



March 11, 2019

The Honorable Lindsey Graham
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Diane Feinstein
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

RE: Full Committee Hearing on “GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation”

Dear Chairman Graham and Ranking Member Feinstein:

The National Retail Federation (NRF) appreciates your leadership in holding tomorrow’s first Senate Judiciary Committee hearing of the 116th Congress on consumer data privacy issues, including an examination of the General Data Protection Regulation (GDPR), which was adopted by the European Union (EU) in 2016 and took effect in 2018, and the California Consumer Privacy Act (CCPA), which was enacted last summer and will take effect in 2020.

NRF is the world’s largest retail trade association. Based in Washington, D.C., NRF represents 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 — 42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation’s economy.

Over the past several decades, NRF has worked closely with its member companies on data privacy statutes and regulations here and abroad. Below we share some principles for U.S. federal privacy legislation based on the lessons learned from our work over the past three years on the GDPR and over the past nine months on the CCPA, including our comments filed with the California Office of the Attorney General last week (a copy of which is attached for your review).

We view our recent engagements in the GDPR and CCPA as part of a continuum of activity to help the retail industry develop best practices on data privacy and security matters since the late 1990s. Since that time, we have worked with members of this Committee and other Congressional committees on data privacy and data security legislation, and we look forward to continuing our important collaboration with you and other interested members of Congress to help develop federal privacy legislation that the retail industry could support.

More than ever, preserving U.S. national interests in technology and innovation requires establishment of a federal data privacy framework that operates with the same global reach as the GDPR but improves upon the EU’s approach to data protection for American consumers and

businesses alike. With a *federal* privacy law, Congress can establish an American policy on data protection that could be exported by the U.S. federal government to protect our national interests abroad. This is not possible today, where a balkanized set of state privacy laws forms a *de facto* U.S. “policy” on data regulation – an incoherent approach based on a patchwork quilt of competing and potentially conflicting state regulations dominated by the law of just one state, California.

With this perspective in mind, we provide below our views on: retailers’ interests in using consumer data to better serve their customers, which contrasts with other parties’ uses of such data; NRF’s principles for federal privacy legislation; and lessons learned from the GDPR and CCPA that support our principles and the approach we recommend Congress adopt in a new U.S. privacy law.

Retailers’ Use of Customer Data and Interests in Protecting Consumer Privacy

Protecting consumer privacy 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 win 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 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 appropriate methods to comply with state, federal and global data protection regulations in ways that further their customer relationships and does 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 to achieving the goal of improved customer service. This differentiates retailers’ principal use of customer data from businesses – including service providers, data brokers and other third parties unknown to the consumer – whose principal business is to monetize consumer data by collecting, processing and selling it to other parties as a business-to-business service. Such data practices are the profit center of the “Big Data” industries whose products are the consumers themselves (and not goods sold to consumers). **As members of the Committee consider federal privacy legislation, it is important to recognize the fundamental differences in consumer data usage between two categories of businesses:**

- **“first-party” businesses**, which sell goods or services directly to consumers and use their data to facilitate sales, provide personalization, recommendations and customer service; and
- **“third-party” businesses**, which process and traffic in consumers’ personal data, very often without consumers’ knowledge of who is handling their personal data and for what purpose.

Federal Trade Commission Views on First-Party vs. Third-Party Data Uses

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 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.¹

Consumer Concerns with Significant Privacy Violations by Third-Party Businesses

Over the past eighteen months, tens of millions of Americans learned of the significant risks of harm they personally face from irresponsible data practices by third-party businesses who are unknown to them. Members of the Committee need to look no further than the recent newspaper headlines with breaking news – often on the front pages of their local newspaper or the nationwide newspapers – to know which privacy violations Americans care most about:

- **AT&T selling their mobile phone subscribers’ precise GPS location data, without sufficient notice or consent, to data brokers, who in turn sold the precise location data to “bounty hunters”** that used it to surveil mobile locations of individuals – not just once, but tens of thousands of times;
- **Cambridge Analytica using data collected on 87 million Facebook users to conduct psychographic analyses of them based on their Facebook content and selling their findings to political clients, without the consent of 99.6% of them** (*i.e.*, while 270,000 Facebook users had consented to data collection for academic use only, they were not told their consent would provide access to data on all of the other individuals in their social network who never consented); and
- **Equifax mishandling its data breach affecting over 145 million Americans, most of whom had never heard of Equifax or knew that the credit bureau held their most sensitive personal data** before its unauthorized disclosure in a breach incident.

