Testimony of Paul Martino, General Counsel to the Main Street Privacy Coalition
"Protecting the Virtual You: Safeguarding Americans' Online Data"
Subcommittee on Privacy, Technology, and the Law
U.S. Senate Committee on the Judiciary

July 30, 2025

Chair Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee on Privacy, Technology, and the Law, I am Paul Martino, a partner at Hunton Andrews Kurth here in Washington, DC, and I serve as General Counsel to the Main Street Privacy Coalition (MSPC).[1] On behalf of the coalition, we appreciate the opportunity to testify before the Subcommittee on the important topic of data privacy.

The MSPC was formed in 2019 to support Congress in passing federal privacy legislation to establish uniform, nationwide privacy standards that protect the privacy of all Americans, regardless of where they live. Members of the coalition share the belief that a preemptive federal privacy law will benefit consumers and Main Street businesses alike. A single, uniform privacy law on consumer data would give consumers the confidence that their data will be protected consistently regardless of where they live or do business and that they will have the right to benefit from their data as they see fit. A federal preemptive law will also provide the certainty Main Street businesses need to consistently and responsibly use consumer data to better serve their customers across the country. As detailed below, the MSPC advocates for a core set of principles that Congress should consider when developing a comprehensive federal privacy law.

MSPC's trade-association members represent a broad array of companies that line America's Main Streets, including retailers, restaurants, grocery and convenience stores, hotels, resorts and hospitality companies, gas stations, and a wide range of franchise establishments. Our trade groups' member companies interact with consumers on a daily basis and can be found in every town, city, and state, providing jobs, supporting our economy, and serving Americans as a vital part of their communities. Collectively, the industry sectors that MSPC member trades represent directly employ approximately 34 million Americans and contribute $4.5 trillion to the U.S. gross domestic product.

MSPC is dedicated to enactment of a federal data privacy law that creates equivalent privacy obligations for *all* businesses handling consumers' personal information. We also appreciate this opportunity to testify because the views of Main Street businesses have been absent in some other Congressional hearings despite the fact that Main Street industry sectors represent the backbone of the U.S. economy and constitute our nation's largest private sector employers.

[1] Additional information about the Main Street Privacy Coalition (MSPC) is available at: https://mainstreetprivacy.com

Previous federal privacy bills have significantly narrowed the obligations of other entities, largely exempting Big Tech, telecommunications, cable, and other "service providers" from the same obligations to protect consumer privacy that apply to Main Street businesses. Further, despite the bipartisan support for federal privacy legislation to protect consumers *comprehensively*, most of the proposed privacy legislation to date has focused on requiring Main Street businesses to protect consumers' data, but has not required the same of financial institutions that process far more sensitive consumer data than other businesses.

We hope the coalition's testimony today and our continued efforts to inform Congress will help reverse this recent trend in federal bills promoting *inequivalent* privacy protections among industry sectors by creating momentum for comprehensive federal privacy legislation that will apply *equivalent* data privacy obligations for all businesses handling consumers' personal data in order to achieve the shared bipartisan goal of enacting an effective nationwide privacy law. In sum, every business in the data-handling chain must be required to do what it can to appropriately protect individuals' privacy. Critically, however, businesses should not be responsible for the data privacy practices of other entities whose actions they cannot control. Some past bills have made Main Street businesses responsible for other businesses by assuming they have powers to control them that they do not have. Bills like this ultimately leave consumers unprotected and foist unjustified liability risk onto Main Street businesses.

Ensuring equivalent data privacy obligations is also inherently pro-consumer. Consumers have a right to expect a regulatory system they can understand, predict, rally around and support *as intended to protect them*. They should not be required to research and understand several sources of law simply to know how their local business or institution will handle their data.

EXECUTIVE SUMMARY

Since 2019, MSPC has supported preemptive federal privacy legislation with provisions modeled on the strong consensus of enacted state privacy laws that ensure equivalent application of national data privacy standards to all businesses handling consumers' personal information. Privacy legislation crafted like this creates critical incentives across industry sectors that provides for the comprehensive protection of consumers' personal data and avoids the potentially unintended consequences that disproportionately impact Main Street businesses and, in turn, harms American consumers and the U.S. economy.

MSPC believes consumers should be empowered to control their personal data and businesses should be permitted to responsibly use such data, subject to the choices consumers are entitled to make following disclosure of the businesses' intended uses. We respectfully suggest a guiding principle for Congress should be passing a federal data privacy law that avoids our current path toward 50 disparate, conflicting state privacy laws. As its central objective, a federal privacy law should establish a uniform and nationwide set of consumer protections to protect all Americans that preempts related state laws to overcome barriers to interstate commerce and enable consistent application of the law.

