April 7, 2025

The Honorable Brett Guthrie
Chairman
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, District of Columbia 20515

The Honorable John Joyce, M.D.
Vice Chairman
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, District of Columbia 20515

RE: Response to U.S. House Committee on Energy and Commerce Privacy Working Group Request for Information

Dear Chairman Guthrie and Vice Chairman Joyce:

ACT | The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. Today, the domestic app economy is worth more than $1.8 trillion annually and provides over 6.1 million American jobs.[1] We work with and for our members to promote a policy environment that encourages innovation while protecting consumer privacy and security.

App Association members are dedicated to improving the safety and security of products and services in the digital economy. The internet offers a wide array of tools and opportunities for consumers to achieve their goals, from financial planning to improving their health. However, this digital engagement necessitates the collection and exchange of significant amounts of personal and sensitive data, which must be properly protected. We appreciate the Working Group's attention to the urgent need for federal comprehensive privacy legislation and look forward to working with you to advance strong, balanced protections for consumer data.

To support the Working Group's efforts toward this essential goal, the following response outlines key considerations for developing a federal comprehensive privacy and security law. These include the roles and responsibilities of different entities, consumer rights, comparisons with existing privacy frameworks, data security concerns, state-level regulation of artificial intelligence, and accountability and enforcement mechanisms. The recommendations reflect the realities and needs of small and medium-sized technology companies and emphasize the importance of clear, scalable, and innovation-friendly policies that protect consumer data.

[1] ACT | The App Association, *State of the U.S. App Economy: 2023*, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf.

I. Roles and Responsibilities

Congress should tailor privacy obligations in federal legislation to reflect an entity's role in the data ecosystem and its capacity to comply. Legislation should differentiate between controllers, processors, and third parties based on the distinct roles each plays in handling consumer data. For example, processors, which act on behalf of controllers, do not have a direct relationship with consumers and should not be subject to the same obligations as controllers. A federal privacy framework should account for these differences and apply requirements proportionate to each entity's role and level of control over consumer data. Similarly, it should be understood that companies leveraging technology to solve problems are typically controllers for some activities, processors for others, and third parties in the remaining instances. Drafters should be sensitive to the complexity this introduces for small firms.

In addition, Congress should consider an entity's size and compliance capacity when determining appropriate obligations. Small businesses should be included within the scope of a federal comprehensive privacy law, as many collect and process consumer data in ways comparable to larger firms and seek clear, consistent rules for doing so. However, given that small businesses often lack the dedicated compliance resources of larger businesses, the law should include a scalable path to compliance that supports strong privacy protections while accounting for their limited capacity. Requirements should be calibrated based on a business's size, the scope of its data processing activities, and its practical ability to comply.

To this end, instead of a complete carve-out for small businesses from all provisions of a comprehensive federal privacy framework, drafters **should provide a "safe harbor" specifically for small businesses**, similar to the safe harbor framework for all covered entities under the Children's Online Privacy Protection Act (COPPA). A model also exists for this in an earlier version of comprehensive federal privacy legislation, the American Data Privacy Protection Act, or ADPPA. Such a safe harbor should provide for a process by which the Federal Trade Commission (FTC) can approve independent third parties to 1) develop compliance guidelines for qualifying small businesses by industry sector and 2) certify small businesses that volunteer to comply with those guidelines as following the underlying comprehensive privacy law. As outlined in ADPPA, certification would come along with periodic audits and reporting as necessary to ensure compliance. In return, small businesses would benefit from assistance with their compliance efforts and a presumption of compliance with the law if they are certified as complying with guidelines. This would give small businesses that want to and are able to comply with the law some assurance that good faith mistakes or misunderstandings can be ameliorated before being unnecessarily exposed to civil penalty liability.

II. Personal Information, Transparency, and Consumer Rights

Policymakers should ensure that a federal comprehensive privacy law is appropriately scoped to protect consumers' data without imposing undue regulatory burdens on businesses and developers. To that end, policymakers should rely on commonly accepted definitions for key terms. For example, "personal information" should be defined as data that can be reasonably linked to or used to identify a particular individual, such as their real name, postal or email address, or internet protocol (IP) address. Drafters should avoid definitions of "personal information" that sweep in information "linked or linkable" to a device. Including such information risks subjecting anonymized data to consumer rights, inadvertently causing reidentification and possible exposure of information intended to be protected by measures like anonymization. "Sensitive personal information" should be defined more narrowly and include identifiers such as precise geolocation information and *known* children's data.

