TESTIMONY OF

DOUG KANTOR

GENERAL COUNSEL, NATIONAL ASSOCIATION OF CONVENIENCE STORES

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

OF THE

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON ENERGY & COMMERCE

HEARING ON

"PROTECTING AMERICA'S CONSUMERS: BIPARTISAN LEGISLATION TO STRENGTHEN DATA PRIVACY AND SECURITY"

JUNE 14, 2022

Thank you for providing me with the opportunity to testify on data privacy and security.

I am testifying today on behalf of my association, the National Association of Convenience Stores (NACS), as well as a coalition that we helped found to try to address these issues, the Main Street Privacy Coalition (MSPC). NACS is an international trade association representing the interests of the convenience industry. In the United States, the industry includes more than 148,000 stores employing 2.3 million people. It is truly an industry of small business with a full 60 percent of the industry comprised of single-store operators. The industry handles about 165 million transactions each day – a number equivalent to about half of the U.S. population. The large volume of data exchanged through those transactions is just one aspect of the business that requires the use and exchange of data to facilitate commerce.

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.[1]

I. Executive Summary

NACS and the MSPC have long advocated for a uniform national privacy law. Having data privacy and security laws 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 law needs to work for Main Street. We appreciate our discussions with the Committee on these questions to date and hope that those discussions will continue as work is done to improve the draft legislation before the Committee.

Given the diverse and complex ways that data is used in our modern world, it helps to have principles to guide efforts to find effective ways to regulate in this area. We think adhering to the following seven principles can help achieve the best public policy results in this area.

- **Establish Uniform Nationwide Rules and Enforcement for Data Privacy**

- **Ensure Industry Neutrality and Equal Protection for Consumers Across Business Sectors**

[1] Information on the MSPC including a full list of its members can be found at https://mainstreetprivacy.com/about/.

- **Impose Direct Statutory Obligations (Rather than Contractual Requirements Alone) for All Entities that Handle Consumer Data**

- **Preserve Customer Rewards and Benefits**

- **Achieve Transparency and Customer Choice**

- **Ensure Accountability for Business's Own Actions**

- **Include Reasonable Data Security Requirements**

The American Data Privacy and Protection Act (ADPPA or the Act) represents an important milestone on the road to achieving a national data privacy standard that meets these principles. We see the intent in the Act to work toward each of the principles set forth above. We also see a number of areas in which additional work will be important to ensure that the Act fulfills the policy goals intended by its authors.

Among the most impactful areas in which we see the benefits of additional work on the bill include the need to cover all industry sectors and participants that interact with data covered by the Act. Currently, the Act creates a rule whereby financial services firms subject to a law that does not have privacy requirements that give consumers credible protection are deemed to be in compliance with the Act. There needs to be a plan to work with the House Financial Services and Senate Banking Committees to rectify that issue and cover financial services companies in the Act.

Additional work should also be done to ensure that the vast category of "service providers" that do the bulk of the work of collecting, processing, transmitting, storing, and transferring data in our modern economy are fully responsible for their role in such work and required to comply with every aspect of the Act as they are able. The Act has language in some areas to advance this goal, but also has language that creates uncertainty which can and should be addressed. More importantly, each of the privacy laws enacted in four States the past two years require service providers to be responsible for protecting consumers' data to a greater extent than this Act, and we urge the Committee to match or exceed those protections.

How any data privacy law handles the questions of whether and on what basis individuals may be able to bring lawsuits against businesses under the law, as well as whether and how a federal law preempts state laws, will be controversial at every stage of the legislative process – and for many years following the passage of any such law. Those two issues have long blocked progress on other aspects of privacy legislation. We appreciate that the work and dedication of the staff and Members of this Committee to put forward a bipartisan legislative draft is allowing all of us to focus on other issues. But, these two issues merit additional attention and we believe changes are in order to ensure that the Act creates a scheme that works for consumers and businesses – and follows the intended goals of the authors.

We also see ways for the language of the Act to be modified to ensure that consumers continue to get the benefits that they have come to expect from the business community and our economic system. These include access to loyalty discounts and rewards that Main Street businesses provide as well as competition on prices and product and service offerings that is enhanced by many forms of advertising that are broadly accepted by consumers.

