June 1, 2026

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 Frank Pallone
Ranking Member
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, District of Columbia 20515

The Honorable Gus Bilirakis
Chairman
U.S. House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, District of Columbia 20515

The Honorable Jan Schakowsky
Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, District of Columbia 20515

RE: ***Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law***

Dear Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky, and Members of the Committee:

Thank you for the opportunity to submit testimony for the record on your hearing titled, *Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law*.[1]

The Association for Competitive Technology (ACT) represents small business innovators and startups in the software development and high-tech space in the United States and around the world. As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping consumers lead healthier lives. Today, the

[1] "Chairmen Guthrie and Bilirakis Announce Hearing on Establishing a Federal Data Privacy Law." *House Committee on Energy and Commerce*, energycommerce.house.gov/posts/chairmen-guthrie-and-bilirakis-announce-hearing-on-establishing-a-federal-data-privacy-law. Accessed 31 May 2026.

domestic app economy is worth more than $1.8 trillion and provides over 6.1 million American jobs.[2]

The Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act) represents a thoughtful and balanced approach to protecting consumers' personal information and supporting small businesses in the digital economy. Small businesses increasingly operate in a digital economy where customers, business partners, and vendors expect strong privacy and cybersecurity practices. As a result, the framework Congress establishes for consumer privacy will shape the compliance expectations and marketplace standards all small businesses encounter, regardless of whether they meet the applicability thresholds detailed in the bill.

As the Committee debates this proposal, policymakers should ensure that any final bill reflects the Four Ps of Privacy: path to compliance, preemption, no private right of action, and protection against unauthorized access. First, the bill should offer small businesses a mechanism to achieve compliance that recognizes their size and limitations. Second, comprehensive federal privacy legislation should preempt the current patchwork of state privacy laws to establish a single uniform standard for protecting consumer privacy. Third, the bill should exclude a private right of action to protect small businesses from opportunistic litigation. Fourth, including strong cybersecurity provisions will ensure that consumer data entrusted to small businesses remains protected from hacking or misuse. As currently drafted, the SECURE Data Act advances each of these objectives by establishing a preemptive national framework that provides businesses with a clear path to compliance, promotes consumer protection, strengthens data security, and creates greater regulatory certainty.

Why Congress Should Enact a Comprehensive Federal Privacy Law

For small businesses, a federal privacy framework would provide meaningful certainty and predictability. Unlike large corporations with dedicated legal and compliance teams, small businesses often lack the time and resources necessary to track and comply with dozens of inconsistent state privacy laws. A single federal standard that preempts this state patchwork will enable small businesses to focus on serving customers, hiring employees, and growing their businesses instead of navigating a complex, costly regulatory landscape.

Moreover, a comprehensive federal privacy law would enable competition in the digital economy. Regulatory fragmentation disproportionately burdens smaller and newer market entrants, which typically have fewer resources to devote to compliance than their larger counterparts. By establishing a uniform set of rules, policymakers can reduce barriers to entry and create a more level playing field.

Finally, consumers would benefit from a federal comprehensive privacy law through the creation of consistent and enforceable privacy rights. Under the current state patchwork, consumers' privacy rights may vary depending on which state they live in. A national framework would ensure that consumers can receive and exercise the same protections regardless of their zip code and enable small businesses to better protect their customers.

---

[2] "State of the App Economy." *ACT | The App Association*, ACT | The App Association, actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf. Accessed 13 Jan. 2026.

Path to Compliance
Among the SECURE Data Act's strongest features is its voluntary code of conduct framework. This provision would enable small businesses who do not meet the applicability threshold to publicly self-certify their compliance with an approved and independently administered code of conduct designed to be cost-effective and appropriate for participants' size, risk profile, and operational limitations. In return, small businesses would receive a rebuttable presumption of compliance. This structure offers small businesses a clear, affordable, and credible path to demonstrating compliance with a recognized standard.

Publicly self-certifying to compliance also enables small businesses to compete in the digital economy. Many of ACT's members operate in a business-to-business marketplace where larger companies routinely require their vendors, processors, subcontractors, and service providers to meet specific privacy obligations before winning a contract. Public participation in an approved code of conduct offers a standardized way to prove readiness and compete for opportunities. In fact, in a 2026 Data and Privacy Benchmark Study, Cisco found that 96 percent of survey respondents reported that external, independent privacy certifications influence vendor selection decisions.[3] In a marketplace where privacy and security expectations increasingly influence purchasing decisions, a recognized certification provides small businesses with a competitive advantage.

