Submitted electronically via ww.regulations.gov

November 21, 2022

Secretary April Tabor
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 Secretary Tabor:

On behalf of the more than 80,000 combined members of the National Multifamily Housing Council (NMHC)[1] and the National Apartment Association (NAA)[2], we submit these comments in response to the Federal Trade Commission's ("FTC" or "Commission") Advance Notice of Proposed Rulemaking on the Trade Regulation Rule on Commercial Surveillance and Data Security (Commercial Surveillance ANPR, R111004). NMHC and NAA represent for-profit and non-profit owners, operators, developers and property managers involved in the provision of rental housing, both affordable and conventional.

Executive Summary

Apartment owners and operators, as well as their service providers, rely heavily on personal data about apartment applicants, residents and employees to run their day-to-day business. Therefore, we are actively engaged in issues surrounding data security and safeguarding consumer privacy. Given the sensitivity of the information that apartment operators rely on and the ever-expanding cyber threat landscape we face, our industry has placed a high priority on strengthening defenses against vulnerabilities and protecting personal data and consumer privacy.

[1] Based in Washington, D.C., the National Multifamily Housing Council ("NMHC") is a national nonprofit association that represents the leadership of the apartment industry. Our members engage in all aspects of the apartment industry, including ownership, development, management and finance, who help create thriving communities by providing apartment homes for 40 million Americans, contributing $3.4 trillion annually to the economy. NMHC advocates on behalf of rental housing, conducts apartment-related research, encourages the exchange of strategic business information and promotes the desirability of apartment living. Over one-third of American households rent, and over 20 million U.S. households live in an apartment home (buildings with five or more units).

[2] The National Apartment Association (NAA) serves as the leading voice and preeminent resource through advocacy, education, and collaboration on behalf of the rental housing industry. As a federation of 149 state and local affiliates, NAA encompasses over 93,000 members representing more than 10.5 million apartment homes globally. NAA believes that rental housing is a valuable partner in every community that emphasizes integrity, accountability, collaboration, community responsibility, inclusivity and innovation.

Technology and innovation have driven significant change in the multifamily industry in recent years and have improved the resident experience while allowing greater business efficiency for multifamily firms as they work to provide rental housing to millions of Americans.

Our industry's vantage point as it relates to the collection, use and safeguarding of data is summarized below:

- **Our most important assets are our apartment residents**. Data collection and use is about serving our customers – America's renters. We are committed to equal access to housing, meeting resident expectations of affordability and livability, and providing residents safe and quality homes.
- **Rental housing providers include small business owners, employers and job creators** that depend on reliable data that produces accurate decisions to protect their business operations while expanding housing opportunities to millions of American families. Accountability, accuracy and transparency in the consumer reporting ecosystem is critically important to both apartment operators as well as our current and future residents.
- **Data-driven asset management** can inform operational efficiencies through energy and other cost savings, leading to improved property operations and reduced operational costs.
- **Security is a shared responsibility across the data ecosystem**, with third party service providers serving as a keystone. Responsibility for security should be shared throughout the supply chain and not lie solely with the party that interacts with the consumer. This is why apartment operators strive to work closely with their supplier partners to ensure contractual obligations in the wake of any security or privacy breach are clear.
- **Automated decision making is not inherently discriminatory** and can be a solution to overcome human bias and prejudices found in conventional decision-making mechanisms, while providing numerous other benefits to consumers by reducing costs and speeding decision times.

Any efforts to regulate date privacy and security should include Congress. The legislative process is important and necessary, as the elected members of Congress can reflect the needs of their constituencies while creating laws that reflect compromise. **The Commission should not circumvent congressional efforts in this space.** Instead, the Commission should continue its important work in educating the public on data security and privacy awareness and providing critical resources to the business community to boost preparedness.

The apartment industry's priority is for Congress to establish a federal data privacy and security standard that includes:

- A clear **federal preemption** of the existing patchwork of often conflicting and contradictory state data security, privacy and breach notification laws
- A **scalable and flexible standard**
- A clear **assignment of financial and legal liability** to the entity that suffered the data security or privacy incident

On behalf of the owners, developers, and operators of rental housing, as well as our nation's renters, we appreciate the opportunity to submit comments on this important discussion about the data ecosystem. The industry is committed to providing a safe and secure community for those who call rental housing home. That commitment extends to ensuring that information collected, used, or retained on apartment residents is secure and their privacy is safeguarded.

We value the Commission's focus on promoting consumer privacy and look forward to working with Congress to develop a clear regulatory framework that enables companies such as apartment firms and providers to comply with a singular standard that takes into consideration the type of data collected and a company's resources.

