November 21, 2022

Submitted via www.regulations.gov

Federal Trade Commission
The Honorable Lina M. Khan, Chair
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Commercial Surveillance ANPR, R111004

Dear Chair Khan,

The National Retail Federation (NRF) respectfully submits these comments on the Advance Notice of Proposed Rulemaking (ANPR) the Federal Trade Commission (FTC) has published on the topic of commercial surveillance and data security.[1] The purpose of these comments is to provide the perspective of the retail industry on the proposal of the Commission to implement new trade regulation rules to govern the ways in which companies collect, use, and disclose consumer data.

NRF is the world's largest retail trade association representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and internet retailers from the United States and more than 45 countries. Retail is the nation's largest private-sector employer, supporting one in four U.S. jobs — 52 million working Americans. Contributing $3.9 trillion to annual GDP, retail is a daily barometer for the nation's economy.

A. EXECUTIVE SUMMARY

Protecting customer data is one of retailers' highest priorities. Retailers know that establishing long-term relationships with their customers requires more than just providing the merchandise they want at the prices they are willing to pay. Successful retailers earn their customers' trust and provide a satisfying shopping experience so that consumers continue to shop with them time and again. A critical element of establishing that trusted relationship lies in how retailers act as reliable stewards of the personal information their customers share with them when shopping.

Retailers have a long history of nurturing customer relationships and meeting consumer expectations for high quality service. Whether offering goods online or in store, retailers use customer data to provide personalized experiences that consumers value. Customers, in turn, expect retailers to process their personal data responsibly and seamlessly when they are shopping. To meet these high customer expectations, retailers invest heavily in technology and spend years developing

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273-51299 (Aug. 22, 2022).

appropriate methods to comply with state, federal and global data protection regulations in ways that further their customer relationships and do not frustrate them.

In short, retailers use consumer data for the principal purpose of serving their customers as they wish to be served. Retailers' use of personal information is not an end in itself but primarily a means of achieving the goal of improved customer service. They use customer data responsibly to do a better job of selling their products to customers – to do what they do better. This differentiates retailers from data brokers and other third parties unknown to the consumer that do not have direct relationships with individual customers. It also differentiates retailers from other first-party businesses that treat the customer as the product and sell their information. For retailers, the products they sell are the *products*, not their customers.

With respect to data privacy laws, NRF has long-supported federal data privacy legislation to establish uniform, national standards that protect all Americans' personal information wherever it is collected and used, regardless of the state where a consumer resides or a business is located. It is critically important for American commerce that Congress act to establish a clear framework that embodies privacy principles we strongly support. In the ANPR, the FTC now "invites comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive."

Although the FTC lacks the authority to establish a uniform, nationwide set of standards by preempting related privacy laws and regulations, its inquiry in the form of the ANPR provides an opportunity to assess the state of current U.S. data privacy laws and how the FTC could improve the approach to federal data privacy rules to ensure that they are customer-centric and risk-based. We believe it is critical for any regulations that result from this effort to align with and not result in further fragmentation of privacy standards in the U.S. If Congress were to enact a preemptive federal privacy law that authorizes the FTC to promulgate a trade regulation rule on data privacy, we believe rules that put customers first and focus on where they are at the greatest risk of harm would protect consumers best. It is with this purpose that we offer a proposed model that reflects these principles we believe the FTC should adopt if it promulgates data privacy rules as authorized by a preemptive federal law.

The customer-centric privacy model NRF proposes in these comments views the benefits and costs of the collection, use, and disclosure of personal data through the lens of the customer whose data is being used by a business. Customers of retail stores and other Main Street businesses value simplicity, clarity, and seamless interactions with the businesses with whom they choose to engage. Consumers know these businesses and benefit from the use of their customer data in ways that promote innovations to enable that business to better serve them. The model is also a risk-based approach that measures the level of risk to the consumer based on whether the consumer has an established customer relationship with the business that is processing the data and whether the use of their data by that business is consistent with their expectations.

This approach is aligned with the focus of the Commission's inquiry as explained in the ANPR. The Commission notes there are companies, and indeed industries, that "develop and market products and services to collect and monetize [consumer] data" that they collect as consumers "engage in the most basic aspects of modern life."[2] Others repurpose consumer data in ways not

[2] *Id.* at 51273.

disclosed to consumers.[3] As the Commission is aware, the web-browsing, searches, and social media posts of consumers are often used in ways that consumers do not understand or approve of, and that are akin to "commercial surveillance." Notably, the fundamental principles embodied in this analysis – established relationships, transparency of practices, and consumers' understanding and approval of data uses are inherent in the customer-centric and risk-based approach we support.

The practices the FTC equates with the moniker "commercial surveillance" are quite distinct in principle and practice from the purposes for which retailers collect and use personal data to better serve their customers. Retailers have first-party customer relationships and are subject to powerful market constraints on the collection and use of consumer data. If retailers are not good stewards of their customers' data and do not use data in ways that their customers anticipate, they will incur significant brand damage and lose those customers. Retailers must consistently earn and maintain the trust of their customers to successfully compete and grow. In a highly competitive industry like retail with millions of choices among retail businesses for consumers to choose to engage, the businesses that routinely lose customers due to irresponsible data privacy practices would surely run the risk of going out of business – a penalty far more severe than a regulatory fine.

