Hearing on
Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law

House Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade

June 3, 2026

Testimony of Kate Goodloe
Managing Director
Business Software Alliance

Testimony of Kate Goodloe,
Managing Director of Business Software Alliance

Hearing on Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law

Before the House Energy and Commerce Committee,
Subcommittee on Commerce, Manufacturing, and Trade

June 3, 2026

Good morning Chair Bilirakis, Ranking Member Schakowsky, Chair Guthrie, Ranking Member Pallone, and members of the Subcommittee. My name is Kate Goodloe, and I am Managing Director at the Business Software Alliance (BSA).

BSA represents the business-to-business technology providers that support companies in every sector of the economy.[1] Privacy and security are core issues for our members, which is why we are deeply engaged on privacy legislation in the United States, including in state capitals and around the world. Companies of all sizes and all industries — including manufacturers, automakers, hotel chains, and energy companies — rely on business-to-business tools like cloud computing, collaboration software, customer service platforms, and cybersecurity services. BSA members provide these technologies so that other businesses can focus on what they do best: making products and serving customers.

The United States needs a national privacy law built for the modern economy — one that pairs strong consumer protections with clear rules that limit how companies can use consumers' personal data. We welcome your focus on this issue and thank you for the opportunity to testify.

This Committee has led the work in Congress to advance comprehensive consumer privacy legislation and we commend you for this leadership. Today, we urge you to continue that work — and to leverage progress made by states in recent years. As you examine legislation to establish a federal comprehensive privacy and data security law, I want to emphasize three key points.

First: The Secure Data Act adopts the right structure for protecting consumer privacy nationwide, grounding it in the experience of the states. Twenty-two states — both red and

[1] BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

blue — have enacted consumer privacy laws. These laws are remarkably consistent, because 21 share the same core structure, with a common set of definitions, rights, and obligations. The Secure Data Act:

- Uses the same structure of privacy legislation that has widespread bipartisan support in the states, anchoring 21 of the 22 state privacy laws.
- Includes a core set of rights for consumers, based on a broad consensus that consumers should have rights to access, correct, and delete their data — and rights to opt out of activities like sale of their data, targeted advertising, and certain profiling.
- Leverages state laws to create clear obligations for companies.

In the past, efforts to draft comprehensive federal privacy legislation started from a blank slate, without the benefit of a consensus to emerge from the states. But the landscape of American consumer privacy laws is no longer blank. Four years ago, when this Committee advanced a comprehensive privacy bill to the full House of Representatives, just one state privacy law was in effect. Today, 22 states have acted. Grounding federal privacy legislation in the structure already widely adopted across the states is a critical step.

Second: The Secure Data Act reflects the modern economy. It adopts the longstanding, widespread distinction between controllers and processors to ensure the bill's obligations fit companies across the modern supply chain. Nearly every consumer-facing company today relies on a network of other businesses, including business-to-business technology providers that power a company's everyday operations. Each company that handles a consumer's personal data should be required to do so responsibly. The Secure Data Act creates obligations for both controllers, which decide why and how to process consumers' data, and processors, which handle data on behalf of other companies. Recognizing the roles of controllers and processors ensures that companies are subject to obligations that reflect their role in handling consumers' data.

Third: Consumer privacy is a national issue that requires a national solution. Consumers nationwide should have rights over their personal data — and companies should be required to use that data responsibly, no matter where a consumer lives. Companies should not have to track 50 moving goalposts to do business in the United States. And consumers should not have to live in one of 22 states to have privacy rights. The United States needs a single, clear set of rules that limits how companies collect and use data, so consumers trust their data is used responsibly.

We urge you to continue this important work. Of course, in order for any federal privacy bill to pass into law it will need to have bipartisan support. As this bill moves through the process, we hope that the text can become a bipartisan product.

There is reason to be hopeful. The core structure of the Secure Data Act has been adopted in privacy laws across blue and red states. Ten Democratic governors and 11 Republican governors have signed privacy bills with this structure into law. We look forward to working with both sides of the aisle as the bill moves forward.

We appreciate this Subcommittee's leadership on passing federal privacy legislation and we urge you to move the Secure Data Act through the legislative process to promote technology adoption across the economy and protect American consumers nationwide.

I. The Secure Data Act Adopts the Right Structure for Protecting Consumer Privacy.

The Secure Data Act adopts the right structure for protecting consumer privacy, drawing on the experience of states.