As we will discuss in more detail, the privacy and security of consumers' information is of utmost importance to both organizations and our collective membership. We stand read to work directly with the Commission and federal policymakers on these important issues.

The Apartment Industry Supports a National Data Privacy and Protection Standard

NMHC and NAA clearly understand and appreciate the importance of protecting consumers and strengthening cybersecurity requirements to combat an evolving threat landscape. For well over a decade, the multifamily industry has called for such protections for our residents and our business operations. As policymakers in Congress, the FTC and other federal agencies explore additional protections, NMHC and NAA support the following principles designed to enhance consumer protections while avoiding costly and burdensome regulation on rental housing providers of all sizes. A federal data privacy and security standard is needed and should include the following:

- **A clear federal preemption of the existing patchwork of often conflicting and contradictory state data security, privacy and breach notification laws.** Large apartment firms that operate across state lines and smaller apartment owners and operators benefit from uniform requirements for privacy and data security, allowing resources to be focused on meaningful defense against vulnerabilities and appropriate controls for handling personal information rather than incurring needless costs to support arbitrary disclosure requirements across different jurisdictions.
- **A scalable and flexible standard** that takes into consideration the needs and available resources of small businesses as well as large firms and the sensitivity of the data in question.
- **A clear assignment of financial and legal liability** to the entity that actually suffered the breach, particularly in the case of third-party breaches.

Core Commitment to Residents' Digital Security and Privacy

At the core of the industry is a focus on service to residents and a commitment to provide a safe and secure community for those who call rental housing home. That commitment extends to ensuring that information collected, used, or retained on apartment residents is secure and their privacy is safeguarded.

As part of the industry's commitment to data protection and privacy, NMHC is a member of the Real Estate Information Sharing and Analysis Center (RE-ISAC) and an NMHC staff representative serves on the Steering Committee of the Commercial Facilities Working Group, a partnership between RE-ISAC, InfraGard National Capital Region, a chapter of FBI's public-private partnership program, and firms in the commercial facility sector across the country.

Apartment owners and operators, as well as their service providers, rely heavily on a wide variety of personal data about apartment applicants, residents and employees to run their day-to-day business. Given the information that apartment operators rely on and the ever-expanding cyber threat landscape we face, our industry has placed a high priority on strengthening defenses against vulnerabilities and protecting sensitive data and consumer privacy. In fact, NMHC and NAA member firms are committing tremendous resources to this cause.

We have undertaken efforts within the apartment industry to mitigate cybersecurity risks, to implement policies to prevent such risks, and to encourage investments in bolstering cyber defenses to protect data. To that end, both NMHC and NAA have worked tirelessly to provide actionable tools for apartment firms to take to strengthen their cybersecurity and data privacy protocols. This content is in the form of commissioned white papers and in-person roundtables and events focused on understanding the threat landscape and providing resources and strategies for the apartment industry. In fact, NMHC and NAA regularly highlight the Commission and other government resources for businesses and work across the real estate industry to ensure regulatory compliance and overall preparedness.

NMHC coordinates a multifamily industry-specific cybersecurity alert system that is paramount to preparedness and awareness of vulnerabilities and law enforcement advisories. This work demonstrates the commitment made by NMHC and our membership to enable information sharing to better residents, business operations and the rental housing sector's cybersecurity posture and resiliency. NMHC also provides a suite of resources and strategies to support member firms in hardening their cyber defenses and creating a culture of data protection and privacy.

NAA provides resources to members through naahq.org/data-security-privacy-operational. Recently, NAA hosted a webinar on data privacy that focused on the types of data currently being collected and what can and cannot be done with that information. The webinar also covered the upcoming changes in privacy laws in 2023 across multiple states efforts on draft federal legislation, resident concerns with data collection, and included an advisable sampling of disclosures and consents.

NMHC and NAA have also submitted comment letters and input on proposed rules and legislation to inform federal policymakers of the industry's commitment to data security and privacy. Of note, NMHC and NAA have submitted the following comment letters in 2022:

- SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposed Rule - Comment Letter
- The American Data Privacy and Protection Act - Comment Letter to the House Energy and Commerce Committee
- H.R. 8152, The American Data Privacy and Protection Act - Comment Letter to the House Energy and Commerce Subcommittee on Consumer Protection and Commerce

Necessary Data Collection in the Rental Housing Industry

The lifecycle of consumer engagement in the apartment industry typically begins when an individual explores moving into a multifamily community. The relationship between the renter and the apartment manager may span years; industry participants collect various types of information, some on a static basis, such as during initial resident screening in the leasing process, and some

continuously, such as via rental and utility payments or other interactions. Consumer data contained in screening reports and data generated regularly and held by property managers and their service providers is crucial in accounting for rental history, tenure, and payment data, which makes up an important part of a resident's profile and can serve as a tool to improve a resident's housing opportunities in the future. It is important to note for regulators and policymakers that the absence of such data could have unintended consequences for consumers and negatively impact their housing opportunities in the future.