These inherent market constraints are not present among the few, dominant social media, search, and other internet businesses that engage in what the Commission defines as commercial surveillance practices. The Commission therefore should be careful when crafting regulations for these businesses that are part of the "surveillance" economy not to miss the mark and inadvertently also cover Main Street retail businesses that are already directly accountable to consumers for their use and handling of personal data and already subject to every state's comprehensive data privacy laws. Rather, the FTC should focus its inquiry on the practices that place consumers at the greatest risk of harm.

We propose in these comments a framework for how the Commission can assess that risk from the viewpoint of consumers and calibrate proposed regulations to the level of risk faced by consumers – we call this framework the Customer-Centric Privacy Model and appreciate the Commission's consideration of this model in determining whether and how it may propose data privacy regulations.

B. THREE PRINCIPLES FOR DATA PRIVACY

The NRF believes that three key principles should shape any data privacy rules that the Commission may propose.

First, consumers should be free to make informed choices about how their data may be used to benefit them. For example, retail customers increasingly want product offerings tailored *by* them and related to their past shopping activity to help them make choices about future purchases. In addition, customers expect retailers to acknowledge and reward return customers with loyalty programs and other similar programs. Retailers should be allowed to respond to these consumer demands. On the other hand, consumers should be equally empowered to exercise rights to opt out of certain data uses, and retailers already make these opt outs and other data management controls available to customers. Put simply, consumers should be free to make informed choices about the collection and use of their data that suits them best.

[3] *Id.* at 51274.

Second, businesses should be permitted to use data responsibly to benefit and serve customers as they choose to be served. Retailers have legitimate business interests in using customer data to manage our relationship with customers and to provide customers with a level of service that they expect. For example, when a retailer alerts existing customers of new offerings that may be of interest to them, the retailer is acting on its legitimate interest in using customer information to better serve them by suggesting product offerings in which the customer may be interested. This concept of "legitimate interests" of retailers in using customer data is reflected in the European Union's General Data Protection Regulation (GDPR) and the United Kingdom GDPR, each of which establishes lawful bases to use personal data, including when a business has a "legitimate interest" in serving customers. Many American consumers value hearing from retailers who make them aware of new offerings that may be of interest. These data-driven communications help retailers build trusted relationships with customers and earn their business.

Third, federal privacy regulations should be both customer-centric and risk-based, and they should apply to all businesses that handle consumer data. The Commission should calibrate its regulations to be proportionate to the level of risk from varying business practices that use consumer data. New rules should not unduly burden customer-serving business models that use data responsibly and consistent with consumers' expectations and choices. They also should not *ignore* higher-risk, third-party data practices, especially those that leave consumers in the dark about who is using their data and for what purposes.

Retailers directly serve their customers in "first-party" relationships that present lower risk because they depend on trust earned and maintained over time. Retailers work to develop long-term, mutually beneficial customer relationships because they want to meet their customers' needs *now and* serve them in the *future*. Retailers need to maintain those relationships to succeed in the marketplace, which is the strongest possible incentive to use data responsibly and as customers expect. The retail industry views privacy and data security as critical to building trusted customer relationships.

By contrast, use of personal data by data brokers and other third parties that lack direct customer relationships creates a greater risk of harm, especially if the data is used for purposes consumers do not expect or approve. The Commission's own words in the ANPR support this principle:

> [M]ost people do not generally understand the market for consumer data that operates beyond their monitors and displays. Most consumers, for example, know little about the data brokers and third parties who collect and trade consumer data or build consumer profiles that can expose intimate details about their lives and, in the wrong hands, could expose unsuspecting people to future harm.[4]

Third-party businesses that are not retailers lack the same level of incentives of *customer*-serving businesses to use data responsibly and in alignment with consumers' interests because they are not in pursuit of long-term *customer* relationships with the consumers whose data they collect and process. Instead, by definition, third-party businesses do not directly serve customers and their lack of direct customer and market constraints on their use of consumer data coupled with the lack of transparency to the consumer regarding their data practices raises the risk to consumers. From the viewpoint of the consumer, data used by unknown parties for unknown purposes is the riskiest of all.

[4] Trade Regulation Rule, 87 Fed. Reg. at 51274 (internal citations omitted).

Federal privacy regulations should not rely on retailers and other businesses with direct customer relationships to contractually limit the rights of third parties whose business models are based on the indirect collection and use of consumer data. Such a regulatory model would protect consumer privacy only to the extent that retailers and other customer-serving businesses are successful in negotiating favorable contractual terms with third-party businesses, thus leading to inconsistent standards for consumers for the protection of their data. Large data analytics and digital advertising providers are often able to dictate the terms of their engagements with retailers and other businesses, including with respect to the rights of these providers in the data assets to which they receive access while delivering services. Negotiating terms can be especially difficult with vendors that post data protection terms online, as they are less willing to adjust those terms for individual business clients and present them on a take-it-or-leave it basis. Such a deficient and inconsistent approach in federal regulations would therefore unfairly target retailers and other customer-serving businesses that have first-party customer relationships while permitting third-party businesses to remain largely unregulated and able to leverage their market dominance against the customer-serving business in any negotiated agreement.