Twenty-two states — both red and blue — have adopted comprehensive consumer privacy laws. These state laws create a remarkably consistent framework, because 21 of the 22 laws share the same structure.[2] Although California took the important step of adopting the first state comprehensive consumer privacy law in 2018, no other state has copied its model for privacy legislation. All 21 of the other state privacy laws start from the same core structure — with a shared approach to definitions, rights, and obligations. In some cases, these newer laws create more consumer rights than California's law.

Despite sharing the same structure, these newer state privacy laws are not the same.

Lawmakers across those 21 states have started with the same structure for privacy legislation — then added and subtracted substantive provisions to reflect their different policy choices. As a result, there are important variations across the state laws. The Secure Data Act builds on that work to create a national standard for protecting consumer privacy.

[2] *See* BSA, "Models of State Privacy," last updated May 2026, *available at* https://www.bsa.org/policy-filings/us-2026-models-of-state-privacy-legislation.

a. The Secure Data Act is Grounded in State Laws.

Over the past four years, states have established the American model for protecting consumer privacy.

- In July 2022, this Committee advanced a comprehensive privacy bill to the full House of Representatives. At that time, California was the only state with a comprehensive consumer privacy law in effect.
- In April 2024, nearly two years later, lawmakers released a discussion draft of a new version of comprehensive privacy legislation. By then, five comprehensive state privacy laws had entered force, with new laws in Colorado, Connecticut, Virginia, and Utah.
- Now, in June 2026, 22 states have acted. New laws have entered force in Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, and Texas. Next year, laws in Alabama and Oklahoma will take effect.

The Secure Data Act takes the critical step of grounding federal privacy legislation in the structure already used by these state privacy laws. This enables consumers, companies, and lawmakers to more readily compare the bill's substantive protections with existing state rights and obligations. For companies, that makes it easier to identify new federal requirements or to recognize obligations that may be satisfied through existing compliance programs. For consumers, it is easier to understand if a new federal bill creates the same rights their state law already provides — or lacks. Lawmakers, too, can more readily contrast the Secure Data Act with laws in their state or region that share the same structure, to know how it would affect their residents and businesses.

b. The Secure Data Act Creates Core Rights for Consumers.

Consumers should have rights over their personal data no matter what state they live in. The Secure Data Act adopts core rights created by 22 state laws and extends them to consumers nationwide — giving all American consumers the right to access, correct, delete, and port their personal data. It would also give consumers nationwide the right to opt out of certain activities, like targeted advertising, sales of their data, and profiling.

There is widespread agreement that these rights are core components of an effective privacy law. At the state level:

All 22 comprehensive state consumer privacy laws create rights for consumers over their personal data. These include:

- Right to access personal data (22 states)
- Right to correct personal data (21 states)
- Right to delete personal data (22 states)
- Right to data portability (22 states)

All 22 laws also create rights for consumers to opt out of certain activities. These include:

- Right to opt out of sale of personal data (22 states)
- Right to opt out of targeted advertising (21 states)
- Right to opt out of certain types of profiling (19 states)

The Secure Data Act would extend these rights to American consumers in the 28 states that have not adopted comprehensive consumer privacy laws. It also recognizes common sense limits on exercising those rights, just as state laws recognize. For example, a consumer's right to delete data should not override a company's legal requirement to retain certain data. Nor should honoring the rights of one consumer create privacy or security risks to others.

c. The Secure Data Act Creates Clear Obligations for Companies.

Companies should be required to handle consumers' personal data responsibly. The Secure Data Act leverages foundational obligations in state consumer privacy laws to require companies to:

- Keep data secure by establishing data security practices that protect the confidentiality and integrity of personal data
- Get a consumer's consent to process sensitive data, like data that reveals someone's religious beliefs or immigration status
- Tell consumers how they will use personal data — and limit the reuse of that data
- Not process personal data in violation of anti-discrimination laws
- Not retaliate against consumers who exercise their new rights
- Disclose if they:
    - Sell a consumer's data
    - Process a consumer's data for targeted advertising
    - Rely on profiling to make important decisions about a consumer

- Explain how consumers can exercise their rights to opt out of sales, targeted advertising, and profiling decisions

In several cases, the Secure Data Act goes beyond requirements imposed in existing state privacy laws. These include:

- Requiring affirmative consent to process sensitive data. This requirement is found in 18 state laws, but goes beyond California's law, which only creates a limited right for consumers to opt out of certain uses of sensitive data. Laws in Iowa and Utah also do not require affirmative consent to process sensitive data.
- Requiring companies to establish a process for consumers to appeal denials of rights requests. This requirement is found in 19 state laws but is not required in California, nor by privacy laws in Alabama or Utah.
- Prohibiting companies from processing data in violation of anti-discrimination laws. Nineteen state privacy laws prohibit processing data in violation of anti-discrimination laws, but this prohibition is not contained in laws in California, Alabama, or Utah.
- Creating a data broker registry, which goes beyond the typical elements included in state consumer privacy laws.

These obligations are grounded in existing state privacy laws, extending clear rules for handling consumers' data to companies nationwide.

II. The Secure Data Act Reflects the Modern Economy.

The Secure Data Act reflects today's modern economy, where one company often relies on a network of other companies to provide products and services to consumers. Importantly, it clearly distinguishes between controllers and processors and assigns obligations to both types of companies reflecting their different roles in handling consumers' data.

a. Consumer-Facing Companies Rely on Business-to-Business Providers.

Across every sector of the economy, companies large and small hire business-to-business providers to power their everyday operations.

For example, a manufacturing company that serves customers nationwide will rely on a network of business-to-business software companies. One vendor may provide ticketing software that tracks engineering, maintenance, and compliance tasks. Another may provide customer relationship management software so the manufacturer can organize information about its

customers. A third may store the manufacturer's data in the cloud, so the data is secure and accessible across multiple offices. A fourth may secure the company's network against intruders and other cybersecurity risks.

Companies generally do not handle these everyday activities in-house because they focus on delivering the products and services their customers want. Instead, they rely on networks of business-to-business providers for the tools that help them manage the everyday aspects of running a business. That lets the company focus on what it does best — whether that is operating a national grocery store, managing a regional chain of fitness centers, or manufacturing custom-built furniture.

Every company in the modern supply chain may handle a consumer's personal data — and each one should be subject to important limits in how it can use consumers' data, based on its role in handling that data.

b. The Secure Data Act Adopts the Longstanding and Widespread Distinction Between Controllers and Processors.

The Secure Data Act creates obligations that fit companies across the modern economy by adopting the longstanding and widespread distinction between controllers and processors.

- **Controllers** decide why and how to collect a consumer's personal data. The Secure Data Act defines them in line with global laws, as a person that, alone or jointly with others "determines the purpose and means of processing personal data."
- **Processors**, in contrast, don't make those decisions, as state and global laws recognize. Rather, as the Secure Data Act makes clear, a processor "processes personal data on behalf of a controller" and pursuant to its instructions.

The distinction between controllers and processors dates back more than 40 years and underpins modern privacy laws worldwide. It is also reflected in all 22 state privacy laws, which create one set of obligations for controllers and another set of obligations for processors. Creating strong but different obligations for both types of companies — based on their role in handling consumers' data — helps to ensure that consumers' data is handled responsibly by all companies across a complex supply chain.[3]

[3] *See* BSA, Controllers and Processors: A Longstanding Distinction in Privacy (April 2, 2025), *available at* https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy.

The Secure Data Act also sets clear limits on these roles. Consistent with state privacy laws and modern privacy frameworks around the world, the bill recognizes that not every vendor is a processor. An entity is only a processor if it handles data on behalf of a controller and follows the controller's instructions. If a company starts out in that role but goes beyond those limits — by deciding for itself how or why the data should be processed — it is treated as a controller and must meet the bill's obligations for controllers. This ensures that companies are held to the responsibilities that match their actual role in handling consumers' data.

III. Privacy is a National Issue that Requires a National Solution.

The United States needs a strong, clear, comprehensive privacy law that creates a single standard for protecting consumers nationwide.

The Secure Data Act takes the right approach to creating a nationwide privacy law, by adopting the same structure used in state privacy laws and leveraging the core rights and obligations those laws create.

It is critical for these rights and obligations to apply nationwide — not state-by-state. Although state privacy laws are remarkably consistent in structure, they have important substantive variations. And those variations are growing, because at least 29 amendments have already revised, expanded, and changed state consumer privacy laws. These changes address important issues, including revising definitions, creating heightened protections for sensitive data, and adopting specific protections for children's data. But as states continue to change their existing privacy laws, it creates more variation — making it harder for both companies and consumers to understand their rights and obligations.