The emergence and operational value of building technologies including smart products, appliances and systems; efficiency measures; and management systems is changing how the multifamily industry designs and builds properties and how apartment firms are working to meet sustainability goals, resident demand and market-driven expectations for new technologies and amenities. Given the inherent diversity in the nation's rental housing stock, the purpose, deployment and management of these new technologies can vary significantly from property to property. For example, when an apartment community provides smart devices throughout a community, the aggregate, de-identified data can be used to improve operational efficiencies and manage whole-building energy use.

Properties of all types are deploying smart building technologies that are revolutionizing operations and lowering the cost of providing housing. Apartment firms are implementing these devices to meet resident demand, increase the convenience of apartment living, and to create environmental and operational efficiencies. It is important to note that residents are demanding smart home technologies for many of these same reasons, including to improve the quality of their living experience, to reduce environmental impact, and to save money (e.g., on utilities). The importance or desirability of smart home technology is only expected to increase in the future.

Renter Preferences for Connected Communities

Resident preferences and the environmental, security, and financial benefits for both residents and apartment operators from these devices ensure that their deployment will continue to drive innovation in the multifamily industry. The *2022 NMHC/Grace Hill Renter Preferences Survey Report*[3] highlights survey results from 221,000 apartment residents nationwide covering leasing decision factors, amenity desires, and the like.

Findings about resident preferences for in-home connected devices include:

- **smart thermostats:** 70% were interested in/would not rent without
- **leak detection**: 67% were interested in/would not rent without
- **video doorbell at the unit:** 64% were interested in/would not rent without
- **smart lighting:** 62% were interested in/would not rent without
- **keyless smart locks:** 59% were interested in/would not rent without
- **biometric access to home:** 38% were interested in/would not rent without

[3] The 2022 NMHC/Grace Hill Resident Preferences Survey Report collects insight from over 221,000 renters, living in 4,564 communities nationwide with data available in 79 markets, https://www.nmhc.org/research-insight/research-report/nmhc-grace-hill-renter-preferences-survey-report/

Community amenities are also a crucial factor in a prospective or current resident's decision to make an apartment community home. *The 2022 NMHC/Grace Hill Renter Preferences Survey Report* also reflects residents' demand for connected amenities, including:

- **controlled property/amenity access**: 71% interested/would not rent without
- **video intercom at the property entrance:** 48% interested/would not rent without

The use of these devices in a multifamily context as opposed to use and deployment by an individual homeowner provides for unique security and privacy considerations that apartment firms take seriously. These technologies and the nature of the information exchanged create nuanced challenges and complexities for the industry in addressing the requirements in the Advance Notice of Proposed Rulemaking (ANPR). By way of example, the use of smart home technologies, such as consumer-permissioned access control systems, could result in the collection of certain data types that potentially could be considered personal information but would differ significantly from traditional types of personal information, both in the type of information generated and the way in which it is transmitted and stored. Relatedly, certain data may be maintained in unstructured formats not conducive to being readily accessed or deleted.

Congress Should Implement a Single, Flexible National Regulatory Framework

The laudable, bipartisan work done by Congress to prioritize consumer data privacy protections reflects a bipartisan recognition that the country must act to protect data privacy and security. Congress is currently debating the American Data Privacy and Protection Act, which is the most significant step forward to creating a federal standard. The broad bipartisan and bicameral support reflects the compromise struck between both sides of the aisle on federal preemption and private right of action. Should ADPPA or similar proposal become law, Congress will have authorized the Commission to enforce data privacy and security and will provide the Commission clear rulemaking and enforcement authority.

The legislative process is important and necessary, as elected members of Congress are able to reflect the needs of their constituencies while creating laws that reflect compromise. **The Commission should not circumvent congressional efforts in this space.** Instead, the Commission should continue its important work in educating the public on cyber and privacy awareness and providing critical resources to the business community to boost preparedness.

NMHC and NAA endorse a single, flexible national regulatory framework for data security, privacy and breach notification. We also support a balanced approach to providing consumers and investors with meaningful insight into a business's operations and how data is being used while not imposing overly burdensome regulations on the apartment industry or unintentionally exposing our members to substantially greater cybersecurity risks. Flexibility is needed to navigate the significant variety of data use and collection practices, resources available, as well as the sophistication of individual apartment firms.