Such an approach leaves the protection of consumers in the position where the most market-dominant third-parties have the freest reign because they can ensure that the clients they serve cannot police their practices. NRF is opposed to such an approach that puts consumers in such a precarious position. For this reason, we support the principle that all businesses handling consumer data be directly regulated by the law, and that privacy protections should not be left to the uncertain results that flow from holding Main Street businesses accountable for the data practices of businesses that they cannot truly control through contractual agreements.

C. CUSTOMER-CENTRIC PRIVACY MODEL

NRF believes that federal privacy legislation and regulations developed in accordance with a customer-centric, risk-based approach will align inherently with consumer expectations, protect the rights of consumers to make informed choices concerning their data, and preserve the ability of retailers to innovate in the areas of product design, promotion, and sales to better serve customers.

The focus of the Commission's efforts should be on the areas of highest risk to consumers – a view which we believe is supported by the Commission's description of the harms underlying the decision to issue the ANPR.[5] The Commission should protect the use of personal data in a first-party context in a manner directed by the customer or for a purpose consistent with a reasonable customer's expectations.[6] These contexts are of inherently minimal risk and are different in kind from those giving rise to the term "commercial surveillance" in the ANPR.

[5] The Commission cites risks such as "[s]ophisticated digital advertising systems [automating] the targeting of fraudulent products and services to the most vulnerable consumers, [s]talking apps . . . endanger[ing] people, cyber bullying, cyberstalking, the distribution of child sexual abuse material [to children and teens], and the association of social media use with depression, anxiety, eating disorders, and suicidal ideation among kids and teens." Id. at 51275 (internal citations omitted).

[6] In the European Union, first-party businesses' data practices directed by their customers or for purposes consistent with their expectations would be considered to have their legal basis in what is referred to in the EU GDPR and UK GDPR as a "legitimate interest."

Main Street businesses depend on trusted relationships with customers earned and maintained over time based on their responsible use of data and strong data security practices. Retailers manage the risk of potential harm to their customers while using their data in ways that are beneficial to them, and they also provide data management tools to customers that enable them to opt out or choose how the retailer uses the data and communicates with them. We do not believe the Commission should focus its regulations on these kind of data practices that are of the least risk to consumers.

Consumers should have a right to exercise choices with respect to uses of data for purposes that are not consistent or compatible with their established business relationship. A consumer should, for example, be able to opt out from true sales of the consumer's personal data to a third party – transactions where the term "sale" is understood by its common meaning to a consumer, such as transfer of the consumer's data in return for monetary consideration to an unrelated third party who uses the data for the third party's own purposes. These would be instances where a consumer with an established business relationship may opt out of inconsistent or unanticipated data uses.

Consumers who do not have an established business relationship with a business that is using their data should have greater control of that data and choices over how that data may be used. Broader choice rights should attach when third parties with no established relationships to the consumer use their personal data. Any use by a third party as a controller should give rise to a right on the part of the consumer to opt out, at a minimum. Where a business without an established relationship is using consumer data benignly for a purpose the consumer may anticipate, such as a new local business marketing to all residents in a neighborhood, the consumer should have the ability to opt out of that use. This is consistent with the GDPR right to opt out of direct marketing and balances consumer and business interests.

