Kentucky Chamber
Uniting Business. Advancing Kentucky.

WRITTEN TESTIMONY OF

ASHLI WATTS

President and Chief Executive Officer
Kentucky Chamber of Commerce

Before the
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
United States House of Representatives

Hearing on
"Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law"
H.R. 8413, the SECURE Data Act (Rep. Joyce, PA)

June 3, 2026

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

I. Introduction

Thank you for the opportunity to testify before this Subcommittee today. My name is Ashli Watts, and I am the President and Chief Executive Officer of the Kentucky Chamber of Commerce. I am a Kentuckian. I have spent my career working alongside the businesses, communities, and leaders that make this Commonwealth run — and I appear before you today as a voice for the employers and entrepreneurs across Kentucky who are directly affected by the policy questions this Subcommittee is considering. I also currently serve as Chair of the U.S. Chamber of Commerce Committee of 100 —representing the chief executives of America's largest state and metropolitan chambers of commerce. Through

this group, we work closely with the U.S. Chamber, which provides exceptional leadership on federal policy issues like this one and serves as an invaluable resource for chambers across the country to engage, share best practices, and align on the policies that matter most to American businesses. The SECURE Data Act is a powerful example of that partnership in action. That perspective informs everything I will share with you today.

The Kentucky Chamber is the Commonwealth's largest business advocacy organization, representing a broad and deeply engaged membership of companies of every size and sector who collectively employ hundreds of thousands of Kentuckians. The Kentucky Chamber has a long history of convening diverse stakeholders to find workable solutions on the issues that matter most to Kentucky's economy — and House Bill 15, Kentucky's comprehensive consumer data privacy law, is proof of that. That same convening spirit is reflected at the national level, where the U.S. Chamber has brought together more than 120 state and local chambers of commerce — including the Kentucky Chamber — in unified support of the SECURE Data Act. That experience is what brings me before this Subcommittee today, and it is why we believe so strongly that federal action is the necessary and urgent next step.

I am here today in strong support of H.R. 8413, the SECURE Data Act. Chairman Guthrie and Chairman Bilirakis, you deserve the thanks of the business community — and the thanks of every Kentucky employer — for your leadership in bringing this legislation forward alongside bill sponsor Representative Joyce. The work of this Subcommittee on a national data privacy standard is long overdue, and the framework before us today represents the right path forward.

II. Kentucky's Experience

To understand why the SECURE Data Act matters, it helps to understand what Kentucky built — and what we learned from building it.

House Bill 15 was the product of an intensive coalition process. The Kentucky Chamber played an important role as a convener, bringing together stakeholders from across industry sectors, business organizations, retailers, and privacy, security, and technology experts to negotiate a workable solution. The result was a law that passed the General Assembly with unanimous support of a super-majority Republican legislature and was signed into law by Democratic Governor Andy Beshear in 2024. The goal was straightforward: give consumers the right to protect their data while maintaining an environment in which Kentucky businesses can operate and compete.

What made that process work was a shared commitment to a framework that was strong on consumer protections and workable for business. That is exactly what the SECURE Data Act reflects at the federal level.

The SECURE Data Act provides Americans with a strong set of consumer rights: the right to access their personal data, the right to correct inaccuracies, the right to delete data, the right to data portability, and the right to opt out of data sales, targeted advertising, and profiling. For sensitive data, the bill requires opt-in consent. It applies a reasonable data minimization standard and includes meaningful child and teen protections. Kentucky's House Bill 15 reflects this same framework — which is precisely why the Kentucky Chamber supports it. We are not being asked to accept something new or untested. We are being asked to extend to all Americans what Kentucky and many other states have already put into law.

Critically, Kentucky's law was designed to align with the framework adopted by Virginia, Indiana, Tennessee, and a growing number of states. That alignment was intentional. Kentucky businesses do not just operate in Kentucky. They sell across state lines, hire across state lines, and compete across state lines. Aligning with other states was the only sensible path — and it is the same path this legislation asks Congress to take nationally.