Achieving that goal has been elusive. One of the central challenges to past efforts by Congress has been its overwhelming focus on the practices of so-called "Big Tech" companies, which obscured the reality that data privacy laws also apply to, and must work for, Main Street businesses that directly and transparently serve our communities, while also contributing the majority of American jobs.

To overcome this persistent challenge, MSPC urges Congress to craft privacy legislation that embraces and fully embodies in its provisions the following core principles to ensure a balanced and effective national privacy framework:

- **Establish a Uniform National Privacy Law:** Congress should enact a privacy law that benefits consumers and businesses alike by ensuring *all* personal data is protected in a consistent manner regardless of where a consumer resides.

- **Protect Consumers Comprehensively with Equivalent Standards for All Businesses:** Federal data privacy law should apply requirements to all industries that handle personal data. A federal privacy law should not place a disproportionate burden on certain sectors of the economy while alleviating others from providing equivalent protections of personal data.

- **Create Statutory Obligations (Not Contractual Requirements) for All Entities that Handle Consumers' Data:** Given imbalances in contractual negotiating power, effective consumer protection cannot be achieved by relying on Main Street businesses to regulate the conduct of market-dominant service providers through contracts. Service providers and third parties must have statutory privacy obligations when offering data processing, transmission, storage, or other services to collectively millions of Main Street businesses.

- **Preserve Customer Loyalty Rewards and Benefits:** A federal privacy law must preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships such as loyalty programs.

- **Require Transparency and Customer Choice for All Businesses:** Consumers deserve to know the categories of personal data that *all* businesses collect, how it is generally used to serve them, and the choices they have regarding those uses.

- **Hold Businesses Accountable for their Own Actions:** Privacy legislation should not include terms that potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of independent business owners.

- **Ensure Reasonable Data Security Standards:** Privacy legislation should include reasonable data security standards for *all* businesses handling consumer data, as well as uniform rules for *any* businesses suffering a data security breach to notify affected individuals.

- **Establish Effective Accountability and Enforcement**: Effective enforcement must hold accountable *all* businesses handling consumer data to *equivalent* data privacy standards using the *same* enforcement mechanisms, thereby creating an even playing field and proper incentives across industry sectors to comply with those standards. Because "mistake-free" compliance is unlikely in this complex area of the law, we support the approach adopted in all enacted state privacy laws of coupling *exclusive* governmental entity enforcement with the regulated entity's ability to "cure" non-compliant practices within a limited period of time after timely and specific notice from the governmental authority.

These principles can also be found in *Appendix A (attached)* and on our website here. Each has important implications for federal privacy legislation. Our considerations in formulating them from our legislative experience are discussed further in our written testimony below.

DISCUSSION OF PRINCIPLES FOR FEDERAL COMPREHENSIVE PRIVACY LEGISLATION

I. Overcoming the Challenges to Establish a Uniform National Privacy Law

MSPC strongly supports Congressional efforts to establish a national framework that provides comprehensive data privacy protections for all Americans under a federal privacy law that supersedes and replaces the fragmented and conflicting state statutes and regulations that artificially differentiate Americans' privacy rights based on states in which they live. Achieving this shared goal in legislation has proven elusive. We respectfully suggest ways to overcome the challenges in perception and drafting statutory language to achieve the primary objective of federal privacy law.

Americans have the right to live and travel to any state in our country, and to engage in commerce in each of these states. The Constitution protects these rights and reserves to Congress the regulation of interstate commerce. This permits citizens from any state to avail themselves of the public highways to travel across the states, enjoy different states' environments and cultures, and visit places of public accommodation across the country that enable their engagement in interstate commerce. When they shop online, make a restaurant reservation, or book a hotel in another state, they similarly are engaging in interstate commerce. In all of these real world and online activities, protecting Americans' privacy interests is the same interest of each state, and it does not vary from state to state based on a state's geography, environment, or other unique attributes of its location.

In this sense, all Americans and all states have the same, uniform interest in protecting data privacy. It is with this perspective too that a national law can create the necessary framework to ensure that consumer data is protected, uniformly, across all states, and wherever Americans choose to travel, shop, eat, purchase goods or stay overnight. Congress can build on the work states have already done to protect privacy by creating a federal law that reflects the strong consensus of existing state laws and sets nationwide standards that apply equally regardless of where Americans engage in commerce.