Further, the code of conduct framework offers small businesses flexibility instead of a one-size-fits-all mandate. Because participation is voluntary, small businesses can assess whether an approved code of conduct aligns with their operations, customer base, and growth plans, and opt in accordingly. As a result, a business operating primarily in a single state can avoid taking on federal obligations that do not reflect its customers' expectations or business operations.

Preemption
Importantly, the SECURE Data Act includes a robust preemption standard that would replace the current patchwork of state privacy laws with a uniform national framework for comprehensive privacy protection. Establishing this single federal standard would provide consumers with consistent rights and protections while also giving small businesses a clear and predictable compliance environment.

To date, 22 states have enacted their own comprehensive privacy laws and two more are expected to do so within the coming weeks.[4] While many of these laws share a common structure, they differ in key provisions, including applicability thresholds, definitions, enforcement mechanisms, and obligations. Although state privacy laws set applicability thresholds to carve small businesses out, some states, such as Connecticut and Montana, have recently amended their laws to lower applicability thresholds and expand the number of businesses captured by their laws. As a result, even businesses that do not currently meet

[3] *Cisco 2026 Data and Privacy Benchmark Study*, www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2026.pdf. Accessed 31 May 2026.
[4] "S.71." *State House Dome*, legislature.vermont.gov/bill/status/2026/S.71. Accessed 1 June 2026.; "SB386," www.legis.la.gov/legis/BillInfo.aspx?s=26rs&b=SB386&sbi=y. Accessed 1 June 2026.

applicability thresholds must devote resources towards monitoring legislative updates and determining whether new changes will bring them within the scope of state comprehensive laws.

This increasingly fragmented regulatory landscape imposes significant costs on small- and medium-sized businesses. Instead of focusing on growth, hiring, and innovation, small businesses must expend limited time and resources on tracking legislative changes, obtaining legal guidance, and implementing compliance programs. In a 2022 report, the Information Technology and Innovation Foundation estimated that a 50-state privacy patchwork could impose up to $23 billion in compliance costs on small businesses.[5] By preempting the growing patchwork of state privacy laws with a single national standard, the SECURE Data Act would reduce unnecessary compliance burdens and allow small businesses to focus their resources on serving their customers and competing in the digital economy.

No Private Right of Action

The SECURE Data Act's enforcement framework effectively balances strong consumer protections with safeguards against unnecessary litigation. By empowering the Federal Trade Commission (FTC) and state attorneys general with enforcement authority instead of creating a private right of action, the bill ensures accountability against malfeasance while protecting small businesses from opportunistic litigation.

While well-intended, private rights of action can incentivize litigation without meaningfully advancing consumer privacy. In practice, private rights of action encourage "sue-and-settle" business models in which plaintiffs' firms file or threaten meritless lawsuits in order to extract settlements from businesses. While large businesses may be able to absorb these costs as routine expenses, small businesses often lack the financial resources to defend against baseless claims. Faced with the prospect of costly litigation, many small businesses may instead choose to settle such claims and pay opportunistic litigants.

A broad private right of action may also undermine the goal of establishing a single national framework for consumer privacy. Private rights of action can produce inconsistent judicial interpretations across jurisdictions, which ultimately creates uncertainty regarding compliance obligations and exposes small businesses to inconsistent legal standards. Over time, this fragmentation will replicate many of the challenges associated with the current state-by-state patchwork.

Instead of relying on a private right of action, the SECURE Data Act's enforcement model mirrors the models included in state privacy laws. Of the 22 states that have enacted comprehensive consumer privacy laws, only California includes a limited private right of action, primarily in the context of certain data breaches. Legislatures across the political spectrum have overwhelmingly chosen to empower attorneys general and other designated regulators with enforcement. By following this approach, the SECURE Data Act promotes consistent and effective enforcement of consumer privacy rights while avoiding the costs, uncertainty, and opportunistic litigation associated with a private right of action.