In addition, there are a number of areas in which additional interpretive and substantive issues can be addressed through continued collaborative work on the Act. We appreciate the effort and dedication it took to get us to a hearing on a bipartisan draft of privacy legislation and the opportunity you have afforded us to be part of that process. We look forward to continued efforts to get us to our shared goal of a uniform law that works for American consumers and businesses alike.

II. Key Principles Essential to Privacy Legislation

The exchange of data is central to much of the world's commerce. Simply 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 writing legislation to cover privacy is so challenging.

Take just one simple example that illustrates the complexity of this topic. When a consumer walks into a convenience store to buy some bubble gum and uses a credit or debit card, simply to ensure that can happen the card data must go from the store's terminal over another company's data lines to a payment processor and/or the store's bank and then over more data lines (which may or may not be owned by the same company) to a payment card network (such as Visa or Mastercard) and then over more data lines to the bank that issued the consumer the credit or debit card . . . and then the entire process happens again in reverse. All of that happens in seconds (or fractions of a second) so that the consumer can walk out of the store with gum. Later, for most transactions, the data travels through a similar process to ensure that the funds are properly settled in the right account.

That is just one of the most common examples which happens millions of times each day all over the nation and must happen for some of our most basic needs for goods and services to be met. There are innumerable other ways in which data is exchanged that are also necessary for our economy to operate in the ways that we have come to expect. And, of course, there are other ways in which data is exchanged and used that raise questions about what we should and should not allow – and the degree of control that all of us as individuals should be in a position to exercise regarding how our data is used.

To make sense of privacy policy in light of the vast number of complex data-sharing activities that happen on a regular basis, it helps to have some guiding principles. Once you lose sight of those, it is easy to lose your way in this area.

In our view, those principles should be:

- **Establishing Uniform Nationwide Rules and Enforcement for Data Privacy** – Congress should create 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 legislation 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 Statutory 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 statutory obligations to ensure they comply with relevant privacy laws, 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. Federal law 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 law 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 law.

- **Data Security Standards** – A federal data privacy law 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.

Collectively, these principles can keep us on track to privacy law that is comprehensive and beneficial for consumers and businesses alike.

One of the things that has come along with the remarkable technological advances of the past generation, however, is a growing sense that the cost of many technologies is individuals' privacy. That concerns us and it is important that consumers trust our members and other businesses with which they deal. But, in constructing policy to deal with concerns regarding the tech sector, we should take care not to forget about Main Street businesses. The folks we represent can sometimes be ignored if the only construct that is considered is how commerce takes places on the Internet or through a mobile application.

Many in other industry sectors (particularly the technology and telecommunications sectors) will argue that their operations are so specialized that they should be exempted from certain requirements in privacy legislation. We are one of the few groups that will say the opposite – we are not special. We know that the Main Street businesses we represent will be covered by any privacy legislation. That is as it should be. Our members accept this responsibility because they value customer trust and consumer protection. But, every business sector should be covered by, and subject to, data privacy law and each business handling consumers' data should be responsible for doing what it can to protect privacy in accordance with the law – and should not be able to push liability for what it can do onto another business that is not in a position to do that on its behalf.

Unfortunately, shifting liability onto other businesses is precisely the tack that many businesses that consider themselves "service providers" take when advocating on these issues. They want Main Street businesses that deal directly with consumers to take the responsibility for what those “service providers” do. If we allow that to happen, consumers will be left with gaps in their privacy protection and Main Street will be saddled with liability that it has no practical way to avoid.

III. The American Data Privacy and Protection Act

The ADPPA represents an important milestone on the road to achieving a national data privacy standard. Gaining bipartisan agreement on a privacy proposal is incredibly difficult. By doing that, the Act makes important progress toward our goal of national policy. It is clear that the authors of ADPPA share many of the principles outlined above for privacy legislation. There also remain a number of parts of the Act on which we hope to work with the Committee to make improvements to ensure that it succeeds in meeting our principles. And, there remain areas of the Act that raise questions regarding how the provisions will apply. We hope this testimony can serve as a helpful roadmap to work through all of these issues.