MSPC has long supported federal privacy legislation that preempts differing state statutes and regulations in an effort to establish a single, uniform national privacy law. Previous comprehensive privacy legislation considered in Congress has not been written effectively to achieve this goal despite including provisions that were intended to preempt state laws. Those past bills, such as the American Privacy Rights Act (APRA), if enacted, would have failed under challenges in federal courts, ultimately leaving American consumers with different privacy rights depending on where they were located.

The federal courts' posture is to maintain a presumption *against* preemption of state law unless Congress clearly and expressly preempts state laws in the ways the Supreme Court has upheld. We respectfully suggest that Congress rely on the precedents of the Supreme Court and federal courts on *how* a federal law must be drafted to effectively preempt state laws.[2] To ensure effective preemption, privacy legislation should avoid using a general rule followed by pages of exceptions – a form the Supreme Court and other federal courts have used as the basis to deny preemption of state law in a range of federal bills on the basis that Congress did not speak clearly or expressly of its interest. These rulings frustrated Congressional intent by preserving state laws covering the same ground as the federal law.

Adherence to these long-standing precedents would permit a federal privacy law to overcome anticipated challenges to preemption in federal court that are likely to come from states and other parties. Failure to preempt state laws would undermine the primary goal of establishing a national law protecting the privacy of all Americans by permitting the continued enactment of conflicting state privacy laws.

A preemption provision in a federal privacy law can be well-crafted to overcome past deficiencies in prior legislation, such as the APRA, by specifying precisely which state privacy laws are preempted and by making it clear that future laws related to the federal law would be similarly preempted. Such an approach holds the promise of making federal privacy legislation much more likely to achieve its primary goal of creating a single, uniform national privacy law for all Americans.

Without the careful attention to detail in how a preemptive standard is crafted, it will most likely fail in the courts despite the best intentions of members of Congress, leaving American consumers with different protections depending on where they live or engage in interstate commerce. The impact of this failure would be felt acutely by America's Main Street businesses that continue to face unclear standards and compliance burdens differing from federal standards set by Congress.

While many stakeholders support preemptive federal privacy legislation in principle, this is the most important and challenging area of drafting a federal privacy law, and where the principle must be honed into effective legislative language to achieve Congressional intent.

[2] *See* white paper on Federal Preemption of State Law prepared originally as a memo to the House Energy and Commerce Committee in 2011 and updated several times since then, with the most recent edition Feb. 6, 2020.

II. Protect Consumers Comprehensively with Equivalent Standards for All Businesses

Consumers should be empowered to control their personal data used by businesses and, consistent with that, businesses should be permitted to lawfully and responsibly use such data that consumers share with them to better serve their needs. MSPC urges Congress to consider the strong consensus of state privacy laws in balancing these interests.

Main Street businesses will bear the full burden of regulatory obligations under proposed federal privacy laws just as they currently comply with all enacted state comprehensive privacy laws and data security standards. Previous federal legislation, however, has often significantly narrowed the obligations of other businesses, largely exempting Big Tech, telecom, cable, and financial industry service providers from the same obligations to protect consumer privacy as Main Street businesses. We strongly recommend federal privacy laws apply *equivalent* data privacy obligations to all businesses and Congress can do so by adhering to certain principles in setting the roles and responsibilities of entities subject to the law.

A. Hold Businesses Accountable for Their Own Actions

Federal data privacy frameworks should apply requirements to all businesses that handle consumers' personal data and should not place a disproportionate burden on certain sectors of the economy while alleviating other industry sectors from providing equivalent protections of personal data. Further, businesses must be held accountable for their own actions.

Each business handling consumer data is in the best position to control its *own* actions and compliance with the law and not necessarily others' compliance. This is particularly true for most businesses defined as "controllers" in privacy legislation, which are overwhelmingly small businesses that often lack the ability to *actually* control the actions and compliance of data "processors," which tend to be large, nationwide or global businesses that serve them. A federal privacy law that obligates smaller controllers to ensure compliance of large nationwide processors will accomplish little, other than adding unnecessary cost and undeserved liability to many small Main Street businesses that are not in a position to absorb either.

For a federal privacy bill to have effective and accountable rules, we must *revise* the proposed language in previous legislation to correct the ineffective mechanisms and imbalance in obligations among stakeholders that exempted certain types of businesses from accountability for their own actions and would have held Main Street businesses liable for actions of other businesses that they cannot control.