¹ *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>

In the three examples above, third-party data brokers, processors and service providers violated the privacy of American consumers who cared deeply about these incidents. This is why it is highly objectionable that leading state privacy laws, such the CCPA, and Washington state's privacy legislation, are being crafted on the inaccurate presumption that consumers' interest in data privacy stops at the front door of a consumer-facing business. These laws fail to recognize that consumers are equally or even more concerned with what third parties do with their sensitive information behind the scenes. We do not believe legislators voting for these state privacy bills are aware of the serious deficiencies in them, and that businesses mistrusted by consumers for recent privacy violations qualify as service providers, processors or third parties exempt from any privacy obligations (or even requirements to notify consumers of their own breaches) under the bills that state lawmakers sponsor and vote to enact. We urge this Committee to examine these flaws in state privacy laws and improve upon them by holding accountable all entities handling consumer data.

Principles for Federal Data Privacy Legislation

NRF began working with our retail company members on best practices to protect customer privacy in the late 1990s, with initial efforts focused on developing principles that promoted transparency and customer choice. Over the two decades since, NRF has participated in efforts by several Congressional committees in the House and Senate to develop federal data privacy legislation. This past fall, NRF submitted comments to the National Telecommunications and Information Administration (NTIA) on high-level goals for federal legislation (a copy of which is available [here](#)). Over the years, we have also submitted comments to the Federal Trade Commission (FTC) on a range of data protection issues as the FTC explored the contours of the Commission's authority, under Section 5 of the FTC Act, to protect consumers' data privacy and ensure that businesses handling consumer data employed reasonable data security practices.

American businesses today, however, cannot solely concentrate on federal and state data privacy regulations. Conceivably, a data regulation adopted halfway around the world may impact a U.S. business operating entirely within our national borders and employing only American workers. Retailers are not immune to the significant challenges described by global tech companies to reconcile newly adopted and conflicting data privacy laws – from the EU's GDPR to California's CCPA. Retailers are also acutely aware of the potential for 50 different U.S. states and an unpredictable number of foreign governments to propose new data regulations each year that have a global reach (like the nature of the data itself that each law intends to regulate).

These proposed regulations, even if well-meaning, may ultimately make it impossible for businesses to use data as they would like to serve their customers in the many ways consumers have come to expect, largely because of the risks companies could face in the form of significant government fines or business litigation if they misjudge how best to use data responsibly to serve their customers. In the end, it may be consumers who stand to lose the most if businesses cease to take advantage of technological innovations to better serve them out of fear of tripping over a hodge-podge of potentially conflicting state, national and multi-national regulations that include very high fines for any non-compliance without even the ability to cure minor violations.

Retailers would like to avert a global data regulation train wreck, and we support a U.S. federal solution to data privacy that would apply nationwide requirements uniformly across all industry sectors handling similar customer information. As the Committee reviews legislative

proposals, we would urge you to adopt several key principles that we believe are essential to federal legislation in this area of the law:

- **Nationwide Data Privacy Regulation:** Congress should create a sensible, uniform and federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that all sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting related state laws is necessary to achieve this important, national public policy goal. Without effective preemption of state law, Congress would simply add another data privacy regulation to what may eventually become a 50-state regulatory regime. Such an outcome would fail to address the problem that the U.S. state privacy laws today operate within a global data regulatory regime for businesses where state laws, foreign national laws, and multi-national regional regulations like the GDPR all potentially conflict. Congress's effort, therefore, to bring sensibility and certainty to U.S. data privacy regulation is as important to the future of e-commerce for American businesses now as maritime law was to facilitating trans-oceanic commerce centuries ago.
- **Comprehensive Application of Equivalent Privacy Regulations to All Entities:** Federal data privacy legislation should apply to all industry sectors that handle the same or similar consumer data, and Congress should not craft rules that are specific to any subset of industry or permit exemptions that pick winners and losers among competitive industry sectors. Some industry sectors cite their compliance with federal laws from last century as the basis for exemptions from any new privacy law, while simultaneously opposing amendments to their outdated federal laws that would bring them up to present-day standards for consumer privacy protection. To protect consumers comprehensively, however, a federal data privacy law must apply equivalent requirements to all industry sectors handling similar sensitive personal information.
- **Transparency and Consumer Choice:** Federal legislation should promote well-understood fair information practice principles, such as transparency and consumer choice, with respect to sensitive customer data. Businesses handling such data should be transparent about their collection and use of sensitive data and should provide consumers with meaningful choices in how such data is used. Retailers support principles like the GDPR's "legitimate interest" concept as a lawful basis for processing sensitive customer data, which properly aligns consumer expectations with business needs by balancing a business's legitimate interest in processing personal information to serve its customers with the customer's interest in protecting her data from misuse. The legitimate interest basis provides the regulatory flexibility necessary to ensure that businesses can use consumer data responsibly in ways that avoid frustrating the customer experience with incessant requests for affirmative consent where it is unnecessary for lawful processing.