Protecting Consumers Across Business Sectors

Ensuring that consumers are protected regardless of the business sector that has or handles their data is fundamental to ensuring we have effective privacy laws. The limits of committee jurisdiction, however, can get in the way of achieving this goal. But, those limitations can be overcome.

The Energy & Commerce Committee does not have jurisdiction over financial services firms. Those firms argue that they should be exempt from any new privacy regime because they are covered by the privacy provisions of the Gramm Leach Bliley Act (GLBA). That argument withers in the face of even the slightest scrutiny. Virtually no one involved in serious privacy discussions today would consider GLBA to be an adequate model for privacy legislation. GLBA, enacted in 1999, requires 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. GLBA does not require the notice to be available at other times (such as on a website) and it does not require providing consumer rights like access to information and an ability to correct or delete information. GLBA does not include prohibited uses of data and it does not require affirmative consent by consumers even for some of the most questionable uses of sensitive data that might be engaged in by financial services firms.

GLBA isn’t sufficient to protect consumer privacy and, frankly, isn’t very relevant to the debate around privacy legislation today. There should be a plan to work with the House Financial Services Committee and Senate Banking Committee to ensure that entities subject to GLBA will be fully subject to the provisions of the Act and any new privacy law. It would be indefensible if a new federal law passed that provided consumers more privacy rights when they go to the dry cleaner than when they go to their bank. We look forward to working with the Committee to address this in the Act.

Accountability for Business's Own Actions and Direct Statutory Obligations

One of the areas of recent privacy legislation that has proven challenging is the treatment of service providers. Some of the difficulty may be due to our assumptions about businesses across the country. We often think about the large businesses with which we deal directly on a day-to-day basis. But, the vast majority of Main Street businesses across the nation are small businesses. These small businesses must deal with a number of service providers including telecommunications firms, data cloud storage firms, data and payment processors, website-hosting firms, advertising firms, financial institutions, and many more. In contrast to Main Street businesses, these service providers are often large national or international businesses with many small business clients.

In fact, with regard to Internet access and other services, Main Street often has very limited choices of service providers in the marketplace. The Federal Communications Commission has reported that nearly half of all Americans have only one choice of high-speed broadband provider. The size disparities between Main Street businesses and service providers, and the lack of market choice leads to contracts of adhesion that disadvantage Main Street and often assign liability in ways that are not fair. Contracts are not an effective way to protect consumer privacy because they allow large businesses to game the system and ultimately mean that consumer rights are only protected if small businesses are willing to sue the large businesses in the face of violations. Typically, smaller businesses aren't willing to do that due to resource constraints and their need to continue to do business with the service provider in question.

Those that argue we should not worry as much about service providers – including telecommunications and technology companies – as we do about businesses with direct consumer relationships are ignoring what we know about privacy. Large businesses providing the communications and technology services that we take for granted today have a history of using private data in ways that most consumers would find objectionable. For example, Verizon agreed to pay a $1.35 million settlement to the Federal Communications Commission because it was inserting tracking cookies into data packets in order to track consumers across the Internet.[2] Main Street businesses often use service providers like Verizon to offer their customers wi-fi and other communications services. But those Main Street businesses would have no better luck determining whether Verizon was committing privacy violations of this sort than individual consumers would. That is just one of many examples of questionable privacy activities by companies that may be considered service providers within this legislation that Main Street businesses are not in a position to know about.[3]

[2] Karl Bode, "Verizon Strikes $1.35 Million Settlement with FCC Over its Use of Stealth 'Zombie Cookies'" *techdirt* (March 7, 2016) (available at https://www.techdirt.com/2016/03/07/verizon-strikes-135-million-settlement-with-fcc-over-use-stealth-zombie-cookies/).