Common Branding and Joint Liability Concerns: In prior House legislation, before it was corrected at the urging of MSPC, language had been proposed to hold franchisors and franchisees liable for each other's privacy law compliance. Many franchisees and franchisors share "common branding" (e.g., the franchisees all use

the same brand on their restaurant, fitness center, hair salon, etc.) but are distinct companies with different owners, employees and operations, and should be treated as such. Past federal privacy bills have defined these entities as one single "covered entity" because the businesses operate with "common branding." We appreciated that subsequent versions of House bills removed the "common branding" language from privacy legislation and we urge that all bills use definitions that avoid making broad groups of independent businesses jointly liable for one another's behavior when there is lack of control.[3]

B. Establish Statutory Obligations for Service Providers Handling Consumer Data

Given imbalances in contractual negotiating power, effective consumer protection cannot be achieved by relying on Main Street businesses to regulate the conduct of market-dominant service providers through contracts alone. Rather, federal privacy law should subject service providers to statutory obligations in federal law that exist in enacted state privacy laws. These require service providers (i.e., defined as "processors" in most state laws) to protect personal data they handle on behalf of other businesses (i.e., defined as "controllers" in most state laws) when engaged in processing data for collectively millions of Main Street businesses.

As shown in *Appendix B (attached)*, which compares the processor requirements in key state laws, a federal privacy law should protect consumers' privacy in the following ways when service providers are processing their personal data:

- **Data Security**: Processors must ensure their own data security when handling personal data they receive from controllers;
- **Privacy Rights Requests and Breach Notices**: Processors must fulfill privacy rights requests and make data breach notifications either directly or through providing all information necessary for controllers to do so;
- **Data Privacy Assessments**: Processors must provide all information necessary to complete required data privacy assessments (also known as privacy impact assessments);
- **Confidentiality**: Processors must ensure the confidentiality of personal data when handled by processors' employees;
- **Subcontractor Accountability**: Processors must hold subcontractors to the same terms that they must meet, and provide controllers with notice and a right to object to engaging subcontractors;
- **Return or Deletion of Data**: Processors must return or delete, at the choice of the controller, data it possesses at the end of the processing contract;

[3] Senators will recall that, last year, Congress approved a Congressional Review Act action overturning the National Labor Relations Board's joint employer standard. Lawmakers opposed the NLRB rule as it would have incorrectly classified two entities as joint employers *where an entity lacked substantial direct and immediate control over the essential terms and conditions of employment of another entity's employees*. Similarly, franchises—most of whom are small businesses—within a franchise system operate under the franchisor's trademark but are *distinct entities with no control* over any aspect of their fellow franchisees' business.

- **Evidence of Compliance**: Processors must provide controllers with all the information required to demonstrate the processor's compliance with the law;
- **Reasonable Audits**: Processors must allow and cooperate with reasonable audit requests or assessments at the request of controllers; and
- **Liability Protections**: The law must protect controllers from liability for violations of the processor's own obligations under the law.

C. Balance All Parties' Obligations to Fulfill Individuals' Privacy Rights Requests

MSPC has spent considerable time working with sponsors of privacy legislation to craft provisions that balance all parties' obligations when receiving, handling, and ultimately fulfilling individuals' requests to exercise data privacy rights provided by law, such as the right to access, correct and delete their personal data. We support efforts to ensure greater balance in the statutory obligations applying to all parties handling customer data with respect to the processing of consumers' privacy rights. This is particularly important where small Main Street businesses and large nationwide or global service providers are handling the same customers' data due to vastly different contractual bargaining power when executing data processing contracts in states that lack statutory requirements for fulfilling consumers' rights requests. Under federal privacy legislation, all companies in the chain of personal data should be required to honor consumers' privacy rights requests regardless of which business first receives that request.

To address the concerns with ineffective accountability among all parties in the chain of personal data, a federal privacy framework should require controllers to act as the *recipient* of consumer privacy rights requests and require controllers to pass valid requests onto processors who are necessary to fulfilling such requests. Controllers' responsibilities from there should be limited to doing what the controllers *themselves* can do to comply with such requests, plus communicating what their data processors must do with their obligations to fulfill such requests – a process that has been delineated in some previous Senate privacy bills.[4]

Ultimately, despite the use of language that might imply greater capability than is the reality, "controllers" should not be required to police compliance by processors, and controllers should not be liable for processors' failures to comply with consumers' rights requests where they have communicated a verified rights request to a processor for fulfillment. For example, a controller that transmits a validated consumer's data deletion request to a processor should not be held liable under the

[4] The Subcommittee should carefully review the provisions of Senator Moran's *Consumer Data Privacy and Security Act* that was last introduced on April 29, 2021. The Moran bill sets the rights and responsibilities of parties in the law in ways that avoided the pitfalls of more recent privacy legislation considered in Congress since 2022. In particular, the Moran bill ensured a process for handling consumer rights requests that carefully balanced the obligations to ensure all parties handling the same consumer's data honored that consumer's rights requests in an accountable way.

law for that processor's failure to delete the consumer's data as requested. The liability for that failure should rest with the processor.