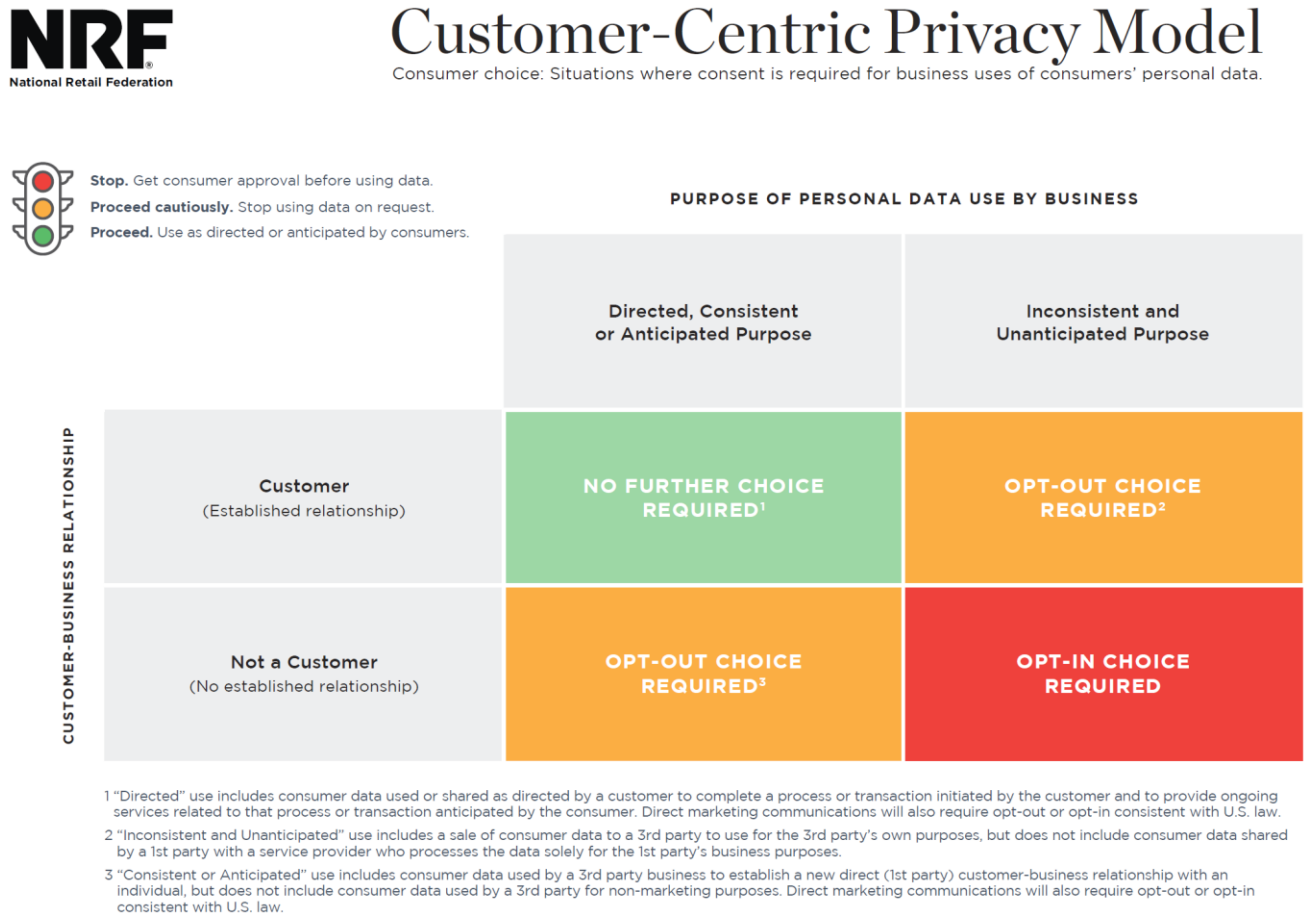
However, consumers are at the greatest risk of potential harm when they both lack an established business relationship with an organization and that entity is using their data for purposes that consumers do not anticipate. We have evidence from well-known scenarios like Cambridge Analytica's use of unsuspecting Facebook users' data in ways these consumers could never imagine. Consumers find these practices to be the most inherently objectionable and the model we propose would prohibit any use of data by an unknown party to the consumer for an unknown purpose unless and until there has been informed consent – a voluntary opt-in choice following full disclosure of the data practices to the consumer. At the moment the consumer makes that informed choice, the business and its purpose for collecting and using the data become known, and the risk to the consumer substantially abates as the consumer becomes a customer by exercising that choice. Until that affirmative consent is provided, however, the business practice is prohibited.

Affirmative consent, obtained by the third party, should be the default, however, when third parties unknown to the consumer use their data in ways that are unrelated to the original purposes of collection or are otherwise inconsistent with consumer expectations. These uses are inherently of higher risk because third parties lack the powerful market incentives to ensure close alignment with consumer expectations and are not bound to a need to protect a direct relationship with the consumer. For example, the use of personal data by third parties, as controllers, to develop behavioral profiles for sale should be restricted by default.

The focus of any proposed federal regulations should be on defining reasonable, workable standards for when data uses require consumer consent after full disclosure to consumers so they can make informed choices. Likewise, regulations should not restrict consumer choices or require

businesses to interpose interfaces that frustrate customers by requiring disclosures and consent requests in every interaction with them, such as requiring customers to click through a "consent wall" for these low-risk, permissible purposes consistent with consumer expectations. The regulations should permit such uses to preserve simplicity, clarity, and seamless customer experiences.

The following diagram illustrates the customer-centric and risk-based approach that should shape and form the basis for federal legislation or regulations on data privacy.[7] The grid's rows indicate the relationship between the consumer and business using personal data; the grid's columns divide over whether the purpose of the data use is directed, consistent or anticipated by the consumer. The quadrants highlight the area of highest risk to the consumer in red, and the least risk in green. Uses of consumer data that give rise to disclosures and opt-out choice obligations are in amber. First-party uses of consumer data by businesses with an established relationship that are directed by the consumer or have purposes that are consistent with or align with consumer expectations fall in the green quadrant.



[7] The diagram reveals the level of risk to consumers based on the nature of the customer-business relationship and the purposes for which businesses use personal data. The level of risk should determine the type of consumer choice required for business use of consumers' personal data. The diagram does not address common exceptions such as with respect to public records data, sensitive personal data, law enforcement use, or uses required by law. Additionally, service providers are considered to have the same customer relationship as the type of business they serve; for example, if they serve a retail business with an established customer relationship, the applicable level of risk would be in the top row of quadrants and the purpose for the use would be the same as the retailer's purpose.