[3] *See, e.g.*, "A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers," Federal Trade Commission (Oct. 2021) (available at https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers); Karl Bode, "Verizon didn't bother to write a privacy policy for its 'privacy protecting' VPN," *Vice* (Aug. 6, 2018) (available at https://www.vice.com/en/article/a3q4gz/verizon-didnt-bother-to-write-a-privacy-policy-for-safe-wi-fi-privacy-protecting-vpn); Julia Angwin, "AT&T Helped U.S. Spy on Internet on a Vast Scale," New York Times (Aug. 15,

We appreciate that the ADPPA has made important progress on aspects of these relationships. The Act imposes statutory obligations rather than relying on contracts. That is a key point.

It also requires service providers to comply with consumer requests when they are received from other businesses. But, more needs to be done to ensure this part of the Act fulfills its purpose. For example, the language of the Act is unclear regarding when a service provider must fulfill a consumer request and when it must only provide assistance to another business. More work is required to ensure these responsibilities are clear. The goal should not be controversial. Service providers should be required by law to do what they are in a position to do to ensure that consumer rights are protected. The same should be true of businesses that deal directly with consumers. But, neither category of business should be liable for the other's failure or refusal to follow the law.

The material difference between service providers and consumer-facing businesses really boils down to a procedural matter – namely, the fact that consumer requests to exercise their rights should go to the consumer-facing business first. Other than that, both categories of business should be required to fully follow the law and not be exempt from entire sections of the bill.

That means service providers should be subject to all sections of the bill, including sections 203 and 204, to ensure that there are no gaps in the privacy coverage that consumers receive. The language in section 302 exempting them from compliance with sections 203 and 204 should be removed so that there is no question that service providers must comply with the law – with the only distinction being that in most instances they would receive consumer requests from consumer-facing businesses and would respond to those consumer-facing businesses rather than responding to consumers directly.

In addition, the ADPPA (at section 302) imposes a due diligence requirement on consumer-facing entities in working with service providers and third parties that it does not impose on those service providers and third parties. Given the size, sophistication, and market power differences, if any due diligence were justified it would be more likely to run in the other direction. The typical single-location corner convenience store or coffee shop does not have the resources or expertise to conduct due diligence on the privacy policies and practices of corporate giants like Verizon, Comcast, Microsoft, and many others on which their businesses rely. The fact that each single store operator would have to conduct such due diligence on multiple large companies – Internet service providers, data storage companies, payment processors and more – makes it more unachievable even for larger businesses. In our view, the due diligence requirement should be removed as it is inconsistent with the disparities in size and resources we see among most of these businesses across the nation.

2015) (available at https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html).

Uniform Nationwide Rules and Enforcement

An important justification for a federal privacy law is that it can provide clear and consistent rules for consumers and businesses regardless of where they are located or operate across the nation. We appreciate that the Act includes language seeking to achieve this goal.

The number and range of exceptions to the preemption provisions of the Act, however, raise troublesome questions regarding the scope of the Act's preemptive effect. Case law in this area indicates that too many exceptions to federal laws attempting to preempt state law can undermine the intent and preemptive effect of the federal law entirely and reduce it to a scheme that simply preempts conflicting state laws (much like any federal law does based on the Supremacy Clause of the Constitution).[4]

In addition to the general question of whether the preemption provision of the Act will be effective, the exception for the California law on data breach notification raises additional questions. That part of the California law includes an ability for individuals to file lawsuits for noncompliance which would not need to adhere to the procedural requirements of the ADPPA. It is not clear to what extent that may create a loophole that could be exploited in a way that is contrary to the intentions of the Act's authors.

The exception in the preemption provision for violations of common law also creates a risk of inconsistent standards applying in different jurisdictions across the nation.

The enforcement provisions of the Act, of course, have been a focus of attention. We support allowing enforcement by the Federal Trade Commission (FTC) and state attorneys general.[5] Many businesses, however, are wary of allowing individuals to file lawsuits to enforce a privacy law. Our members share those concerns which stem from the complexity of achieving compliance with privacy laws as well as from experience with large volumes of questionable legal claims that have proliferated in other areas of the law. For example, Main Street businesses have received many demand letters from lawyers alleging violations of telemarketing rules, ADA website accessibility requirements, and patent laws. All too often, potential litigants are able to exploit the knowledge that obtaining legal representation and defending against a claim under a complex federal law is expensive. Those costs can lead businesses to agree to settlements of even non-meritorious claims simply to avoid litigation.