D. Prohibit Liability-Shifting of Statutory Obligations Via Contractual Provisions

Privacy responsibilities should not simply be shifted from one industry sector onto another. It is manifestly unfair to businesses that bear the brunt of those shifted burdens when it should be the other businesses' own obligations to the consumer. Too often powerful businesses within the Big Tech, telecom, cable, and financial services industry sectors use their superior market power to shift what should be their own responsibilities onto smaller businesses they serve via contractual requirements, often leaving Main Street businesses with outsized compliance burdens and costs. If Congress relies on parties' contractual relationships alone to implement comprehensive privacy protections with the goal of exalting such contracts into having the force of federal law behind them, it will assuredly leave holes in consumer privacy rights because federal enforcement agencies will have no effective way to compel service providers or third parties to comply with the law. To avoid this, a federal privacy framework must create effective federal statutory obligations that hold each party accountable.

E. Correct Imbalances in Financial Privacy Law to Meet Consumers' Expectations

In our American society that relies on fast and convenient commerce, successful businesses serve customers as they expect and strive to accept a variety of forms of payment that meet customer needs. Most Main Street businesses, for example, accept credit and debit cards for the purchase of goods and services they provide. Increasingly they also accept other forms of payments, like consumers' using virtual cards in "wallets" on their mobile phones to make purchases in person and using digital payments from popular financial technology (fintech) companies online. Main Street businesses can accept those payments by securely interfacing with and sharing payment data with payment processors, card companies and banks authorizing payments.

We have concerns about any exemptions for financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) from comprehensive privacy legislation. Privacy legislation should ensure the payment data required to be shared in the financial system is protected equivalently by other parties, such as payment processors, payment networks and financial institutions.

GLBA was enacted in 1999, and its provisions are far outdated by decades of improvements in data privacy laws that render GLBA stale by comparison. MSPC supports efforts in the House Financial Services Committee to update GLBA because, in its present form, it does not provide consumers with *equivalent* privacy protections they would expect from enacted state privacy laws.

To illustrate the disparity between today's most referenced privacy laws to what financial institutions face under GLBA, the chart in *Appendix C (attached)* compares GLBA's provisions to the base privacy protections in privacy laws established by the European Union (which applies the General Data Protection Regulation to banks serving European customers) and in California (which exempts banks from the California Consumer Privacy Act). The chart demonstrates where GLBA does not include anything approximating the data privacy protections that most consumers have now come to expect after two and a half decades of improvements in this area of the law to protect consumer privacy. Most Americans would be surprised to learn they have far more privacy protections when buying an ice cream cone than when engaging in sensitive financial transactions involving their life savings with their financial institution. That simply should not be the outcome of federal privacy law and it is an area where Congress can improve on the state laws.

Congress has the opportunity to correct this imbalance in federal law when passing comprehensive privacy legislation to protect consumers' privacy in an equivalent manner when they purchase goods and services across the American economy.

III. Preserve Customer Loyalty Rewards and Benefits

A federal data privacy law must preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships like immensely popular customer loyalty, rewards, premium features, discounts or club card programs.

Loyalty programs are a critical and ever-growing facet of today's business models employed by a wide range of American businesses serving consumers in their daily lives. These programs are not to be mistaken with the principal business model of "free" online services that are paid for by commercial advertising, but rather are programs designed to provide discounts or rewards to a company's best customers to encourage future engagement with the same business when purchasing goods like food, apparel, or gas, and services like flights, hotel rooms, or rental cars. These programs are already inherently privacy-protective because they typically require customers to affirmatively opt into the plan in order to receive discounts, rewards, or other benefits as a member of the program.

Americans greatly benefit from customer loyalty programs offered by Main Street businesses. Bond Brand Loyalty Inc. has issued reports on loyalty programs and benefits to consumers for the past 14 years. In prior years, their reports found that 73% of consumers said they were more likely to recommend brands with good loyalty programs and 79% said loyalty programs make them more likely to continue doing business with the brands offering them.[5]

More recently, *The Bond Loyalty Report 2024* found that brands "using loyalty programs *well*…focused on personalization and superb customer care—both essential aspects of successful loyalty programs." As highlighted in Bond's press release, "participants must be

[5] See *The Loyalty Report 2019*, published by Bond Brand Loyalty, Inc.