Regulations that target low-risk, consumer-friendly uses that fall within the green zone in the chart should not be the focus of new federal privacy regulations. NRF believes the efforts of the Commission should instead be directed, at a minimum, at the highest-risk uses of consumer data that fall within the box highlighted in red. This approach will align inherently with consumer expectations, protect the rights of consumers to make informed choices concerning their data, and preserve the ability of retailers to innovate in the areas of product design, promotion, and sales.

NRF is concerned with any proposal to enact new federal regulations that apply to the retail industry but excludes other industry sectors. Such a proposal would be particularly inappropriate where the industries that are excluded are the ones engaged in higher risk forms of consumer data processing. Consumers should expect their personal data to be uniformly protected by every business that handles it. Laws and regulations therefore should not have any loopholes permitting some businesses to provide fewer or no protections than other businesses that are handling the same personal data of the same consumer.

D. COMMENTS SPECIFIC TO ANPR QUESTIONS

In this section, we provide additional views to the Commission to augment our comments above in response to certain specific questions the Commission has enumerated in the ANPR:

ANPR Question 7: How should the Commission identify and evaluate these commercial surveillance harms or potential harms? On which evidence or measures should the Commission rely to substantiate claims of harm or risk of harm?

NRF Comment:

The processing of personal data by retailers does not give rise to the types of harms at issue in the ANPR as explained in further detail below. NRF believes, however, that the Commission should identify and evaluate potential commercial surveillance harms by other businesses based on the level of risk to, and the impact on, consumers from particular types of uses and processing of personal data.

We have presented in Part C above a Customer-Centric Privacy Model for identifying and evaluating the risk of potential harm to consumers from business uses of data by examining the type of relationship a business has with a consumer and the purposes for which the business is using the data. The model clearly does not anticipate that the risk of harm rises to the level of "commercial surveillance" for any purpose that is directed by the consumer or consistent with a consumer's expectations, all of which would fall into the first column on our diagram of a directed, consistent or anticipated purpose. However, there may be some purposes that are inconsistent and unanticipated by consumers and used by non-retail businesses that lack a direct relationship with that person where risk of a potential commercial surveillance harm may exist.

In the following paragraphs, we provide further suggestions on how the Commission may make use of our proposed Customer-Centric Privacy Model and apply this conceptual framework to identify and evaluate the level of risk of potential harms to consumers from business use of data.

Directed, Consistent or Anticipated Purposes for Using Data to Serve Consumers

The lawful use of personal data by retailers in first-party contexts is not a high-risk activity and does not result in consumer harms. Retailers use consumer data for the principal purpose of serving their customers as they wish to be served. Retailers use customer data responsibly to do a better job of selling their products to their customers – to improve their offerings and do what retailers typically do *better*. This differentiates retailers from data brokers and other third parties unknown to the consumer that do not have direct relationships with individual customers.

Retailers engage in advertising by necessity. In fact, advertising is one of the primary methods by which retailers communicate with their customers. Customers want to see ads that make them aware of relevant offerings by retailers, and targeted ads directed to customers based on their past shopping experiences are an effective method of communicating product offerings of the greatest potential interest to the consumer. In all of these activities, retailers must and do use data responsibly and securely in order to maintain the trust of their customers.

Retailers' lawful advertising and marketing practices to existing and prospective customers, including the related delivery of promotional information such as product coupons, rebates and discounts, whether by physical or digital means, are legitimate business practices that have long been understood and anticipated by American consumers. These practices by retailers, among similar practices across other industry sectors that directly serve customers, would fall within the first column on our diagram labeled directed, consistent or anticipated purposes.

It is also important to recognize that retailers' advertising practices are already subject to the Commission's advertising regulations and the range of retailers' customer-serving marketing and communications are permissible acts or practices so long as they are not unfair or deceptive according to Section 5 of the FTC Act. When such advertising, including online behavioral ads, are directed to customers by businesses with whom they have a relationship, the Commission has found in its past staff reports that these practices present far less risk of harm to consumers than practices of third parties with whom they have no relationship.

In 2009, the Federal Trade Commission explained in its staff report on online behavioral advertising the distinct differences they found between first-party and third-party uses of data, particularly regarding consumers' reasonable expectations, their understanding of why they may receive certain advertising, and their ability to register concerns with, or avoid, the practice, as follows:

> For example, under the "first party" model, a consumer visiting an online retailer's website may receive a recommendation for a product based upon the consumer's prior purchases or browsing activities at that site (e.g., "based on your interest in travel, you might enjoy the following books"). In such case, the tracking of the consumer's online activities in order to deliver a recommendation or advertisement tailored to the consumer's inferred interests involves a single website where the consumer has previously purchased or looked at items. Staff believes that, given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the

> practice altogether by taking his business elsewhere. By contrast, when behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice.[8]

This focus on advertising to existing customers should not be construed to suggest that advertising in the retail context to consumers who are not existing customers should be considered harmful or present a risk of a commercial surveillance harm. To the contrary, lawful advertising is part of the fabric of the American economy and customer experience that dates back to our founding as a country. Our free market economy and capitalist system has long endorsed advertising as a legitimate practice for companies to make their products and services known to prospective customers in order to drive future sales.