While the Act requires individuals to file with the FTC and state attorneys general 60 days prior to filing litigation, it appears that regardless of how those authorities evaluate the merits of those claims the individuals would still be able to pursue litigation. That raises questions about the purpose and effectiveness of the 60-day waiting period. This is an area of the Act that we think needs additional work.

[4] *See, e.g., Williamson v. Mazda Motor of Am., Inc.*, 562 U.S. 323 (2011); *Sprietsma v. Mercury Marine*, 537 U.S. 51 (2002); *Geier v. American Honda Motor Co.*, 529 U.S. 861 (2000); *Beyond Systems, Inc. v. Keynetics, Inc*., 422 F.Supp.2d 523 (D. Md. 2006).

[5] We would note that the authority of the FTC to seek fines under the Act, potentially before providing necessary clarity regarding requirements and what constitutes a violation of law, raises concerns.

Consumer Transparency and Choice

The Act lays out important consumer rights including the right for consumers to access their data, get mistakes corrected, and have data deleted. The Act also requires privacy policies to give consumers information regarding items including the categories of data collected, purposes of processing such data, and the categories of other entities receiving data. All of these are important rights that we support.

We do think there should be some recognition that certain data that relates to consumers is business data that should not be subject to deletion. Data that helps businesses track products sold, exchanged or returned by consumers, products under warranty, and other transaction information are important for businesses to maintain their operations, customer service, and inventory tracking. Financial records of businesses necessary for accounting, tax compliance and the like, for example, also should not inadvertently be subject to a consumer deletion request.

Preservation of Customer Rewards and Benefits

The Act seeks to address questions that have arisen in the context of state privacy laws regarding the viability of customer loyalty and rewards programs. Those programs offer customers things like free or discounted items after a certain number or dollar value of purchases. Of course, in order to provide those types of rewards, businesses must have a way to keep a count of the purchases made by those customers. But, State laws requiring that customers must be treated the same, even if some of them choose to prevent a business from tracking their purchases, created the possibility that offering other customers who voluntarily signed up for loyalty or rewards programs any price discounts would violate the law.

It is clear that Americans overwhelmingly want these programs to remain legal.[6] Generally, the states that most recently have passed privacy laws have all found ways to sufficiently preserve these programs.

The right principle to apply in this area is that consumers should not face retaliation for exercising their rights under privacy laws. The language of the Act might not get us to that principle. Rather than focusing on retaliation, section 104 of the Act requires "loyalty . . . with respect to pricing." This is a concept that does not exist today. If a sales price only applies to customers who have signed up for a rewards program, does that fulfill "loyalty" to the customers who decline to give their consent to enter the rewards program?

There is a rule of construction in the Act that is clearly intended to preserve these rewards programs. But, that language is made less clear by the way the section is positioned as requiring loyalty to all customers on pricing. And, the rule of construction is conditioned on the reward being given "in exchange for an individual's continued business." Typically, these programs are

[6] 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.

rewards for past business – not exchanges for future business (that is just a desired outcome). The rule of construction in the Act is also conditioned on the rewards program complying with all of the other requirements in the Act and regulations. That language is unnecessary and raises an interpretive question as to whether things in the Act that would not otherwise apply to the rewards program would now apply.

Getting this right is an important aspect for consumer acceptance of any new privacy regime.

More broadly, the Act recognizes that privacy should not unnecessarily hold up the normal and uncontroversial workings of commerce. Section 209 of the bill includes a number of helpful provisions to protect against negative outcomes. For example, that section provides a general exception to requirements in the bill for the data exchanges necessary to complete transactions and deal with "billing, shipping, and accounting."[7] There are similar exceptions allowing for data to be used to undertake system maintenance, inventory management, prevent fraud, deal with security incidents, and the like. The exceptions enumerated in this part of the bill are needed.

We do recommend, however, that section 209 make clear exactly the parts of the bill to which these exceptions apply. We would expect, for example, that these exceptions would override the need for any affirmative consent of consumers under sections 202 and 204, as well as for minors in section 205. We would also expect these exceptions to override the right to deletion in section 203. A number of other such questions arise throughout the bill. Given those questions, it would improve the bill to include a clear statement of the provisions of the bill to which the provisions of section 209 apply.

