Main Street
PRIVACY COALITION

Lina Khan
Chair of the Commission
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610
Washington, DC 20580

RE: Commercial Surveillance ANPR, R111004

Dear Commissioner Khan,

The Main Street Privacy Coalition ("MSPC") appreciates this opportunity to provide comments on the Federal Trade Commission's ("FTC" or the "Commission") advanced notice of proposed rulemaking on the Trade Regulation Rule on Commercial Surveillance and Data Security.[1] MSPC has long advocated for uniform national data privacy and security regulation. Having data privacy and security regulation that create clear protections for Americans while allowing our members' businesses to serve their customers in the ways they have come to rely upon is a key goal. Achieving that goal, however, has been elusive. One of the challenges that has been central to this effort is that the overwhelming focus on the data practices of technology companies by many participants in public debates about privacy should not blind us to the fact that privacy and security regulation needs to work for Main Street. Therefore, MSPC has provided a set of guiding principles that we believe the Commission should consider before setting any regulation of data privacy and security. We also take this time to comment on specific questions raised in the Commission's advanced notice of proposed rulemaking.

I. Background on MSPC

The MSPC is comprised of a broad array of 19 national trade associations that together represent more than a million businesses that line America's Main Streets. From retailers to Realtors®, hotels to home builders, grocery stores to restaurants, gas stations to travel plazas, and self-storage to convenience stores, MSPC member companies interact with consumers day in and day out. Our members' businesses can be found in every town, city and state in our nation, providing jobs, supporting our economy and serving Americans as a vital part of their communities. Collectively, the industries that MSPC trade groups represent directly employ approximately 34 million Americans and constitute over one-fifth of the U.S. economy by contributing $4.5 trillion (or 21.8%) to the U.S. gross domestic product.[2]

[1] Federal Trade Commission, *Trade Regulation Rule on Commercial Surveillance and Date Security*, 87 Fed. Reg. 51273, *available at* https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.
[2] Information on the MSPC including a full list of its members can be found at https://mainstreetprivacy.com/about/.

II. Principles of Coalition

The exchange of data is central to much of the world's commerce. To ensure that business occurs as intended on a daily basis requires large volumes of data to be used and exchanged by a multiplicity of different actors. The ways in which this happens is incredibly diverse across the economy and therefore quite complex. That diversity and complexity is one of the reasons that data privacy regulation is so challenging.

While data regulation tends to focus on policy dealing with how commerce takes place on the Internet or the tech sector, MSPC's chief concern is how these regulations would impact Main Street businesses. It is important to note that Main Street businesses use data to more effectively serve their customers. It is not "commercial surveillance" of the type that animates the concerns underlying the FTC's request for comments. That "surveillance" consists of tracking consumers across multiple services/websites or devices over time by businesses in situations in which the consumer does not know he or she is interacting with that business. That is quite different than what Main Street businesses do. Merchants using data to communicate offers to their existing customer base is fundamentally different than what data brokers and third parties unknown to consumers do with information. And, it is quite different than businesses which treat customers and their data as the product. Main Street's use of data should not be grouped with these other uses of data.

To make sense of privacy policy in light of the vast number of complex data-sharing activities that happen on a regular basis, MSPC has formulated some guiding principles that summarize our position:

- **Establishing Uniform Nationwide Rules and Enforcement for Data Privacy** – We should have a sensible, uniform federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws by enacting a set of nationwide rules for all businesses handling consumers' personal data is necessary to achieve the important, national public policy goal of uniform consumer privacy protections.

- **Industry Neutrality and Equal Protection for Consumers Across Business Sectors** – Federal data privacy frameworks and regulation should apply requirements to all industries that handle personal data and not place a disproportionate burden on certain sectors of the economy while simultaneously alleviating other sectors from providing equal protection of consumer data. An equivalent data privacy standard should apply, regardless of whether a business directly collected data from a consumer or obtained it in a business-to-business transaction.

- **Direct Legal Obligations (Rather than Contractual Requirements Alone) for All Entities that Handle Consumer Data** – Effective consumer protection regulations

cannot be achieved by relying on some businesses to regulate the conduct of other businesses through contracts alone. Data service providers and other third parties need direct regulatory obligations to ensure they comply with relevant privacy scheme, particularly those offering transmission, storage, analytical processing or other consumer data services for thousands of small businesses.

- **Preservation of Customer Rewards and Benefits** – Any federal data privacy framework should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships and set the terms of those relationships. FTC regulation should include safe harbors to ensure that consumers can purchase, or otherwise obtain, the goods and services they want by taking advantage of benefits, incentives or enhanced services they earn from being loyal customers, even if other customers choose not to engage in such programs.