Further, when there is a direct communication to a prospective customer, such as commercial email that is unsolicited, or where a telemarketing call is placed to a consumer's landline outside of an existing business relationship, there are well-established precedents under acts enforced by the FTC for these practices to require the provision of an opt-out to the prospective customer and retailers comply with these laws. Likewise, online behavioral advertising is subject to a self-regulatory program that requires providing consumers with the ability to opt-out of such advertising, and retailers participate in this program as well. All of these statutory and self-regulatory requirements are consistent with the lower-left quadrant in our proposed model.

Lawful advertising and marketing practices by legitimate retailers, whether mass advertising or targeted as described above, does not cause harm to consumers – and certainly not the types of harm described by the Commission, such as "targeting . . . fraudulent products and services to . . . vulnerable consumers."[9]

Inconsistent and Unanticipated Purposes for Using Personal Data

When it comes to the risk of harm from personal data used for purposes that are inconsistent with a consumers' experience or unanticipated in light of the relationship they have with the business using such data, our model suggests evaluating the customer relationship to determine the level of risk presented to the consumer from that activity and assigning the appropriate level of choice required to be provided for that use case.

The greatest risk of a commercial surveillance harm to a consumer would arise in the lower-right quadrant of our model, colored red, where an entity without a direct relationship to the data subject is using data for a purpose that is not consistent or anticipated by the reasonable consumer. We do not suggest by this conceptual model that *all* activity within this quadrant presents a commercial surveillance harm, but only that *potential* commercial surveillance harms could exist as a subset of some of the activity covered by this red-colored quadrant.

---

[8] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), pp. 26-27, available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

[9] Trade Regulation Rule, 87 Fed. Reg. at 51275.

For example, this red quadrant would be where the practices of an unscrupulous data broker or other third party, such as practices similar to those engaged in by Cambridge Analytica, may fall when assessing the lack of a direct relationship to the consumer and the inconsistent or unanticipated purposes for which the data is being used. These activities could include the risk of potential commercial surveillance harm as that phrase is defined by the Commission.

It is therefore the practices within this red quadrant of activity – data used for inconsistent or unanticipated purposes by businesses lacking a direct customer relationship with the data subject – where we believe the Commission should limit its focus on identifying and evaluating the risk of commercial surveillance harms to determine whether proposed regulations are warranted.

Conclusions and Commercial Surveillance

NRF believes that uses of consumer data by retailers in ways that are directed or anticipated by consumers, or consistent with consumer expectations, do not constitute commercial surveillance in the first instance. Rather, we submit that commercial surveillance should refer to the persistent tracking of consumers' activities across mobile apps, websites, or devices over time by third parties without direct relationships with consumers, and without consumer awareness. This type of collection and use of consumer data is not directed or anticipated by consumers, or performed consistent with their expectations, and it gives rise to a greater likelihood of negative impacts and harms.

Additionally, we would submit as support for these conclusions that the practices of retailers would not fall within the ambit of "commercial surveillance" as that phrase has been commonly understood since it first came into use. For example, in *The Age of Surveillance*, authored by Dr. Shoshana Zuboff, the professor who coined the phrase, she cautions at the outset that distinctions must be made between what she considers capitalism as compared to *surveillance* capitalism:

> First, it is necessary to distinguish between capitalism and surveillance capitalism. As I discuss in more detail in Chapter 3, that line is defined in part by the purposes and methods of data collection. When a firm collects behavioral data with permission and solely as a means to product or service improvement, it is committing capitalism but not surveillance capitalism.[10]

Dr. Zuboff goes on to explain immediately after this passage that the retail activities of some of the top five tech companies, such as Apple and Amazon, are ones that "derive revenues from physical and digital products and therefore experience less financial pressure to chase surveillance revenues than pure data companies."

In examining Dr. Zuboff's distinctions alongside the Commission's ANPR, it is important to recognize that the retail practice of selling products to consumers for a price is the principal means of revenue within the retail industry, and the purposes for which customer data is used to improve that service and the methods of data collection are not commercial surveillance.

In conclusion, we believe that a subset of the data uses captured by the lower-right red quadrant in our model is where practices such as commercial surveillance may fall, but not all practices

[10] Shoshana Zuboff, *The Age of Surveillance* 22 (2019).

that are captured by that quadrant will rise to the level constituting surveillance. It is here where the Commission should focus its examination of commercial practices to evaluate the practices that it considers to potentially rise to the level of commercial surveillance harms.

***ANPR Question 11*: Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and business models more likely to protect consumers than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?**

***NRF Comment*:**

Retailers are subject to powerful market incentives to protect consumers and consumer data. If retailers are not good stewards of their customers' data and do not use data in ways that their customers and the broader market anticipate, then they will incur significant brand damage and lose consumer trust. In a highly competitive industry like retail, loss of consumer trust can have a devastating impact. The retail business model therefore inherently protects consumers from potential harm, including lower-level potential harms that do not rise to the level of commercial surveillance harm.