In addition, an area in which there are complex relationships among companies exchanging data includes advertising. Some of this is necessary as smaller businesses in particular must use service providers to help them keep up with their large competitors on marketing activities. Those small businesses cannot replicate the in-house advertising operations the many large businesses have.

There are, of course, legitimate concerns about how data is used in advertising. At the same time, that advertising fuels a significant amount of U.S. commercial activity and provides people information they want and need regarding available product and service offerings as well as pricing information. The economy would not be nearly as price-competitive without a healthy advertising sector and current price competition clearly benefits consumers. The breadth of the definition in the Act of sensitive data (including, in particular, that it does not include clear exceptions for the use of data when it is not linked to a specific individual) paired with some of the affirmative consent requirements in the Act may lead to difficulties for some of the types of advertising that are expected and helpful to people. This is an area that is complex and we welcome the opportunity to further explore it with the Committee.

[7] ADPPA section 209(a)(1).

The provision in section 302 of the Act requiring consent of the individual before a service provider can share data with another service provider will lead to problems with certain types of first-party advertising and other uses of customer data that are not controversial and do not require affirmative consent. There are often multiple service providers involved in making advertising happen and it should not require specific individual consent to ensure that those businesses can share the tasks involved in providing these and other services. As long as all of the service providers in the data chain must fully comply with the Act, consumers will remain protected.

<u>Data Security Standards</u>

The Act includes provisions relating to data security and we appreciate that the legal standard it sets is one of reasonableness. That is the appropriate standard and one we have long advocated. The generality of that standard is necessary due to the tremendous diversity among organizations that will be subject to the law. And, having that standard take account of factors like the size and complexity of the entity and the sensitivity of the data it handles makes sense.

We would recommend, however, that there be changes to the "specific requirements" in section 208 of the Act. Requiring those specifics overrides the helpful flexibility of the reasonableness standard. The requirements also override considerations like the size and complexity of the business being regulated. The specifics are, in short, both too lenient and too strict. For large, sophisticated businesses that many of us picture when thinking about privacy, the specific requirements in section 208 are minimal measures. Clearly, we should expect these things to take place.

For many small businesses, however, the specific requirements elevate form over substance and are overly burdensome. As noted previously, the vast majority of Main Street businesses are small and the specifics mean that the FTC cannot fully take into account size and complexity when considering data security. 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. Does it really help anyone for that individual owner to formally designate "an officer, employee, or employees to maintain and implement" data security practices? It is clear that owner is the person responsible. Requiring that designation to be formally made will not improve data security and, at worst, will serve as an easy "gotcha" for lawyers to look for when filing individual lawsuits. The other specific requirements could serve the same unfortunate purpose of providing a litigation checklist rather than materially advancing the data security provided by these small businesses.

In our view, these issues could be addressed by removing the specific requirements or simply making them examples of things that could be done if they are reasonable based on the size and complexity of the entity and the other considerations laid out in section 208. While there is an exception in the Act for businesses that handle smaller amounts of data, we are concerned that it is too stringent to allow many businesses to qualify – though that provision may provide another avenue to address some of these concerns.

We note that the Act does not include data breach notification requirements. It has been our position that the burdens of varying state requirements are particularly acute in this area. When companies suffer data breaches, they often need to hire counsel to advise them on the varied timeframes and requirements around the manner of notification in different states. This is an area that would benefit from uniformity.

It is also an area in which coverage of entities subject to the Gramm Leach Bliley Act would be particularly helpful. Many state laws exempt GLBA entities on the mistaken notion that they are subject to federal data breach notification requirements. They are not. GLBA recommends that notice should be provided following a data breach, but it does not require it.[8] That ought to be remedied in any privacy bill.