- **Transparency and Customer Choice** – Consumers deserve to know what categories of personal data businesses collect and how that data is generally used. These policies should be clearly disclosed in company privacy policies readily accessible to consumers. These obligations should apply to all businesses handling consumers' personal data, including service providers, third parties, and financial services businesses.

- **Accountability for Business's Own Actions** – Privacy regulation should not include terms that could potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of a business partner. Those business partners should be responsible for their own compliance and any resulting liability. In particular, consumer-facing businesses should not be unfairly saddled with liability if other types of businesses do not fulfill their own obligations under the regulation.

- **Data Security Standards** – A federal data privacy regulation should include a reasonable data security standard for all businesses handling consumer data, as well as a uniform process for businesses suffering a data security breach to notify affected individuals. Currently, consumer-facing industry sectors are required to comply with 54 state and U.S. territorial laws on data breach notification requirements, and nearly half of the states have enacted data security laws. However, financial institutions and service providers are often exempt from these state breach notice requirements. All businesses handling consumers' data should be required to protect personal data and provide notice of their own security breaches when they occur.

We believe these principles provide fundamental guidance for proposing any privacy regulation that will be effective and beneficial for consumers and businesses alike.

III. Answers to FTC's proposed rulemaking questions for comment

- Which kinds of data should be subject to a potential trade regulation rule? (question 10)

Businesses should be able to collect and use the types of consumer data that consumers reasonably expect the business to retain. Consumer expectations are an important consideration for both consumers and businesses when engaging in any transaction. FTC should be careful not to impose overinclusive limitations or restrictions on businesses' ability to collect and store consumer data that consumers reasonably expect businesses to collect and store. To take the simplest example, if a Main Street business has agreed to send a product to a consumer's home, the business needs to collect and store data pertaining to the consumer's mailing address and connect that to information about the product purchased. Not only does a consumer expect this, but this data is also necessary in order for the underlying transaction to occur.

In the case of advertising, most consumers understand and expect a business from which they have already purchased a good to retain data and market new or related products or services to that consumer. Advertising to prospective customers is also an expected part of regular commerce for businesses and consumers alike. That type of advertising has been a fundamental part of the U.S. economy throughout its history and has been determined to be protected commercial speech under the First Amendment in many cases. Its important role in daily commerce should not be disrupted.

While many small businesses can only carry out these expected marketing practices through the use of service providers, consumers expect them and they are an essential part of many business relationships that consumers have with businesses they frequent as they provide helpful suggestions of products consumers may be interested in and are often a source of discounts. Overall, FTC should consider reasonable consumer expectations when deciding on any restrictions on the types of data that businesses can collect and store.

- To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm? (question 12)

There are risks involved with a sectoral regulatory approach. In particular, financial institutions by necessity retain some of the most sensitive consumer financial data – including social security numbers, driver's license numbers and other data that which can be used to perpetrate identity theft. Yet, Main Street businesses send data to, and receive data from, these financial institutions millions of times each day to effectuate the basic functioning of commerce across the nation. If businesses that interact this frequently have different regulatory regimes, there is a strong risk that consumer protections for some data practices will be lost in the gaps between those regulatory schemes.

A similar situation exists with many categories of "service providers" that process data in ways that is essential to the conduct of business – from payments data to marketing and other

data. These "service providers" are often the very technology companies that have engendered some of the strongest concerns among consumer regarding how their data is collected and used. Unfortunately, sectoral approaches to regulation risk under-regulating these service providers and leaving gaps in privacy regulation.

In each of these instances, it is important to note that the vast majority of Main Street businesses are small businesses that rely on financial institutions and service providers to conduct business. Yet, Main Street businesses are typically in a disadvantaged bargaining position with respect to these other businesses. Sectoral approaches to regulation often assume that businesses with the direct consumer relationship can control the other businesses involved in effectuating commerce (such as financial institutions and service providers). That is a false assumption. In fact, if anything, control most often runs in the other direction as service providers and financial institutions write contracts of adhesion to which Main Street businesses must agree. We strongly urge the FTC to avoid these pitfalls which have hampered past efforts at privacy regulation.

- Should the Commission take into account other laws at the state and federal level (*e.g.,* COPPA) that already include data security requirements. If so, how? (question 35)

An important justification for federal data protection regulation is that it can provide clear and consistent rules for consumers and businesses regardless of where they are located or operate across the nation. There are a multitude of state laws governing data privacy and security around the nation with differing compliance requirements. Therefore, promulgating a federal regulation that does not preempt state law would merely add another inconsistent standard. Any federal privacy regulation must be preemptive and establish national rules.

