consume. Many of the practices that this proposed rulemaking would seek to address are best left to consumers to decide what they want. If lawmakers disagree with those decisions, it is Congress that should reconcile the difficult societal compromises implicated by privacy requirements and decide whether to provide greater clarity to the Commission's privacy-related authority.

I. **The FTC's Rulemaking Would Exacerbate the Existing Fragmentation of Requirements Governing Consumer Privacy and Security Across Jurisdictions and Sectors**

Separate from any particular standard, the rulemaking previewed in the ANPR would simply add yet another, inconsistent, set of requirements with which U.S. companies and consumers would be required to grapple.

The United States is home to a growing patchwork of privacy laws, which are increasingly difficult for companies to navigate. Unlike in Europe with its General Data Protection Regulation (“GDPR”), the United States does not enjoy a comprehensive federal privacy regime. The U.S. privacy legal regime is instead comprised of a handful (though growing number) of state-level privacy regimes—currently enacted in California, Virginia, Colorado, Utah, and Connecticut—a variety of topic and sector-specific federal statutes (*e.g.*, HIPAA, the Fair Credit Reporting Act, the Children’s Online Privacy Protection Act, GLBA), and case-by-case enforcement of federal- and state-law prohibitions on unfair or deceptive acts and practices. The price tag for compliance is significant, with the most recent International Association of Privacy Professionals (“IAPP”) governance report estimating that the average spend on privacy compliance was nearly \$900,000, and that 90% of companies expected to expand or maintain their privacy budgets over the next 12 months.⁵ Indeed, the California Department of Finance estimated that compliance alone for the first iteration of California’s privacy regime (the California Consumer Privacy Act) would cost \$55 billion.⁶

The “commercial surveillance” rulemaking will only exacerbate these burdens by imposing another set of requirements on companies. Because the FTC Act itself does not preempt state privacy or consumer-protection laws, an FTC rule here in the absence of new legislation would likely not be able to do so, certainly not to the same extent as federal legislation. As a result, the FTC’s new requirements would exist alongside—and perhaps in tension with—the myriad other privacy requirements in place. Consumers will be forced to navigate increasingly complex privacy notices and likely will be confused about the applicability of the Commission’s rules as compared to state laws.

A “commercial surveillance” rule also could affect companies complying with existing federal laws related to privacy or security. For example, companies in the health and medical fields have well-established practices and procedures governed by statutes such as HIPAA and adding new or different requirements atop HIPAA will only burden the numerous entities and doctor’s offices that comply with this law and the rules promulgated thereunder every day.

As another example, the ANPR’s decision to include “workers” into the definition of “consumers”⁷ will complicate compliance for any business with employees or that hires independent contractors. Indeed, earlier this month, the Department of Labor indicated its interest in expanding its review of so-called “Surveillance Reports” required by the Labor-

⁵ IAPP & EY, IAPP-EY Annual Privacy Governance Report 2021 at v, https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf.

⁶ Lauren Feiner, CNBC, California’s new privacy law could cost companies a total of \$55 billion to get in compliance (Oct. 5, 2019), <https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html>.

⁷ 87 Fed. Reg. at 51,277.

Management Reporting and Disclosure Act,⁸ as part of President Biden’s announced Blueprint for an Artificial Intelligence “Bill of Rights.”⁹ The practical impact of including “workers” into this rulemaking raises substantial questions regarding whether the agency has the authority to redefine “consumers” so expansively.

Finally, by including broad data security requirements within “commercial surveillance,” the ANPR risks injecting itself into a space in which other government bodies have been providing companies with best practices for years, and where certain sectors are subject to specific requirements. For example, many companies look to the cybersecurity, privacy and artificial intelligence risk management frameworks published by the National Institute of Standard and Technology (“NIST”)¹⁰ and the various recommendations made by the Department of Homeland Security’s cybersecurity arm, the Cybersecurity & Infrastructure Security Agency (“CISA”). Data security requirements that deviate from recommendations made by NIST and CISA will not only complicate compliance but may also reduce the effectiveness of corporate data security programs.