'recognized' to feel seen, leaning into the human-to-human connections that leave them feeling special." Bond also found consumers join a "huge number of programs" as the average person participates in 19 different loyalty plans that influence their brand choices. "The influence of loyalty programs on customer behavior is higher than ever with 79% of consumers being more likely to recommend brands with solid loyalty programs and 85% of consumers saying they are more likely to continue buying from the brand."[6]

State privacy laws appropriately preserve customer loyalty programs but do so with very narrowly tailored provisions that do not alleviate businesses from the transparency, disclosure, and other provisions of state laws that provide consumer rights. Nor do state laws exempt providers of these programs from the laws' general prohibitions on retaliating against a consumer for exercising privacy rights. These state laws instead include savings clauses that indicate the prohibitions on retaliating or discriminating against consumers who exercise privacy rights cannot be construed to prohibit businesses from offering customers the ability to voluntarily participate in customer loyalty programs providing better prices or services. In short, they clarify that when some customers choose to participate in these programs, their individual choices cannot be viewed as an act of discrimination against any customer who does not choose to participate in the program.

MSPC strongly urges Congress to adopt provisions in federal privacy laws similar to the strong consensus of state laws that preserve loyalty programs and benefits where consumers voluntarily participate in *bona fide* programs offering better prices and services.[7]

IV. Ensure Reasonable Data Security Standards

MSPC supports federal privacy laws that ensure all businesses handling consumer data have reasonable data security standards appropriate to their size, nature of business, and scope of transactions involving personal data. We also support legislation designed to provide uniform federal rules for data security breach notification.

Consumer-facing companies like Main Street businesses must comply with data breach notification laws in all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. However, many of these laws exempt third-party service providers and financial institutions from the same breach notification requirements. Federal privacy law should correct these "breach notice holes" by requiring *all* businesses handling personal data to provide notice to affected individuals of their *own* data security breaches when they occur unless the non-breached party elects to notify individuals of a breach by a third-party processor. This approach would hold accountable *all* breached entities and create proper incentives for third parties to secure personal data they process on behalf of another business while preventing the shifting of notice obligations onto non-breached businesses.

---

[6] *See* Press Release, Bond Brand Loyalty Inc. (July 25, 2024)*:* https://info.bondbrandloyalty.com/the-loyalty-report-2024-press-release

[7] These laws use a savings clause clarifying that the state law's anti-retaliation or non-discrimination provisions shall not be construed to prohibit a business from offering better prices or services in connection with bona fide loyalty programs.

V. Establish Effective Accountability and Enforcement

Effective enforcement of a federal privacy law requires holding accountable *all* businesses handling personal data to *equivalent* data privacy standards using the same or similar enforcement mechanisms, thereby creating an even playing field and proper incentives across industry sectors to comply with those standards. Additionally, because "mistake-free" compliance is unlikely in this complex area of law, we support the approach adopted in all enacted state privacy laws of coupling *exclusive* governmental entity enforcement with the regulated entity's ability to correct or "cure" non-compliant practices within a limited period of time after receiving specific notice from the enforcement authority.

A. Benefits of *Exclusive* Governmental Entity Enforcement

Every enacted state comprehensive data privacy law relies on *exclusive* government enforcement coupled with a notice-and-cure provision. No comprehensive state privacy laws permit private rights of action to enforce the *privacy* provisions of those laws, even in California. Three critical reasons explain why this approach has developed into the appropriate consensus method for ensuring uniform application, interpretation, and enforcement of privacy standards under state privacy laws:

- Meaning of "Reasonable." All comprehensive state privacy laws contain dozens of uses of the words "reasonable" or "reasonably" when setting forth business obligations. Each use of those terms raises the possibility of widely different interpretations in meaning. Leaving private lawsuits to define what are "reasonable" privacy practices would result in endless litigation and differing standards that would call into question even the practices that government enforcement authorities find reasonable. It would also chill investment in innovative, responsible business practices that improve service to customers in a rapidly evolving technology environment. Exclusive governmental enforcement is the only way to ensure uniform interpretation and enforcement of the law.[8]

- Robust Compliance with Privacy Laws and Rapid Error Correction. To protect consumers, there must be a mechanism to encourage regulated entities to rapidly correct errors to get their privacy compliance right. All state privacy laws have adopted a notice-and-cure mechanism for this purpose, especially when a law is new. It provides an expedited means for businesses to correct technical errors without fearing bankrupting lawsuits. The California Attorney General confirmed the benefits of its notice-and-cure provision reporting that 75% of the