Any federal law governing data privacy and security must include a clear federal preemption. The current and ever-evolving patchwork of state laws creates a compliance burden and leaves consumers vulnerable to mistakes, misunderstandings, and unintended consequences. For example, North Carolina's breach notification law requires the notice to the impacted individual include a brief description of the nature of the incident (N.C. Gen. Stat. § 75-65(d)(1)), while Massachusetts prohibits such a description (Mass. Gen. Laws ch. 93H(Sec. 3)(b)(para. 3)). The California, Colorado, Virginia, Connecticut and Utah new privacy laws all ascribe special protections and

disclosures to "sensitive" data, but each state defines sensitive data slightly differently. California Civil Code. § 1798.140(ae)(as amended) (uniquely includes social security number, drivers license number, trade union membership, philosophic beliefs); Colorado C.R.S. §§ 6-1-1303(24)(includes "citizenship status" but not immigration status); Virginia Code § 59.1-575 (includes "immigration status" but not citizenship status); Connecticut P.A. 22-15 § 1(27)(adds "sex life" to Virginia's list); Utah Code § 13-61-101(32)(does not include data on children in definition, which is included in the other states). A business collecting social security numbers for credit checks would need to disclose it is collecting sensitive data in California, but would be misdescribing its collection practices in the other four states.

A federal data privacy and security law also must be flexible and scalable, as well as take into account the data collected and the size of the company, and the needs/available resources of small businesses. Importantly, it also must include clarity on third-party liability. In an increasingly connected world, the consumer-facing apartment company must engage with multiple third-party service providers for a variety of services. Each service provider must be responsible and accountable for their own security and privacy safeguards and for any third-party security lapse or privacy violation.

Rental Housing Perspective on the Commercial Surveillance ANPR, R111004

ANPR R111004 includes 95 questions covering a broad range of issues. Given the scope of the ANPR, it is impossible to cover the full breadth of this initial inquiry, but there are broad themes and assumptions included that are of concern to the rental housing industry.

1. Which practices do companies use to surveil consumers?

NMHC and NAA take issue with framing the topic of data-informed decisions as "corporate surveillance." The Commission's decision to frame this conversation in this manner minimizes the important role that data and smart technology play in critical business operations and the role it plays in meeting the evolving demands and expectations of our residents. There are innumerable reasons that a company would gather data to best serve their customer by making informed business decisions. We support a national data privacy and security standard broadly, but the debate must acknowledge that data collection is not inherently nefarious.

2. Which measures do companies use to protect consumer data?

NMHC and NAA and their collective membership understand the critical importance of maintaining the integrity of the highly sensitive data collected, used, and maintained to support applicants, residents, and employees in the apartment industry. In the course of doing business, rental housing owners and operators, and their third-party service providers, collect, use, and maintain a significant amount of personal data about applicants, residents, and employees. This information is used in a wide variety of essential business operations but also makes apartment firms and their suppliers a target of malicious actors.

Given the ever-expanding cyber-threat landscape, the apartment industry has made defense against these vulnerabilities a top priority. We have undertaken efforts within the apartment industry to mitigate cybersecurity risks, to implement policies to prevent and mitigate such risks, and to encourage investments in bolstering cyber defenses to protect data. To that end, we have

commissioned white papers on the threat landscape and provide resources and strategies for the apartment industry.

NMHC and NAA are broadly supportive of federal legislative and regulatory efforts to bolster cybersecurity and to ensure that investors and consumers receive comparable material information regarding companies' cyber risk management and incidents. The industry has been challenged by the lack of harmonization amongst the various incident reporting obligations, which is burdensome, especially for smaller businesses. Apartment firms increasingly operate across multiple states and must comply with a patchwork of 50 different state laws governing data security and breach notifications, various federal cybersecurity incident reporting requirements, and potentially foreign laws. The lack of harmonization amongst these governmental entities increases costs and causes confusion as agencies and consumers receive notifications at different times concerning the same cybersecurity incident.

NMHC and NAA urge greater flexibility and scalability with reporting cybersecurity incidents to reduce burdens on companies, especially concerning the details sought and the constant periodic reporting obligation. Moreover, NMHC and NAA cybersecurity incident disclosure obligations to be consistent with other federal agencies and state laws.