II. Comprehensive Federal Privacy Legislation Would Be Far Preferable to an FTC Rulemaking for Improving Consumer Trust and Regulatory Harmonization

Business Roundtable is a strong proponent of a federal privacy law. A national consumer privacy law would strengthen protections for consumers across the country, recognizing that consumers’ digital lives and experiences are not restricted by state boundaries, while offering Congress the opportunity to harmonize new requirements with the other federal obligations under which companies operate. In today’s economy, it is imperative for companies to utilize consumer data to deliver products and services, run day-to-day operations, and personalize offerings to fit customers’ needs. Only federal legislation setting a single, nationwide framework for data privacy and security can provide the benefits to consumers and certainty to businesses necessary for both to thrive. A comprehensive national privacy law that preempts state laws could benefit consumers and businesses alike by halting the growing trend of fragmentation.

In this context, rulemaking here is premature and will divert resources away from perhaps the agency’s most important function – stopping fraudsters and allowing legitimate businesses to compete – and also distract industry efforts from achieving and improving a national privacy law. At worst, a completed rule, followed by comprehensive federal legislation, with likely

⁸ Jeffrey Freund, Dep’t of Labor, How We’re Ramping Up Our Enforcement of Surveillance Reporting (Sept. 15, 2022), <https://blog.dol.gov/2022/09/15/how-were-ramping-up-our-enforcement-of-surveillance-reporting>.

⁹ White House, Fact Sheet: Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public (Oct. 4, 2022), <https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/>.

¹⁰ NIST, Cybersecurity Framework, <https://www.nist.gov/cyberframework>.

Administrative Procedures Act rulemaking authority being granted to the FTC,¹¹ could require yet another lengthy rulemaking process to repeal the rule that Congress had obviated. Efforts by businesses to stay ahead of compliance during such a lengthy rulemaking process would create a chilling effect on a broad swath of consumer-friendly data applications and innovations, all for a rule that may not withstand judicial scrutiny. It is thus not surprising that Chair Khan and every Commissioner expressed their individual preference for federal legislation over rulemaking.¹²

In weighing the benefits of FTC rulemaking versus Congressional legislation, the Commission risks exceeding its statutory authority by recasting itself as a legislature. Nothing in the FTC Act explicitly provides the Commission with the statutory authority to police specific privacy or security practices. To be sure, the FTC has constructed its privacy and enforcement program largely by relying on theories of consumer deception—that companies promised to do one thing with data but then did another. But rules related to data minimization or purpose limitation, or that restrict the use of automated decision-making, are far outside that ambit. Given the immense economic significance of data collection and usage in our modern economy, and the extremely vague grant of authority to police “unfair and deceptive acts and practices,” the FTC’s rulemaking as previewed in the ANPR also would appear to present a strong case for vacatur under the “major questions” doctrine recently articulated by the U.S. Supreme Court in *West Virginia v. EPA*.¹³

Business Roundtable understands that crafting sound data privacy requirements is a difficult endeavour, weighing many competing interests against each other and calibrating such requirements to affect the appropriate balance. But only Congress can create one nationwide framework. Our recommendation is that the FTC should thus encourage Congress to continue to work towards forging lasting compromises and legally sustainable requirements in this area.

III. **The ANPR Fails to Explain How Its Rule Would Comply with Substantive Requirements for Rulemaking Under Section 18**

Section 18 requires that the Commission identify—“with specificity”—“unfair or deceptive” acts or practices that would be the subject of a new rule.¹⁴ With respect to unfair acts or practices, the Commission has to further demonstrate that such acts or practices cause or are likely to cause substantial injury that is not reasonably avoidable by consumers, as well as not outweighed by countervailing benefits to consumers or competition.¹⁵ Further, the

¹¹ See 5 U.S.C. § 553 for general rulemaking requirements under the APA.

¹² See 87 Fed. Reg. at 51,287 (Statement of Chair Lina M. Khan); *id.* at 51,288, 51,290 (Statement of Comm. Rebecca Kelly Slaughter); *id.* at 51,293 (Statement of Commissioner Alvaro M. Bedoya); *id.* at 51,293-94 (Dissenting Statement of Comm. Noah Joshua Phillips); *id.* at 51,298 (Dissenting Statement of Comm. Christine S. Wilson).

¹³ 142 S. Ct. 2587 (2022).

¹⁴ 15 U.S.C. § 57a(a)(1)(B).

¹⁵ 15 U.S.C. § 45(n).