We have come to these conclusions on which principles are critical to a U.S. federal data privacy law through our continuous work with member companies on both the GDPR and CCPA. There are certainly lessons to be learned from each of these laws: some areas of enlightened thinking that Congress should support in its own legislation, such as the GDPR's legitimate interest basis for processing customer data, as well as areas of concern – the CCPA's non-discrimination clause, for instance – that we would urge Congress to avoid duplicating as it crafts alternative

provisions to achieve the public policy ends of a federal data privacy law. We address several aspects of the GDPR and CCPA below to inform members of retailers' views on each law as the Committee considers the testimony of other stakeholders offered at today's hearing.

Lessons Learned from the GDPR

With the GDPR taking full effect less than one year ago, there are still many questions that remain about how the regulation applies to critical areas of retail business operations, such as: using customer data for improved service or promotional opportunities, managing customer information databases and loyalty programs, collecting customer consents, and honoring customer rights to erase data, port data to another business, or access their personal data held by a business.

A business does not have to be a large multi-national company to feel the regulatory impact of the GDPR. Retailers operating in the U.S. with websites, mobile apps and other digital platforms serving consumers may face new compliance standards, increased liability for violations and more stringent enforcement. While the GDPR is aimed primarily at EU-based businesses, it also applies to companies headquartered anywhere in the world that have stores in Europe or simply target sales to Europeans through the Internet, mobile apps or other remote commerce channels. The GDPR therefore has significant implications for many U.S. retailers.

Following adoption of the GDPR nearly three years ago, NRF engaged our retail company members and those of a counterpart EU-based retail trade association, EuroCommerce, in a multi-year transatlantic effort to develop the first common global retail approach to compliance with the GDPR. This collaborative work within the U.S. and European retail sectors culminated in the *GDPR Discussion Document for the Global Retail Industry* (a copy of which is attached for your review). NRF and EuroCommerce [released](#) this discussion document last year and shared it with the data protection authorities (DPAs) in each of the current twenty-eight member nations of the EU, as well as with key EU officials in Brussels.

Although our principal purpose in developing the attached GDPR paper was to provide the basis for an on-going dialogue between the global retail industry and relevant stakeholders that would facilitate retail-specific approaches to GDPR compliance and enforcement, we believe this document has considerable importance for members of the Committee as you examine lessons learned from the GDPR. In developing their compliance programs to meet the GDPR's requirements, retailers have discovered several elements of the GDPR that raise shared concerns. The GDPR discussion document takes great strides to illuminate specific areas where retailers' efforts to meet consumer expectations may be frustrated by the GDPR's approach to data regulation if DPAs' interpretations of the GDPR's provisions in the retail context are not carefully drawn.

The discussion document identified six critical areas of the GDPR that are highly relevant to the Committee's examination, specifically: data erasure; data portability; the validity of prior consents; other legal bases for processing data, like legitimate interest; data breach notification; and automated decision-making, including profiling. We have found that well-meaning requirements in certain of these GDPR provisions may not align with existing consumer expectations, and we have tried to develop a retail approach to GDPR compliance to help minimize its unintended effects. We invite you to review this document and its discussion of areas where the intended purpose of the GDPR meets up with the reality of trying to practically implement a comprehensive global data

privacy regulation in a way that will not upset customers' expectations with how they like to shop and receive personalized service from their favorite retailers.