Additionally, ensuring that consumers are protected regardless of the business sector that handles their data is fundamental to ensuring effective data protection regulation. This includes the regulation of financial services firms. Currently, those firms are covered by privacy provisions of the Gramm Leach Bliley Act (GLBA). However, the privacy provisions under GLBA are wholly inadequate for protecting consumers in today's digital age. GLBA, enacted in 1999, required that covered businesses send customers a written privacy policy once per year and provide them with a limited ability to opt-out of third-party marketing. That is it. Although financial services firms collect and hold some of customers' most sensitive data, GLBA does not include many of the privacy provisions that have become common in state laws. GLBA is not sufficient to protect consumer privacy and should not be relied upon in any data privacy regime.

- The Commission invites comment on the relative costs and benefits of any current practice, as well as those for any responsive regulation. How should the Commission engage in this balancing in the context of commercial surveillance and data security? (question 24)

Any regulation needs to take into account the types of data collected and how some data collection benefits consumers and businesses alike. One of MSPC's chief concerns is that FTC

regulation could interfere with loyalty and rewards programs. Those programs often provide customers things like free or discounted items after a certain number or dollar value of purchases. In order to provide those types of rewards, businesses must have a way to keep track of the purchases made by those customers. The accounting done to enable these programs are not "commercial surveillance" and the FTC should take care not to take actions that would treat them as such. These programs are valuable to both consumers and businesses who employ them. Americans overwhelmingly want these programs to remain intact and FTC should be careful to preserve them in any rulemaking.[3]

Additionally, MSPC believes that any regulations relating to data security be based on a standard of reasonableness. This is necessary due to the tremendous diversity among organizations that could be subject to FTC regulation. This standard for data security should take into account factors like the size and complexity of the entity and the sensitivity of the data it handles. This is important because the vast majority of Main Street businesses are small and unsophisticated compared to other businesses in the tech, telecommunication, and financial sectors. For example, in many single store operations – like a convenience store or restaurant – the owner of the business may work behind a counter serving customers for long hours every week. Overly complicated data security regulations could be unnecessarily burdensome for owners without a corresponding benefit to consumers. Therefore, it is important that any data security standards be based on reasonableness, taking into account the diversity of different businesses covered by the regulation.

- Given the reported scale, opacity, and pervasiveness of existing commercial surveillance today, to what extent is consumer consent an effective way of evaluating whether a practice is unfair or deceptive? (question 73)

Having clear consumer consent standards is key to effective data protection. Consumer consent allows consumers to receive the benefits they want and allow businesses to tailor their products to these consumers. Therefore, FTC should allow consumers to consent based on clear disclosures.

There are some commercial settings, of course, for which consent is not necessary or can be implied. For example, it is necessary for many Main Street businesses to retain data that tracks products sold, exchanged or returned by consumers, products under warranty, and other transaction information that are necessary to fulfill functions that consumers expect including allowing for the return or exchange of products or honoring warranties. We caution FTC against undermining the ability of Main Street businesses to operate. Focusing on how Internet

[3] According to a survey conducted by Bond Brand Loyalty Inc., 79% of consumers say loyalty programs make them more likely to continue doing business with brands that offer them and 32% of consumers strongly agree that a loyalty program makes their brand experience better. Bond Brand Loyalty Inc., The Loyalty Report (2019) available at https://cdn2.hubspot.net/hubfs/352767/TLR%202019/Bond_US%20TLR19%20Exec%20Summary%20Launch%20Edition.pdf.

companies process and use consumer data might unintentionally undermine some Main Street business practices that consumers expect and rely upon every day.

- 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? (question 44)

Any time restrictions on the retention of data must take into account the purposes for which data is used. If the FTC fails to recognize those different purposes, it risks undermining the essential elements of the bargain that consumers and businesses think they are getting. For example, Main Street businesses often have return or warranty policies that last for decades. In order to have such policies, businesses have to retain data for an extended period of time. Consumers today rely upon these policies and part of the value they have received in purchasing certain products could be undermined by a regulation that prevented businesses from honoring those warranties or returns. A blanket time restriction simply does not make sense in many commercial settings.

* * *

MSPC appreciates this opportunity to present our views on the FTC's advanced notice of proposed rulemaking on the Trade Regulation Rule on Commercial Surveillance and Data Security. We believe that uniform national data security and privacy regulation is important to protect consumers and allow our economy to function properly for all entities involved in data collection and holding. In order to achieve this goal, we believe that the seven principles presented above can help achieve the best public policy results in this area.

Sincerely,

Main Street Privacy Coalition