To be clear, it is important for policymakers to ensure that consumer privacy protections remain fit for purpose over time. But adopting these changes on a state-by-state basis does not benefit consumers nationwide, and it creates significant challenges for companies to identify new obligations and comply with the expanding set of state-level laws. Instead, new privacy protections should be applied nationwide.

a. Federal Privacy Legislation Benefits Both Companies and Consumers.

For American businesses, the advantages to a national privacy law are clear. Companies must currently keep up with quickly changing state requirements, monitoring not only potential new laws but also amendments to existing statutes and the rulemakings that implement them.

Tracking those obligations is difficult even for large companies with dedicated privacy legal teams but can be particularly challenging for small and medium-sized enterprises. A federal law is needed to replace this fragmented approach to privacy with a single, nationwide standard that limits how companies collect and use data — so that consumers trust that it is used responsibly.

For consumers, a national law ensures that everyone's data is protected — no matter where they live. A consumer should not lose privacy protections simply because she moves across state lines. Adopting a single national set of consumer privacy protections will also increase consumer awareness about their rights over personal data and knowledge about how companies must handle that data.

More broadly, adopting a federal privacy law will strengthen consumers' trust in technology, which has real economic benefits. Countries that adopt clear privacy safeguards and rules that promote the responsible and broad-based adoption of technologies, including artificial intelligence, will see the greatest economic and job growth in the coming years.[4]

b. A Federal Consumer Privacy Law Should be Worthy of Preemption.

A federal privacy law should replace, but not undermine, comprehensive state consumer privacy laws — and extend the protections already adopted in 22 states to consumers across the country. The goal of a federal privacy law should be to bring consistency to existing protections, not to weaken protections already provided by states. BSA supports a federal privacy law that is worthy of preempting existing state laws and ensures a consumer's privacy rights do not depend on the state in which she lives.

IV. The Modern Economy Also Relies on International Data Transfers.

The Secure Data Act also recognizes the importance of international data transfers in today's digital economy. This reflects the reality that cross border data transfers are now a routine and necessary component of modern commerce.

Companies of all sizes depend on employees, vendors, and infrastructure spread across the globe, requiring them to send data across international borders for everyday activities.

---

[4] While other countries have adopted laws to protect privacy through strong national frameworks, the United States remains one of the few advanced economies without a comprehensive national privacy law. In January 2025, 144 countries had national-level privacy laws, up from 120 countries with such laws in 2017, according to the International Association for Privacy Professionals. *See* IAPP, Data Protection and Privacy Laws Now In Effect in 144 Countries (Jan. 28, 2025), *available at* https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries.

Manufacturers rely on international data transfers to manage supply chains and logistics. Financial institutions transfer data internationally to detect fraud, process payments, and comply with regulatory obligations. Hospitals, airlines, retailers, and small businesses all depend on global data transfers to coordinate operations and serve customers. In today's interconnected economy, even businesses that operate locally often rely on international vendors for cloud computing, cybersecurity, human resources, or customer support.

International data transfers also strengthen competitiveness and support broader economic opportunities. They allow American companies to reach customers abroad, collaborate with partners around the world, and scale new products and services more efficiently. Cross border data transfers also help drive research, scientific collaboration, and emerging technologies. And they enable people and companies worldwide to use cutting-edge technologies like cloud computing, data analytics, blockchain, and artificial intelligence — boosting productivity, efficiency, and safety.

V. The Path Forward

We appreciate your work on the Secure Data Act and your focus on legislation to establish a federal comprehensive privacy and data security law that is grounded in the same core structure as existing state privacy laws.

Ultimately, enacting a federal privacy law will require bipartisan support. At the state level, both Republican-led and Democratic-led states have adopted privacy laws built around the same structure and core concepts reflected in the Secure Data Act. Ten Democratic governors and 11 Republican governors have signed into law state comprehensive privacy bills that are grounded in the same structure that underpins the Secure Data Act. These frameworks are no longer theoretical — they have created a foundation of consumer privacy law across the country.

We encourage lawmakers to work together, on a bipartisan basis, to build on that foundation and to adopt a comprehensive national consumer privacy law.

* * *

We appreciate this Committee's focus on the importance of protecting Americans' privacy. Thank you and I look forward to your questions.