A federal comprehensive privacy law should also provide consumers with rights that enable meaningful control over their personal information. These rights should include the ability to access, correct, or delete information, the right to data portability, the right to opt out of the sale of their data, and protection from discrimination for exercising these rights. The rights should operate as a requirement for businesses to respond to requests by consumers, subject to a couple caveats. For example, entities subject to the requirements must be required to verify the legitimacy of a consumer request, including verifying that the consumer is who they claim to be. Similarly, entities must be empowered to refuse manifestly unfounded requests or harassing request campaigns and to take additional time to respond, depending on the complexity of the request or requests at issue. In addition, a federal comprehensive privacy law should include heightened protections for sensitive personal information. For example, companies should be required to obtain affirmative, opt-in consent before processing sensitive data. However, protections for sensitive data should be carefully balanced to avoid impeding legitimate and beneficial uses of data or outweighing the countervailing benefits processing could offer.

Finally, a federal comprehensive privacy law should require companies to inform consumers as to how and for what purpose they collect, use, store, protect, and share data. Disclosures should be written in plain language with unambiguous terms and should clearly explain the company's data collection and processing activities.

III. Existing Privacy Frameworks and Protections

Congress should preempt the existing patchwork of state privacy laws with a uniform federal standard to reduce regulatory burdens on small businesses and protect innovation. To date, 20 states have enacted comprehensive privacy laws, each with its own set of requirements that businesses must follow to protect consumer privacy. Further, every state has enacted laws that touch on targeted privacy or security elements, such as health data, child-specific data, or data breach notification mandates. Complying with this growing web of disparate laws forces small businesses to divert limited resources away from hiring, research and development, and other critical functions, and toward costly compliance efforts. Indeed, in a 2022 report, the

Information Technology and Innovation Foundation estimated that state privacy laws could impose up to $23 billion on small businesses annually.[2] This dynamic effectively advantages larger companies that have the capacity to manage complex regulatory obligations while continuing to innovate and scale. While many state privacy laws include valuable provisions worth incorporating into a federal standard, Congress should wholly preempt them by enacting a single, uniform federal framework for protecting consumer privacy.

In addition, Congress should avoid replicating overly burdensome privacy laws that have stifled innovation. For example, in 2022, the U.S. National Bureau of Economic Research published a report examining the impact of the European Union's (EU) General Data Protection Regulation (GDPR) on innovation.[3] The authors found that the GDPR led to the exit of approximately one-third of available apps on the Google Play store and significantly reduced the number of available apps after its implementation. Some U.S. states, including California, have sought to emulate the GDPR in their own privacy laws. However, this approach is misguided and risks undermining innovation. Similarly, consumers do not benefit from conflicting privacy laws, particularly when they depend on consistent access to digital services and tools that offer privacy protections regardless of where they live or where the service provider is located. Congress should preempt such laws and avoid incorporating similarly restrictive provisions into a federal comprehensive privacy law.

Finally, Congress should ensure that a federal comprehensive privacy law does not override existing, specialized sectoral frameworks. Sectoral laws, such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and COPPA, reflect the distinct risks and operational realities of the industries or protected classes they govern. Rather than duplicating or conflicting with these laws, a federal comprehensive privacy framework should defer to them where applicable and preserve the strong, sector-specific protections they provide. For example, the framework should carve out organizations acting as covered entities or business associates under HIPAA to avoid overlapping regulatory obligations and ensure consistency in the protection of health data. Carving around each of these federal privacy silos will require thoughtful drafting. They are unique and have idiosyncratic characteristics that all but rule out plug-and-play rules of construction or exceptions. We further detailed why these carve-outs are so important in 2023 as a witness in the Commerce, Manufacturing, and Trade Subcommittee hearing, "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information."[4] We believe that although the silos serve an important function, a

[2] Castro, Daniel, et al. "The Looming Cost of a Patchwork of State Privacy Laws." *Information Technology and Innovation Foundation*, Information Technology and Innovation Foundation | ITIF, 24 Jan. 2022, itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

[3] Janßen, Rebecca, et al. "GDPR and the Lost Generation of Innovative Apps." *National Bureau of Economic Research*, National Bureau of Economic Research, May 2022, www.nber.org/system/files/working_papers/w30028/w30028.pdf.

[4] "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information." 2023,

comprehensive privacy law is needed in particular to apply a risk-based, flexible framework to sensitive personal information that falls outside each of those silos.

IV. Data Security

Congress should include robust but flexible cybersecurity mandates in a comprehensive federal privacy law. These mandates should require that businesses design cybersecurity programs that protect the security, privacy, confidentiality, and integrity of data against risks, such as the unauthorized access or use of the data or its unintended or inappropriate disclosure. Through their programs, businesses should build administrative, technological, risk management, and physical safeguards into their products and services to ensure that consumers' data remains secure and available only to authorized entities.

In addition, in a comprehensive federal privacy bill, policymakers should require that companies limit access to consumer data to only the employees or third-party service providers who require access to the data. Restricting access to consumer data secures it against unwanted intrusions from internal sources and provides another layer of security against potential malfeasance or data breaches caused by human error.