[8] In the Vermont Senate debate on June 17, 2024 (*see* webcast starting at 09:29) that sustained Governor Scott's veto of H. 121, the Vermont Data Privacy Act that included private rights of action, a key argument to sustain the veto (i.e., kill the bill) was that the bill had approximately 70 uses of the terms "reasonable" or "reasonably" that could not be left to private litigation in state courts to uniformly interpret and enforce. The Vermont Attorney General and other state AGs, however, could bring uniformity to the analysis. (Note: In California, there is joint AG and privacy agency enforcement authority, but it is still exclusively governmental enforcement authority of the privacy provisions of the California Consumer Privacy Act).

businesses notified had corrected their errors within 30 days.[9] Adversarial litigation, on the other hand, can take years and is not the best mechanism to encourage or achieve uniform, consistent, or timely compliance with the law.

- Private Litigation Disproportionately Impacts Main Street Businesses. Private rights of action have been rejected in every one of the states that have enacted comprehensive privacy laws. Private litigation often disproportionately impacts Main Street businesses, such as when plaintiff attorneys use "sue-and-settle" campaigns aimed at thousands of small businesses to collect quick settlements for vague, alleged violations of federal law. Dominant technology companies can force arbitration or otherwise fight litigation; small Main Street businesses cannot. Congressional committees have witnessed problems with so-called litigation trolls in many areas of law and passed legislation to stop it.[10] There is a significant risk that a similar cottage industry of *privacy* trolls, if given the chance, would leverage private rights of action against Main Street businesses in bad faith here as well.[11] Finally, as MSPC raised in its letter opposing private rights of action in the APRA, federal privacy legislation can risk disproportionately impacting Main Street businesses when exempting other parties from the same type of enforcement.[12]

~

Thank you for your consideration of MSPC's testimony. We appreciate the opportunity to participate in today's hearing and welcome your questions.

[9] California Attorney General Bonta reported that, in the first full year of implementing a notice-and-cure provision, 75% of companies notified of potential violations responded by amending their practices to come into compliance within the 30-day cure period, with the remaining 25% either in the process of their 30-day cure period or under further investigation. *See:* https://iapp.org/news/a/california-attorney-general-offer-ccpa-enforcement-update-launches-reporting-tool

[10] To curb the pattern or practice of sending vague and abusive demand letters alleging, in bad faith, patent infringement by Main Street and other businesses, the House Energy and Commerce Committee approved and reported to the House floor H.R. 2045, the *Targeting Rogue and Opaque Letters (TROL) Act*, to protect these businesses from the deceptive acts and practices of patent trolls.

[11] In the previously discussed Vermont Senate vote to sustain the governor's veto of the legislation with private rights of action *(see footnote 12)*, another compelling argument raised in opposition to private rights of action was that Vermont small businesses would be disproportionately impacted by out-of-state trial lawyers, driving up prices for consumers.

[12] The APRA exempted service providers and third parties from almost all enforcement by private rights of action while subjecting all Main Street businesses to this mass litigation threat, creating a severely disproportionate impact on some businesses over other and picking winners and losers in the marketplace.

Main Street
PRIVACY COALITION

MSPC Testimony to Senate Subcommittee on Privacy, Technology and the Law

Appendix A

Main Street Principles for Data Privacy Legislation

American businesses have no higher priority than earning and maintaining trusted relationships with their customers. To preserve those relationships, businesses must protect and responsibly use the personal information that customers share with them. As Congress considers legislative and regulatory solutions to address data privacy concerns, our coalition urges adoption of the following principles.[1]

- **Establish a Uniform National Privacy Law**
  Congress should enact a privacy law that benefits consumers and businesses alike by ensuring *all* personal data is protected in a consistent manner regardless of where a consumer resides.
- **Protect Consumers Comprehensively with Equivalent Standards for All Businesses**
  Federal data privacy law should apply requirements to all industries that handle personal data. A federal privacy law should not place a disproportionate burden on certain sectors of the economy while alleviating others from providing equivalent protections of personal data.
- **Create Statutory Obligations (Not Contractual Requirements) for All Entities that Handle Consumers' Data**
  Given imbalances in contractual negotiating power, effective consumer protection cannot be achieved by relying on Main Street businesses to regulate the conduct of market-dominant service providers through contracts. Service providers and third parties must have statutory privacy obligations when offering data processing, transmission, storage, or other services to collectively millions of Main Street businesses.
- **Preserve Customer Loyalty Rewards and Benefits**
  A federal privacy law must preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships such as loyalty programs.
- **Require Transparency and Customer Choice for All Businesses**
  Consumers deserve to know the categories of personal data that *all* businesses collect, how it is generally used to serve them, and the choices they have regarding those uses.
- **Hold Businesses Accountable for their Own Actions**
  Privacy legislation should not include terms that potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of an independent business owners.
- **Ensure Reasonable Data Security Standards**
  Privacy legislation should include reasonable data security standards for *all* businesses handling consumer data, as well as uniform rules for *any* businesses suffering a data security breach to notify affected individuals.
- **Establish Effective Accountability and Enforcement**
  Effective enforcement must hold accountable *all* entities handling personal data to *equivalent* data privacy standards using the *same* enforcement mechanisms, thereby creating an even playing field and proper incentives across industry sectors to comply with those standards. Because "mistake-free" compliance is unlikely in this complex area of law, we support the approach adopted in all enacted state privacy laws of coupling *exclusive* governmental entity enforcement with the regulated entity's ability to "cure" non-compliant practices within a limited period of time after timely and specific notice from the governmental authority.