III. The Patchwork Is Not a Solution

When every state writes its own law, even good policy creates a patchwork. Today, over twenty states have enacted comprehensive data privacy laws, each with its own definitions, obligations, and enforcement mechanisms. For a business operating across state lines — even a small business with an online presence — that means navigating a different set of rules in every market they touch. The majority of the businesses the Kentucky Chamber represents are small businesses — and no business should have to navigate a 50-state compliance landscape just to protect their customers' data. Small businesses in particular often lack in-house legal teams, chief privacy officers, or large compliance budgets.

The U.S. Chamber's The Impact of Technology on U.S. Small Business report makes the stakes plain: nearly two-thirds of small businesses are worried that having to comply with different state laws on privacy, AI, and technology in states where they are not headquartered will expose them to higher compliance and litigation costs — a figure that jumped fourteen percentage points in a single year. Three-quarters of small businesses say that limiting their access to data would harm their operations.[1] These are not abstract concerns. They are the daily reality of Kentucky employers trying to run their businesses and keep their doors open.

A fragmented privacy landscape is estimated to cost the U.S. economy as much as $1 trillion over ten years, with $200 billion of that burden falling on small businesses.[2] That

[1] U.S. Chamber of Commerce, "Empowering Small Business: The Impact of Technology on U.S. Small Business," 2025, available at https://www.uschamber.com/assets/documents/20251621-CTEC-Empowering-Small-Business-Report-2025-v1-r10-Digital-FINAL.pdf.

[2] ITIF, "The Looming Cost of a Patchwork of State Privacy Laws," January 2022, available at https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.

is not a compliance challenge. That burden falls hardest on the businesses least equipped to absorb it.

IV. The SECURE Data Act Is Built on Proven, Bipartisan Foundations

The SECURE Data Act does not ask Congress to invent something new. It asks Congress to codify what the states have already proven works. Strong consumer privacy protections and economic growth are not competing goals. They reinforce each other. When customers trust that their information is being handled responsibly, they are more willing to engage, transact, and participate in the digital marketplace. Clear rules help build that trust.

The SECURE Data Act is built on the Consensus Privacy Approach — the same framework that Kentucky, Virginia, Indiana, Tennessee, New Jersey, and a growing number of states have enacted into law. As detailed in Section II, the bill is functionally aligned with the core protections in these state laws, including the strong consumer rights, opt-in requirements for sensitive data, child and teen protections, and a reasonable data minimization standard. This is not a new or untested framework. It is the approach that twenty states have already chosen, that lawmakers and governors of both parties have supported across the country— protecting more than 135 million Americans today.[3]

The bill also follows the Kentucky approach with respect to small businesses. A food truck or an independent coffee shop does not have a team of compliance lawyers and privacy consultants. For this reason, Kentucky's privacy law is limited to companies that process data of over 100,000 Kentuckians or derive a significant amount of revenue from selling consumer data. The SECURE Data Act follows this same approach. With the SECURE Data Act's strong language that preempts state laws "related to the provisions of this Act," small businesses will not be subject to a patchwork of state laws.

The bill's enforcement framework reflects the same approach Kentucky and other states have taken — placing authority with government regulators rather than opening the door to private litigation. That is a model the Kentucky Chamber supported in Frankfort, and it is one we believe works.

V. A Single National Standard Is Not a Weakness — It Protects Everyone

Some have argued that replacing state privacy laws with a single national standard will leave consumers with weaker protections than they have today.

Kentucky's House Bill 15 is a strong privacy law, and the SECURE Data Act is built on this same framework — and it is already working for Kentucky consumers and businesses. The argument that a national standard weakens protections assumes that more laws mean

[3] U.S. Chamber of Commerce Technology Engagement Center, "The SECURE Data Act Is Based on Bipartisan Consensus," 2026 (infographic). State population total reflects 20 states using July 1, 2025 U.S. Census Bureau estimates.

more protection. What our members tell us is different. More laws mean more confusion, more cost, and more uncertainty — none of which makes a single Kentucky consumer's data more secure.

Think about what a single national standard actually means for a small manufacturer in Elizabethtown or a retailer in Bowling Green who sells online. Today, that business potentially has to navigate over twenty different state privacy regimes — each with its own rules, timelines, and obligations. For example, if that Bowling Green online retailer wanted to expand its e-commerce business to California residents, she may be exposed to over $16,000 annually in compliance costs as a result of one rulemaking alone.[4] One national standard does not take rights away from that business owner's customers. It gives that business owner one clear set of rules to follow so they can focus on running their company rather than managing legal exposure. And their customers end up with the same strong consumer protections — enforced consistently and accountably. That is not a weaker standard.