---

[5] Castro, Daniel, et al. *The Looming Cost of a Patchwork of State Privacy Laws*, www2.itif.org/2022-state-privacy-laws.pdf. Accessed 31 May 2026.

Protection Against Unauthorized Access
The SECURE Data Act appropriately includes strong cybersecurity requirements for businesses, and requires them to establish and maintain reasonable administrative, technical, and physical safeguards that are tailored to the volume, sensitivity, and nature of the data they process. By adopting this risk-based standard, the bill promotes strong cybersecurity practices that reflect the operational realities small businesses face across sectors.

Further, by linking a rebuttable presumption of compliance to adherence with an approved code of conduct, the SECURE Data Act creates meaningful incentives for businesses to adopt strong cybersecurity practices and invest in proactive data security measures. This framework enables small businesses to protect consumer data, promotes the adoption of effective cybersecurity measures, and allows enforcement resources to be focused on bad actors and genuinely deficient security practices.

Age Assurance Concerns
Section 2(b)(3) of the SECURE Data Act would prohibit a controller from processing any sensitive data of an individual between the ages of 13 and 15 without first obtaining "verifiable consent." Because this provision would impose a blanket prohibition on processing sensitive data pertaining to these individuals based on their age—absent verifiable consent from a guardian—age estimation and less privacy-intrusive forms of age assurance may be insufficient. As discussed further below, all controllers subject to the SECURE Data Act may face an obligation to conduct riskier forms of age assurance, such as age verification, either in-house or through a third-party processor.

Except when used to validate eligibility for discounts or similar benefits, age assurance techniques are typically deployed as a means of addressing age-related risks—either to restrict access by individuals under a certain age to content that poses foreseeable risks related to users' ages, or to direct individuals to age-appropriate experiences. Services that are not designed to make age-inappropriate content available or expose children and teens to age-related risks do not use age assurance techniques. Doing so presents privacy and security risks associated with age assurance, without providing an age-related risk mitigation benefit. Given the broad definition of "sensitive data" to any information that is "linked or linkable" to a teen, Section 2(b)(3)'s obligation appears to require all controllers that happen to have a teen as a user to conduct age verification. For example, if a 14-year-old downloads an app made by an ACT member, the ACT member would have to conduct age verification for all of their users in order to comply with this provision, regardless of whether they provide age-inappropriate content for 14-year-olds.

Section 2(b)(3)'s requirement to obtain "verifiable consent" from a parent of a teen would compound the privacy risks of age verification alone, by obligating all controllers with a teen user to associate teen profiles with parent profiles. The existing Children's Online Privacy Protection Act (COPPA) imposes a similar obligation to obtain "verifiable parental consent" from guardians of children under 13. As a practical matter, the requirements as applied are formidable for small businesses. COPPA's saving grace is that it only applies to services that are either intentionally directed to children under 13 or to services with "actual knowledge" of a child's under-13 status. This has helped prevent the application of COPPA's prohibitive compliance and liability regime to barber shops and restaurant chains with scheduling and

ordering apps. Unfortunately, Section 2(b)(3) would likely expand COPPA-style obligations to all apps on the stores and services on the internet. As a result, unintended liability exposure and compliance hurdles would hamper innovation and job creation by small business innovators, while also posing unnecessary privacy risks in the form of big data honeypots required to conduct age verification for all users and associating teen accounts with parent accounts. We urge the Committee to work with ACT on targeting any measures intended give parents more meaningful oversight of their teens' online experience, without producing these unintended consequences. The Parents Over Platforms Act (POPA, H.R. 6333), which the Subcommittee approved unanimously in December 2025, would be a good start with respect to apps on the major stores, since it would apply age assurance obligations in a risk-based manner to services that are differentiated between adults and minors.

Conclusion

As Congress debates the SECURE Data Act, it should preserve the key features that make the bill a balanced and workable framework: a clear path to compliance, robust preemption, regulator-led enforcement without a private right of action, and strong protections against unauthorized access. Together, these provisions would protect consumer privacy while ensuring that federal privacy legislation remains practical for the small businesses and startups that drive innovation in the digital economy.

Thank you for your time and consideration. We appreciate the Subcommittee's focus on federal comprehensive privacy legislation and welcome the opportunity to further engage as the legislative process moves forward.

Sincerely,

Morgan Reed
President
Association for Competitive Technology