Other Issues

There are a number of other issues that would benefit from additional work through the legislative process. Some of the most impactful topics that merit attention include:

- Definition of covered entity – Currently, the way a covered entity is defined in section 2(9) of the Act includes that an entity that "shares common branding with another covered entity." Many franchisees and franchisors share common branding but are distinct companies. Similar arrangements are common to about half of the convenience industry. While the major integrated oil companies own just 0.2 percent of motor fuel outlets, about half of them use the branding of an oil company or refiner. The owners of these retail outlets are independent businesses, typically small businesses, that have an arm's length contract allowing them to display that branding. If those companies are deemed to be the same covered entity, then they will each be liable for the privacy practices of the oil brand or franchisor as well as all of the other branded outlets or franchisees. That is not a tenable outcome and we don't believe that was the intended outcome of the authors of the Act. But, this is an important issue and one we are eager to fix in the next iteration of the Act's language.

- Definition of large data holder – The Act treats large data holders differently than other businesses regulated under the bill in several respects. That definition, therefore, should avoid sweeping small- and medium-sized businesses within its bounds. The provision at section 2(17)(B)(ii) regarding the number of individuals' sensitive data that it handles creates a risk that those small- and medium-sized businesses could be viewed as large data holders simply because their business

[8] GLBA instructs various agencies to establish security guidelines, not regulations, to implement the directives in GLBA. Gramm-Leach-Bliley Financial Services Modernization Act, Title V of the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. §§ 6801, 6809, 6821, and 6827). When designing security controls, financial institutions need to "consider" a data breach response plan but are not required to develop a data breach response program or notify consumers after a breach. *Interagency Guidelines Establishing Information Security Standards*, 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS).

depends on having a large number of small-dollar transactions with customers. We think this issue could be addressed by making clear that transaction data does not count toward the large data holder definition. This would be consistent with the concept in section 209 providing that transaction data is subject to a general exception from some requirements in the Act and with the exemption for those with small amounts of data in section 208.[9]

- Privacy policies – Everyone will have an interest in businesses doing more on privacy over time and improving their policies. Language in section 202(d) of the Act, however, might create a disincentive to doing that. It references the need for affirmative express consent when a material change is made to a privacy policy. But, that requirement seems to extend even to changes that under the Act would not otherwise require affirmative express consent. That will create a strong reluctance for businesses to update and change their policies, even in consumer-friendly ways, because policies or actions that are viewed as not requiring affirmative consent will be transformed into ones that do. We recommend making clear that such affirmative consent only attaches when the change to the policy implicates affirmative consent under the Act.

- Restricted practices – In general, we have always been open to making clear that some data practices should be prohibited. This can provide clarity for businesses and consumers and allow other commerce to take place without as much friction. The Act includes a recitation of such practices in section 102. We see some areas within that section which could be improved. For example, the use of social security numbers needs exceptions allowing that data to be used for prospective employees for the purpose of conducting background checks. It also appears that there should be an exception for current employees (unless section 102 will be limited to covered data).
    - Another example is the use of the term "authentication." That is a term of art with respect to payments, but it's not clear how broad the term is intended to be in the Act – particularly because the term is used at multiple points in the Act. Defining that term could help avoid confusion.
    - Smaller businesses rely on service providers to do what some of their competitors are able to do in-house. One of those things is providing advertising to their own customers. That type of advertising is something that American consumers expect. The use of their data, including such things as past purchases or parts of their history browsing a retailer's website, generally are not controversial when they involve that retailer using the information to market directly to their own customers. But, as noted, these retailers don't have the technological sophistication to do all

[9] It is worth noting that without this change, large numbers of businesses could be deemed both large data holders under the definition in section 2 and simultaneously fall within the small data exception in section 209 of the Act.

of that themselves (or the employees to do the work of putting together even basic advertising like direct mail).

- Sensitive Covered Data – The Act includes credit and debit card numbers in its definition of "sensitive covered data." But, the last four digits of those numbers are printed on receipts and used to help facilitate product returns and track the status of purchases in other ways. The definition should make clear that the last four digits of payment card numbers do not constitute "sensitive" covered data.

* * *

We appreciate the dedication of the Members and staff in getting us to this point and the opportunity to discuss these issues with you. A bipartisan draft of federal privacy legislation marks a significant milestone on the journey to get a federal law. There remain many areas on which we look forward to working with the authors to make changes to improve the legislation and clarify how it will work.