Commission must show that those specific acts or practices are prevalent in the economy.¹⁶ Although the FTC is not required to make this showing until release of a proposed rule, the ANPR's minimal analysis thus far, the vagueness of the individual questions, as well as the realities of the current marketplace, all cast doubt that the Commission can make these demanding showings and withstand judicial scrutiny.

Of the 95 questions raised in the ANPR, very few are focused on deceptive practices. Accordingly, the FTC instead must show how each specific practice satisfies the three-part test for unfairness, which the FTC likely cannot do. First, the practice must cause or be likely to cause substantial consumer injury. Yet the ANPR, in discussing the reasons for engaging in the rulemaking, admits that the harms at issue often "do not lend themselves to broadly accepted ways of quantifying harm" or are "opaque or hard to discern in the near term."¹⁷ If the FTC is so uncertain about whether it can measure the harms the agency seeks to prevent, it is unclear how the FTC can assert that any injury it has identified is "substantial." Second, that injury must not be reasonably avoidable. Because consumers must frequently expressly consent to companies' data collection and use, even if substantial injury was possible, consumers can avoid any such injury by exercising their right to not consent. Third, the injury must not be outweighed by the benefits to consumers or to competition. As we demonstrate in the section below, companies provide numerous benefits to consumers, such as fraud detection and anti-money-laundering measures, that would be impossible absent many of the data collection and use practices broadly and unjustly defined as "commercial surveillance" in the ANPR.

Even if a specific practice satisfies the rigorous test for unfairness, Section 18 also requires that the Commission have reason to believe that the practice is "prevalent." For the practices to be "prevalent," the FTC must have previously issued cease and desist orders regarding such practices or found that other information indicates a "widespread pattern" of unfair practices.¹⁸ Indeed, the Commission's pending rulemaking on imposter scams is a perfect case-in-point of a prevalent practice: a very specific, obviously unlawful practice that commenters and consumer complaints reveal is widespread.¹⁹ In contrast, the practices at issue in the ANPR vary considerably, with very few of them the subject of prior enforcement actions, and for many others there is not enough information to demonstrate that the practices are widespread throughout the industry. It is not enough for the agency to desire additional remedies in its one-off enforcement actions, which the ANPR candidly admits is driving this rulemaking.²⁰

¹⁶ 15 U.S.C. § 57a(b)(3).

¹⁷ 87 Fed. Reg. at 51,280-81.

¹⁸ 15 U.S.C. § 57a(b)(3)(A),(B).

¹⁹ FTC, Trade Regulation Rule on Impersonation of Government and Businesses (to be published in Federal Register), https://www.ftc.gov/system/files/ftc_gov/pdf/R207000%20Impersonation%20NPRM.pdf.

²⁰ 87 Fed. Reg. at 51,280.

IV. Overly Broad Restrictions on “Commercial Surveillance” Will Prohibit Many Practices that Benefit Consumers and are Essential to Business Operations in the Modern Economy

As part of the ANPR, the Commission appropriately sought comment on whether rulemaking in this area might negatively affect consumers or competition. Respectfully, it unavoidably will. “Commercial surveillance,” as defined by the Commission, is not limited to some narrow category of nefarious acts. Rather, under the Commission’s definition, it encompasses all conceivable ways in which businesses collect, share, analyze or otherwise use consumer data in commercial settings.

There are many examples of legitimate business activities that leverage consumer data to offer products and services that benefit customers and society more broadly. For example, responsible collection and use of consumer data enables companies to innovate and improve the efficacy and efficiency of existing products and services. Additionally, companies are able to tailor offerings to customers’ unique needs and preferences, improve customer service, and strengthen the security of consumer services. Some of these beneficial data uses are integral to business operations and to the consumer experience.

Specific examples collected from Business Roundtable member companies regarding these practices clarify some of the harm that could come if a prohibition on broadly defined “commercial surveillance” were incorporated into FTC rules:²¹

Health care. Analysis of personal data and other information is essential to making advances in medicine and medical services for patients. Personal data can propel prevention and diagnoses of health conditions and accelerate development of medical technologies, allowing rapid advances in general medical knowledge and saving patient lives. Companies pursue these significant benefits while protecting the privacy of individuals through use of certain technologies and processes, such as deidentification, pseudonymization and anonymization, transparency, and preference management—some of which are required by existing health privacy laws. Grouping health data (including data linked to a device) and data used for purposes of medical research, innovation, and patient support with other types of non-health related commercial data for the purpose of regulation would adversely impact innovation and research.