Finally, policymakers should include the principles of data minimization and purpose limitation in a comprehensive federal privacy bill by requiring that companies limit data processing to that which is necessary, proportionate, or limited in relation to the purposes for which the data is processed. However, data minimization must not fall into the trap of prohibiting any and all collection *unless* it meets strict requirements, as GDPR does. This would create a presumption that all collection is illegal, unless the data collection and use is specified by Congress. This construct creates unnecessary problems in the context of developing and iterating software-based products and services and is especially awkward for development, adaptation, and iteration of AI systems. Instead, data minimization should be flexible and require that companies limit data collection and retention in ways that are reasonably anticipated within the context of a company's ongoing relationship with an individual, or meeting a particular purpose identified publicly on a company's website or marketing materials. Including a data minimization provision could mitigate damage in the event of a cyber breach, as bad actors will only be able to access a minimal amount of consumer data.

V. Artificial Intelligence

Congress should preempt all corresponding state privacy laws, including provisions related to automated decision-making, with a uniform federal standard. However, federal privacy legislation should not attempt to replace or duplicate state-level AI frameworks, especially those that go beyond addressing privacy harms and venture into areas like imposing pre-market review on models in order to prevent potential harmful bias. Instead, Congress should maintain a clear focus on data privacy and security and

---

https://d1dth6e84htgma.cloudfront.net/IDC_Reed_Testimony_American_Data_Privacy_Hearing_2023_04_27_9fba684eb0.pdf?updated_at=2023-04-26T18:59:08.111Z.

ensure that consumers receive strong protections for their personal information. Broader efforts to regulate artificial intelligence should be addressed separately and deliberately, rather than folded into a privacy-focused law.

VI. Accountability and Enforcement

Effective enforcement of a federal comprehensive privacy law is essential to compel compliance and safeguard consumer data. To achieve this, Congress should ensure that both the FTC and state attorneys general are equipped with the authority necessary to investigate violations and hold bad actors accountable. Specifically, a comprehensive federal privacy law should clearly designate the FTC as the primary enforcer of the law. In preempting state comprehensive privacy laws, it should also authorize state attorneys general to enforce the federal law's provisions, including access to appropriate remedies and investigative powers, after notifying and coordinating with the FTC. Finally, the law should avoid authorizing the FTC to conduct rulemakings under the Administrative Procedure Act (APA), except if strictly necessary to interpret statutory concepts and only with clearly defined guardrails that combat efforts to expand the law's scope or purpose.

Similarly, Congress should not include a private right of action in a federal comprehensive privacy law. While intended to empower consumers, such provisions often open the door to opportunistic litigation. Many businesses may be forced to settle meritless claims or divert limited resources away from hiring, research and development, or other areas critical to growth.

Moreover, privacy law is still an evolving legal landscape. The first comprehensive state privacy law, the California Consumer Privacy Act, was passed in 2018, and courts across the country continue to interpret similar statutes in divergent ways. While a federal comprehensive privacy law could end the patchwork of differing state laws, introducing a private right of action may inadvertently create a new kind of patchwork through inconsistent judicial interpretations in different jurisdictions. Congress should avoid this outcome by excluding a private right of action from a federal comprehensive privacy law.

Finally, as described above, Congress should include a safe harbor provision in a federal comprehensive privacy law specifically for small businesses to promote compliance. As previously noted, small businesses lack the infrastructure, legal departments, and resources that larger companies have to comply with new laws. A safe harbor would give these businesses a clear path to compliance and protect them from penalties for mistakes made in good faith.

VII. Additional Information

In conclusion, a federal comprehensive privacy law should establish clear, consistent, scalable standards that protect consumer data and support innovation. To that end, the

law should reflect the four central pillars of the App Association's federal privacy priorities:

1. **Preemption**: A federal privacy framework should preempt related state laws so that small businesses do not have to contend with a patchwork of differing privacy laws.
2. **Protection Against Unauthorized Access**: A federal framework should include data security provisions that require businesses to prevent unauthorized access to consumer data.
3. **Path to Compliance**: Instead of carving small businesses out of a federal comprehensive privacy law, policymakers should include a path to compliance that helps them come into compliance while easing associated burdens.
4. **Private Right of Action Exclusion**: Policymakers should exclude a private right of action in a federal comprehensive privacy law to protect small businesses from opportunistic litigation that could divert critical resources away from growth and innovation.

Thank you for your time and consideration. We appreciate the Working Group's focus on developing an effective federal comprehensive privacy law and welcome the opportunity to provide additional comments or further engage as the legislative process moves forward.

Sincerely,

Graham Dufault
General Counsel
ACT | The App Association