Data brokers and other third parties that lack direct relationships with consumers, however, do not operate under the same level of incentives as retailers to protect consumers and consumer data. Instead, the market incentivizes these businesses to maximize collection of personal data, to build more robust consumer profiles, to develop more precise insights about consumers, and to monetize and sell the results to other businesses. These third parties are subject to incentives to follow reasonable security and privacy practices, of course – such as the desire to comply with law, to reduce the risk of litigation, and to avoid adverse publicity. But we submit this is a significantly higher risk environment than presented by retailers that enjoy and rely upon direct relationships with consumers.

***ANPR Question 35*: 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? Should the Commission take into account other governments' requirements as to data security (e.g., GDPR)? If so, how?**

***NRF Comment*:**

Sector-specific regulations that may be appropriate for specific data practices within an industry sector are not necessarily appropriate for application to businesses outside that sector, such as retailers. NRF supports the use of a standard based on reasonableness for the protection of the security of personal data. There is no "one-size-fits-all" regulation or standard for data security as it depends on the particular risk of misuse, misappropriation or theft for a given data set. Data security practices must therefore be flexible and adaptable to differing levels of security protection based on the nature and use of the data and an entity's current practices.

Further, while the Commission is well meaning it is unfortunately not well-positioned to keep abreast of rapidly-evolving security best practices within industry and across its various

sectors because it lacks the direct experience of monitoring, mitigating and preventing evolving cyber threats to industry that proliferate on a daily basis. For these reasons, businesses should have the operational flexibility to rapidly identify and implement security measures that are reasonably designed to provide a level of security appropriate to the level and type of risk they face at any moment.

Data security requirements, where they exist in law or regulations, should provide such flexibility for businesses to adapt based on changes in corresponding cybersecurity vulnerabilities and threats. Businesses should also have the ability to identify and align with one or more recognized industry standards that are reasonable to the nature of their operations and their industry as their applicability may change over time. Retailers already apply applicable standards, where appropriate as dictated by the context, to protect consumer data.

Rules from the Commission laying out cybersecurity requirements also may interfere or conflict with the goals of other federal agencies, and the advances that members of the retail industry sector have made building public-private relationships. For example, there are forthcoming presidential guidelines on cybersecurity, Securities and Exchange Commission (SEC) rules relating to cybersecurity, and a highly active Cybersecurity & Infrastructure Security Agency (CISA), which is increasingly integrated with businesses. The goals of these agencies and their efforts are potentially put at risk by newly proposed regulations that could be used to bring actions and/or levy fines against businesses victimized by a data security incident, particularly while these agencies are seeking stronger relationships with industry to help prevent or mitigate the impact on industry of such cyberattacks. In fact, the Department of Justice has issued several white papers that lay out areas where they will not charge, and where they seek cooperation with businesses that have been the victims of cyberattacks.[11]

If the Commission determines that it will pursue a proposed regulation related to the provision of reasonable data security practices, it should also adopt a notice-and-cure mechanism for alleged deficiencies in data security practices so that businesses have the opportunity to remediate any elements in their programs that the Commission finds insufficient to meet the reasonableness standard before enforcement actions may be brought in the first instance of an alleged violation.

This important enforcement tool has been used effectively in state privacy legislation and addresses the concern that subjective standards such as those based on reasonableness may fairly have a range of interpretations. The notice-and-cure mechanism therefore encourages government agency-to-business communications and would provide effective incentives for businesses to modify their data security practices as needed to come into compliance within a reasonable period of time upon notice from the Commission of any potential deficiencies in such practices.

---

[11] *See, e.g.*, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*, Department of Justice and Department of Homeland Security, October 2020.

***ANPR Question 39*: To what extent, if at all, should the Commission limit companies that provide any specifically enumerated services (e.g., finance, healthcare, search, or social media) from owning or operating a business that engages in any specific commercial surveillance practices like personalized or targeted advertising? If so, how? What would the relative costs and benefits of such a rule be, given that consumers generally pay zero dollars for services that are financed through advertising?**

***NRF Comment*:**

Question 39 presumes that personalized and targeted advertising constitute commercial surveillance. We respectfully suggest, based on our analysis in response to Question 7, that personalized or targeted advertising by retailers to current or prospective customers is not commercial surveillance.

NRF believes that any rule limiting companies that provide certain types of services from owning or operating a business that engages in personalized or targeted advertising would unnecessarily restrict retailers and other customer-serving businesses from engaging in commercial speech protected by the First Amendment and lawfully communicating with customers and prospective customers. Advertising is one of the primary methods by which retailers inform consumers about product offerings in which they may be interested. Rather than adopting a punitive rule that requires the divestiture of entire business lines, NRF would encourage the Commission to adopt a risk-based approach aligned with the Customer-Centric Privacy Model proposed in Part C above as further explained in response to Question 7.