[1] MSPC's principles for federal privacy legislation are also available at: https://mainstreetprivacy.com/principles/

MSPC Testimony to Senate Subcommittee on Privacy, Technology and the Law

Appendix B

Comparison of Processor Requirements in Three Key State Privacy Laws that Set the New Standard

- The chart below compares the processor requirements in the three key state privacy laws that were enacted early and set the standard for processor requirements: Virginia, Colorado, and Connecticut. These states passed laws in 2021 and 2022, after California's 2018 California Consumer Privacy Act (CCPA), which *failed to establish* any data processor requirements to protect consumers' data.
- Without statutory processor requirements, small-business controllers would lack the bargaining leverage necessary (in contractual negotiations with much larger data processors) to require processors to ensure the privacy of the controller's customer data when in the processor's hands.
- These key state privacy laws established a strong model that influenced most other state privacy laws, which adopted similar processor requirements to protect consumer data.

✓=Required ☒=Not Required KEY STATES THAT REQUIRED PROCESSORS TO:	VIRGINIA CDPA (2021)	COLORADO CPA (2021)	CONN. SB 6, Sec. 7 (2022)
Ensure Processor's Own Data Security when handling Controller's personal data	☒	✓	☒
Assist Fulfilling Privacy Rights Requests from Individuals and w/ Data Breach Notices	✓	✓	✓
Give Info to Controller to Complete DPAs (Data Privacy Assessments) Required of Controller	✓	✓	✓
Ensure Confidentiality of Personal Data by Processors' Employees w/ Personal Data	✓	✓	✓
Hold Subcontractors to Processor's Terms / Give Controller the Right to Object to Subs	✓ / ☒	✓ / ✓	✓ / ✓
Return/Delete Personal Data at Contract End (at the Choice of the Controller)	✓	✓	✓
Provide Controller Compliance Info Needed to Demonstrate Processor's Legal Compliance	✓	✓	✓
Allow and Cooperate w/ Reasonable Audits or Assessments at the Request of Controller	✓	✓	✓
Respect Cross-Liability Protections (Parties Not Liable for Another Party's Violations of their Own Obligations under the Act)	✓	✓	✓

MSPC Testimony to Senate Subcommittee on Privacy, Technology and the Law

Appendix C

Data Privacy Frameworks Adopted by European Union and California, Compared to GLBA Applying to U.S. Financial Institutions

PRIVACY LAW COMPARISON CHART

Consumer Privacy Rights regarding their Personal Information	GDPR (2016)	CCPA (2018)*	GLBA (1999)	Notes
Transparency	✓	✓	!	GLBA: partial transparency; only annually-*mailed* disclosure notice of data uses (w/ some exceptions)
Control (Choices)	✓	✓	✗	GLBA: no meaningful control; opt out *only for* non-affiliate sharing that is not excepted (e.g., some marketing)
Access	✓	✓	✗	
Correction	✓	✓	✗	
Deletion	✓	✓	✗	
Portability	✓	✓	✗	
Breach Notification	✓	!	!	CCPA: CA breach law requires notice, but not CCPA GLBA: Not required (guidance *only* says "should" notify)
Opt-Out of Direct Marketing	✓	✗	✗	GDPR: opt out of processing for direct marketing GLBA: joint marketing agreements override opt-out
Opt-Out of Data Sharing for Targeted Ads	✗	✓	✗	CCPA: opt out of data sharing to third parties for purposes of processing data for targeted advertising
Opt-Out of Data "Sales"	✗	✓	✗	CCPA: opt out of data "sales" to third parties for purposes beyond marketing/advertising (w/ some exceptions)

**CCPA, as amended by CPRA (2020)*