The SECURE Data Act does not replace stronger protections with weaker ones. It embraces an already strong standard and establishes one clear, enforceable national standard that every American can count on.

VI. On Enforcement: Government Authority Is the Right Model

The SECURE Data Act places enforcement with government regulators rather than creating a private right of action. Every state that has passed this type of legislation has made the same choice. During our work on House Bill 15, our members supported this approach because it produces consistent, meaningful outcomes for consumers and businesses. Kentucky chose that model, and we believe it is the right model for federal law.

This model is the correct because it has empowered expert agencies like the Federal Trade Commission and state Attorneys General to engage in collaborative compliance that protects privacy and innovation. This approach contrasts with private rights of action which encourage an adversarial approach to privacy where lawyers allege technical violations of laws without showing real harm to consumers. In the end these suits do not provide significant benefits to consumers. Examples like this include my neighboring state of Illinois where the trial bar has abused the Biometric Information Privacy Act which provides for statutory damages even where there is no real harm to consumers. As a result, Illinois residents have reduced access to web services. In California, the trial bar has taken a privacy law, the California Invasion Privacy Act, which was meant for telephone calls and sued restaurants, retailers, and hospitals for legitimately collecting

[4] *See* Economic Impact Assessment for CCPA Updates, Cyber, Risk, ADMT and Insurance (2025) *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_eis.pdf.

data to maintain websites and advertise. Private rights are action are used to target small businesses in particular who are incentivized to settle cases as opposed to engaging in costly litigation. For this reason, the SECURE Data Act gets it right by giving sole enforcement authority to government agencies which are incentivized to go after bad actors.

VII. What This Means for Kentucky's Economic Future

I want to close by bringing this back to what is at stake for Kentucky. From the perspective of the Kentucky business community, this is not just a technology policy issue — it is a competitiveness issue. It affects whether Kentucky businesses can confidently adopt new tools, reach new customers, and participate fully in the modern economy.

Our businesses are increasingly dependent on data to serve their customers and stay competitive. The Kentucky Chamber has made it a legislative priority to ensure that our regulatory environment supports this growth. A clear, consistent national privacy standard is essential to that goal. Overly burdensome or conflicting state mandates create compliance uncertainty that gets in the way of business investment and growth. The SECURE Data Act provides the clarity Kentucky's economy needs.

Ninety-nine percent of Kentucky's small businesses already use at least one technology platform to operate. Seventy-four percent plan to increase that investment in the next two to three years.[2] These statistics are a picture of an economy in transition — one that depends on data to function, on technology to compete, and on clear, stable rules to invest with confidence.

The Kentucky Chamber urges this Congress to pass the SECURE Data Act and give Kentucky businesses and consumers the clear, consistent national standard they deserve.

VIII. Conclusion

Chairman Guthrie, Chairman Bilirakis, Ranking Member Pallone, Ranking Member Schakowsky, and Members of the Subcommittee: The model is proven, the consensus is bipartisan, and the work at the state level is done. What remains is federal action.

The SECURE Data Act offers American consumers a strong, uniform set of privacy rights. It offers American businesses the clarity and consistency they need to innovate, compete, and grow. It replaces a costly and confusing patchwork of state laws with a single national standard.

---

[2] U.S. Chamber of Commerce, "Empowering Small Business: The Impact of Technology on U.S. Small Business," 2025, available at https://www.uschamber.com/assets/documents/20251621-CTEC-Empowering-Small-Business-Report-2025-v1-r10-Digital-FINAL.pdf.

I urge this Subcommittee and the full Congress to pass the SECURE Data Act. The Kentucky Chamber of Commerce, the U.S. Chamber of Commerce, and our more than 120 state and local chamber partners across the country stand ready to support you in that effort.

Thank you. I look forward to your questions.

Ashli Watts

President & CEO, Kentucky Chamber of Commerce

Testimony submitted for the record — June 3, 2026