43. To what extent, if at all, should new trade regulation rules impose limitations on companies' collection, use, and retention of consumer data? Should they, for example, institute data minimization requirements or purpose limitations, i.e., limit companies from collecting, retaining, using, or transferring consumer data beyond a certain predefined point? Or, similarly, should they require companies to collect, retain, use, or transfer consumer data only to the extent necessary to deliver the specific service that a given individual consumer explicitly seeks or those that are compatible with that specific service? If so, how? How should it determine or define which uses are compatible? How, moreover, could the Commission discern which data are relevant to achieving certain purposes and no more?

Some of the areas of regulation seemingly being considered by the Commission may unintentionally raise the cost of providing housing that is affordable by adding additional hurdles in property operation and make it even more challenging to meet the daily needs of our residents. The Commission should proceed cautiously with any type of rulemaking that could disrupt the work and goals of a number of federal agencies that have jurisdiction over the housing market, including the Department of Housing and Urban Development (HUD), the Federal Housing Finance Agency (FHFA)/Government Sponsored Entities (GSEs), the Department of Agriculture (USDA) and federal banking regulators. Rental housing providers have existing data collection, retention and compliance obligation through a variety of federal laws and regulations that govern housing operation and renter protection.

By limiting the time period of data availability on consumer/housing reports, regulation may ultimately work against the goal of expanding housing opportunity, forcing property owners to rely on less information/mainly financial in nature and narrows the available housing for renters, especially those of lower-incomes or less established financial profiles.

44. By contrast, should new trade regulation rules restrict the period of time that companies collect or retain consumer data, irrespective of the different purposes to which it puts that data? If so, how should such rules define the relevant period?

As discussed in response to the previous question, limiting the time period of data availability on consumer and/or housing reports ultimately may work against the goal of expanding housing opportunity. Without access to robust data, rental housing providers may be forced to rely on less comprehensive data, such as data that is mainly financial in nature. This may in turn narrow available housing for renters, particularly for those with less established financial profiles.

69. Should the Commission consider new rules on algorithmic discrimination in areas where Congress has already explicitly legislated, such as housing, employment, labor, and consumer finance? Or should the Commission consider such rules addressing all sectors?

Housing, and the real estate market more broadly, is a heavily regulated sector at nearly all levels of government. At the federal level alone, myriad agencies and regulators are involved in everything from the development, operation and financing of real estate because of their critical importance to housing Americans and contributing to the economy.

For example, many of the issues being examined in this proceeding face regulatory oversight and compliance requirements from a number of federal agencies that have jurisdiction over the housing market, including the Department of Housing and Urban Development (HUD), the Federal Housing Finance Agency (FHFA)/Government Sponsored Entities (GSEs), the Department of Agriculture (USDA) and federal banking regulators. The Commission should proceed cautiously with any type of rulemaking that could disrupt the work and goals of these federal partners, which is essential to data collection, retention and compliance provisions of various federal laws and regulations that govern housing operation and renter protection.

This is particularly important in light of the nation's housing affordability challenges. Some of the areas of regulation seemingly being considered by the Commission will unintentionally raise the cost of providing housing that is affordable by adding additional hurdles in property operation and make it even more challenging to meet the daily needs of our residents.

Smart regulations play an important role in ensuring the health and well-being of the American public and often require data collection and use to demonstrate compliance. This is not corporate surveillance, but instead part of a rental housing provider's obligation to demonstrate compliance with existing regulations.

The ANPR suggests that automated systems may make decisions that impact protected classes access to housing, employment and credit in a negative manner. Automated decision making is not inherently discriminatory any more than any other decision-making mechanism and has the potential to negate human bias and prejudices. Existing anti-discrimination laws still apply to these emerging tools, which may have the benefit of reducing the decision-making time, allowing the incorporation of additional positive information into the decision-making process for those with lower credit histories, and creating efficiencies throughout the system.

Policymakers across the federal government and within federal agencies must work in coordination, and not at cross-purposes, to help increase our nation's housing supply and drive down the cost of housing development and operation, while ensuring the broader real estate market is able to operate efficiently without undue regulation so that it can continue to drive our economy and ensure that Americans have quality housing that is affordable to them.

Conclusion

On behalf of the owners, developers, and operators of rental housing, as well as our nation's renters, we appreciate the opportunity to submit comments on this important discussion about the data ecosystem. We value the Commission's focus on promoting data security and privacy and look forward to working with Congress to develop a clear regulatory framework that enables companies such as apartment firms and providers to comply with a singular standard that takes into consideration the type of data collected and a company's resources.

As noted above, the privacy and security of consumers' information is of utmost importance to NMHC, NAA and our collective membership. We stand read to work directly with the Commission and federal policymakers on these important issues.

Sincerely,

Doug Bibby
President
National Multifamily Housing Council

Robert Pinnegar, CAE
President & CEO
National Apartment Association