Lessons Learned from the CCPA

In California, retailers face similar issues with the State's enacted data privacy law, but their concerns have been compounded by the fact that California spent little more than a legislative week trying to accomplish what took the EU nearly a decade to achieve with the GDPR. The under-whelming results and drafting errors throughout the law are glaringly obvious, and businesses across industry sectors are facing a regulatory regime that, if it takes effect as currently drafted, may create greater costs for California consumers than benefits.

One of the most significant concerns we raised with the authors of the CCPA is that the law's non-discrimination clause² could lead to the decline of customer loyalty programs (e.g., "club" discount cards, free merchandise, rewards, coupons, advanced release programs, exclusive experiences, etc.) offered by retailers and other businesses to California residents. According to a 2017 study published by Forrester Research, 72% of American adults online belong to at least one loyalty program, and the average number of loyalty program memberships that each adult has is nine.³ The CCPA puts extraordinary pressure on these customer-favored programs by creating significant liability for businesses that provide rewards or other benefits, such as preferred service or pricing, to customers who want them.

Under the CCPA, businesses offering preferred service or pricing through loyalty programs to their customers who wish to participate in them – when other customers exercising privacy rights do not or cannot participate in them – may only continue to do so, without violating the non-discrimination rules, if the "value" of the personal information to the consumer that is used by the business is met by an equivalent value in discounts or benefits received by the consumer. This is a novel and untested legal equation fraught with such ambiguity and uncertain outcomes that it invites virtually an infinite array of "economic" opinions on the value of personal information for California state courts to weigh in potentially protracted, class action litigation.

The value of personal information that may be "priceless" in one consumer's eyes would never equate subjectively to a reasonable discount on a product. The potential for litigation over this most basic of retail practices could lead some stores to shut down loyalty programs altogether – or not make them available to Californians – because the CCPA creates an untenable business litigation risk. These stores reasonably could determine that the potential costs of lawsuits testing the meaning of the non-discrimination section of the CCPA outweigh the potential benefits to the business from providing better service and discounts to their most loyal customers.

The CCPA raises other significant concerns that retailers will continue to address within the California legislature this year before the law is expected to take effect in 2020. For example, at the 11th hour, on the final day of the California legislature's 2018 session, the CCPA was amended by "clean-up" legislation to clarify the language of the bill. However, several of the so-called

² Cal. Civ. Code § 198.125(a) ("A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by...charging different prices or rates for goods or services, including through the use of discounts or other benefits...")

³ Forrester Research, *How Consumers Really Feel about Loyalty Programs*, May 8, 2017.


“improvements” were refinements to the exemptions in the bill that permit businesses with highly sensitive customer information to avoid the data privacy requirements that must be borne by other businesses handling the same or even less sensitive information. In some cases, there is no corresponding federal law that would require the exempted sector from providing equivalent consumer data privacy protections. The CCPA’s disparate treatment of businesses handling sensitive consumer data is one reason why Congress should move forward with comprehensive federal legislation to establish a *uniform* set of requirements nationwide that applies evenly to all industry sectors handling similar sensitive personal information.

American consumers expect all businesses handling their sensitive information to do so responsibly, regardless of when and where that data is processed. By developing a data privacy law that does not pick regulatory winners and losers with the stroke of a pen before the stroke of midnight, as California has done, Congress can ensure that Americans’ privacy will be protected by federal law regardless of which business is collecting, transmitting, storing or otherwise processing their sensitive personal information.

We look forward to working with the Committee to help members understand the deep flaws in the California regulation that hold the potential of negatively impacting U.S. commerce and exasperating consumers in California and elsewhere who could lose their preferred loyalty programs and benefits that they have come to expect. Congress would do well to avoid making the quickly-considered and problematic CCPA the model for federal legislation.

As this Committee considers federal data privacy legislation going forward, we urge you to continue to examine the lessons learned from the GDPR and CCPA, and to avoid the flaws in these and other foreign and state data regulations while preserving the more enlightened elements of the GDPR that would advance the U.S. approach to data privacy protection. We look forward to working with you and members of the Committee on federal data privacy legislation that will provide a uniform and fair framework for consumers and businesses alike that respects and promotes consumer privacy across all industry sectors.

Sincerely,



David French
Senior Vice President
Government Relations

cc: The Honorable Mitch McConnell
The Honorable Charles E. Schumer
Members of the Senate Committee on
the Judiciary

Attachments