A Divestiture Rule Would Have a Material Adverse Impact on the Ability of Retailers to Advertise to Consumers

NRF is concerned with the significant impact a divestiture rule would have on the retail industry. If, for example, the Commission promulgated a rule limiting companies engaged in retail operations from "owning or operating a business that engages in . . . personalized or targeted advertising," then it would arguably become illegal for retailers to conduct personalized advertising operations. We would hope this is not the intent of the Commission, yet it is a conceivable unintended consequence of any such rule.

A rule more narrowly tailored to healthcare, financial services, or other specified businesses would create a similar risk. Some retailers own pharmacies or provide other healthcare services; others may offer private-label credit cards and other financial products. These businesses should not be prohibited from engaging in personalized advertising to consumers. In addition, the specific personal data these retailers process in providing these services may be subject to sector-specific laws that regulate marketing, advertising, and affiliate sharing such as HIPAA,[12] the Gramm-Leach-Bliley Act,[13] and the Fair Credit Reporting Act.[14] State

[12] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.
[13] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338.
[14] Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1128.

medical privacy standards may also apply, such as the California Confidentiality of Medical Information Act.[15]

The movement of the retail industry into digital commerce also means that retailers offer search functions (e.g., search bars within mobile apps and eCommerce sites) and may offer social media-related features associated with customer reviews. These features enable customers to shop more efficiently and with greater information, and thus significantly benefit them. Yet these features that have consumer benefits would be imperiled by a rule that requires divestiture of operations offering search or social media functionality to consumers on retail websites or mobile apps.

A Customer-Centric, Risk-Based Approach to Federal Privacy Regulation Would Protect Consumers while Avoiding Unnecessary Adverse Impacts on Businesses and Technological Innovation

A divestiture rule would impact businesses in all four quadrants of the Customer-Centric Privacy Model shown in Part C above equally, rather than focusing new rules on the areas of greatest risk to consumers. The Customer-Centric Privacy Model provides a less intrusive approach that will preserve the ability of businesses to serve customers as they expect and enable consumers to make informed choices concerning their data. It also preserves the ability of retailers to innovate in the areas of product design, promotion, and sales.

Retailers' lawful advertising and marketing practices to existing and prospective customers, including the related delivery of promotional information such as product coupons, rebates and discounts, whether by physical or digital means, are legitimate business practices that have long been understood and anticipated by American consumers. These practices by retailers, among similar practices across other industry sectors that directly serve customers, would fall within the first column on our diagram labeled directed, consistent or anticipated purposes.

E. CONCLUSION

NRF submits that the practices the FTC equates with the moniker "commercial surveillance" are quite distinct in principle and practice from the purposes for which retailers collect and use personal data. In a highly competitive industry like retail, where retailers must consistently earn and maintain the trust of their customers to stay in business, those retailers engaging in any data privacy practices that undermine customer trust – including lawful ones that fall far short of being commercial surveillance practices – run the risk of going out of business, a penalty far more severe than any regulation. In short, robust competition in the retail industry creates a significant, inherent market incentive to ensure careful and limited collection, use, and handling of personal data. The retail industry is distinct in this regard from other industries that lack robust competition, like social media, or lack the direct customer connection, such as third-party data brokers.

The Commission therefore should be careful not to draft new data privacy regulations so broadly as to extend beyond the surveillance capitalism economy to also cover millions of Main

[15] Cal. Civ. Code §§ 56 to 56.37.

Street retailers – businesses that are already directly accountable to consumers for their use and handling of personal data and are already subject to every state's comprehensive data privacy laws. Instead, the Commission should focus its inquiry on the entities likely unknown to most consumers and which have practices that place consumers at the greatest risk of harm, including practices that may truly be defined as commercial surveillance. We find these risks to be greater in industry sectors where competition is weak and market constraints and consequences for consumer data use are limited.

We have proposed in Part C above a conceptual data privacy framework – the Customer-Centric Privacy Model. The Commission can use this model as a four-quadrant decision matrix for assessing the risk of harm, from the viewpoint of consumers, of a range of data uses and for determining the appropriateness of future proposed regulations requiring a level of consent that is calibrated to the level of benefit and risk faced by consumers in a given situation. The 2 x 2 quadrant model poses two questions for the FTC to ask of *every* consumer data use case: 1) has the data user established or intended to establish a customer-business relationship (i.e., is the data subject an existing or prospective customer); and 2) are the purposes for using the consumer data directed by a consumer or are they consistent with a customer experience or anticipated by the reasonable consumer? Using this model, the Commission can ask these questions of data use cases to determine whether there is a sufficient risk of harm that outweighs the benefits of the data use to the consumer.

We appreciate the Commission's consideration of this customer-centric and risk-based approach in determining the necessity and scope of regulations to address commercial surveillance practices. Based on our comments above, we respectfully submit that the consumer data practices engaged in by retailers to better serve their customers (i.e., including marketing communications and advertising of sales promotions that are intrinsic to the American shopping experience) are not only consistent with customer experiences and anticipated by consumers, but are directed and appreciated by them as well. Similarly, these practices fall well outside the scope of any commercial surveillance practices that are potentially harmful to consumers and should therefore not be included in any future proposed regulation the Commission develops to address such practices.