Financial Services. Credit and payment systems rely on deidentified and securely stored consumer data to provide an array of core services to customers. Critical security functions like

²¹ Business Roundtable also has produced numerous reports that highlight beneficial uses of consumer data and other issues potentially jeopardized by the FTCs rulemaking here. See, e.g., Business Roundtable, *Business Roundtable Roadmap for Responsible Artificial Intelligence* (Jan. 2022), https://s3.amazonaws.com/brt.org/Business_Roundtable_Artificial_Intelligence_Roadmap_Jan2022_1.pdf; Business Roundtable, *Putting Data to Work* (2015), <https://s3.amazonaws.com/brt.org/archive/reports/BRT%20PuttingDataToWork.pdf>.

fraud-prevention, anti-money laundering and cybersecurity protections depend on data-driven technologies to be effective and accurate. Financial services firms also leverage data to better serve historically underserved communities.

Energy. Many energy companies are heavily regulated by state and federal agencies other than the FTC, and routinely collect and use customer data to improve services and achieve energy efficiency and emission reduction goals. For example, consumer data related to energy usage (e.g., via smart thermostats) allows energy providers to offer customers personalized options for how to reduce energy use and expenditures. Smart thermostats also can help identify whether a consumer's HVAC system is working by comparing home temperatures to weather data. Data obtained from connected devices is used to improve commercial building efficiency and are helping companies across sectors meet their net-zero carbon emission goals.

Communications. Companies offering customer communications solutions use consumer data in many of the ways other companies do—to offer new and improved services to customers and to improve user experience. But these companies also regularly use consumer data to perform vital and basic business functions such as maintaining network operations, identifying and repairing problematic aspects of the infrastructure, and determining and remedying the reasons for service issues.

Retail. Consumer data is vital to understanding customer needs, including whether new features might be beneficial, more convenient, or more relevant to consumers. Indeed, algorithmic decision-making support is an additional vital tool that companies use to improve the consumer experience by enabling the creation of self-service portals, consumer preferences and customer service with faster resolution of consumers' questions. As a result, companies can provide consumers with a more personalized experience and offer consumers products and services based on their preferences. Depending on just how far the FTC stretches "commercial surveillance," retail firms, particularly in the food services sector, might not be able to implement key business processes, such as automated inventory management or integrated loyalty programs.

E-Commerce. Anonymized consumer data also allows companies to improve customer experience through updating key features of retail webpages. For example, certain data can identify areas of websites that do not work and frustrate consumers. Location-based personalization allows companies to only show products that are available in the consumers' city or state.

Advertising. Companies use consumer information to help connect consumers with products or services that suit their interests, providing additional information that helps consumers make more informed choices. Many brands rely on customer data that they themselves obtain from their own customers, using that information to provide more-relevant products and services to their own customers, who provide their express consent to be informed about new products or

services. And strict limitations on using customer information to show targeted advertising to potential new customers ultimately would harm consumers and competition, as advertising would revert to the antiquated “spray and pray” model that (a) inundates consumers with information irrelevant to their consumption priorities and (b) drives up the cost of customer acquisition for companies.

Conclusion

Business Roundtable shares the FTC’s desire to protect consumers from unscrupulous privacy and security practices. However, the solutions previewed in the ANPR risk greater consumer harm than many of the problems the FTC has identified. Sweeping restrictions on the use and collection of consumer data will limit consumer choice and stifle innovation. And, in the end, the FTC’s rule will lead to yet another set of inconsistent standards that serve only to confuse consumers as to their privacy rights.

For these reasons, we urge the Commission to defer to Congress to forge a lasting legislative compromise on these important issues and to provide greater clarity to the Commission with respect to the scope of the agency’s privacy and data security authority.

Business Roundtable appreciates the opportunity to provide our input during this process. We would be happy to discuss these comments or any other matters you believe would be helpful. Please contact William Anderson, Vice President, Business Roundtable, at wanderson@brt.org or 202-496-3259.