Hearing on
Protecting the Virtual You: Safeguarding Americans' Online Data

Senate Judiciary Committee
Subcommittee on Privacy, Technology, and the Law

July 30, 2025, at 2:30 p.m.
Dirksen Senate Office Building, Room 226
Washington, DC

Testimony of Kate Goodloe
Managing Director
Business Software Alliance

Testimony of Kate Goodloe,
Managing Director of Business Software Alliance

Hearing on Protecting the Virtual You: Safeguarding Americans' Online Data

Before the Senate Judiciary Committee,
Subcommittee on Privacy, Technology, and the Law

July 30, 2025

Good afternoon Chair Blackburn, Ranking Member Klobuchar, and members of the Subcommittee. My name is Kate Goodloe, and I am Managing Director at the Business Software Alliance (BSA).

BSA is the leading advocate for the global enterprise software industry.[1] Our members create the business-to-business technologies used by companies in every sector of the economy. As a result, privacy and security are core to BSA members' operations. I commend the Subcommittee for convening today's hearing and thank you for the opportunity to testify.

Americans share their personal information online every day, just by using routine products and services. Whether we are shopping online, using apps to track workouts and sleeping habits, taking rideshares, or hosting video calls with friends and family, we provide personal information to a broad range of companies. Consumers deserve to know that their data is used responsibly.

As you look at safeguarding Americans' online data, I urge you to focus on the different types of companies that handle that data — and recognize that different companies must adopt different safeguards to effectively protect consumers.

Not all companies are consumer facing. BSA represents the business-to-business technology providers used by companies across the economy. An online store that sells clothing, for example, relies on a network of business-to-business technology providers. The store may use one provider to manage customer-service inquiries, another to generate shipping labels and track deliveries, and a third to adopt strong cybersecurity protections. Each of those companies should be required to handle consumers' personal data responsibly — but they must take different actions to protect consumers, because they play different roles in handling their data.

The United States needs a strong, clear, comprehensive privacy law that creates a single standard for protecting consumers nationwide. For too long, American consumers and businesses have not had a clear set of national rules that limit how companies can collect and use personal data. Instead, federal laws create sector-specific protections, including for health and financial records, which sit alongside traditional consumer protection laws prohibiting unfair or deceptive acts and practices. Some states have enacted privacy laws with comprehensive protections, but they only apply to residents of certain states.

---

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

Adopting a federal privacy law would bring consistency to existing protections, create broad and long-lasting privacy safeguards for consumers, and advance US leadership.

A federal privacy law should achieve three goals:

- Require companies to handle consumers' personal data responsibly, with obligations that reflect the company's role in processing that data;
- Give consumers new rights over their personal data; and
- Adopt a strong and consistent enforcement system.

In each area, a federal privacy law can — and should — build on the protections and obligations that states have advanced and enacted.

I. American Consumers Should be Protected by a Nationwide Privacy Law.

BSA members compete to provide privacy-protective products and services to other businesses, and they understand that robust data protection is a key part of building consumer trust and promoting full participation in the digital economy. Business-to-business technologies like cloud computing rely on data and, in some cases personal data, to function, and consumers deserve to know their personal information is being used responsibly.

Although there is no uniform federal law to protect consumer privacy nationwide, 20 states — both red and blue — have adopted comprehensive consumer privacy protections. Those state laws create a remarkably consistent framework, because 19 of the laws share the same structure but add and remove some substantive protections to reflect the different policy choices of lawmakers in each state. [2]

Congress should look to these state privacy protections to create a uniform federal privacy law.

a. Companies Should Be Required to Handle Data Responsibly, With Obligations That Reflect Their Role in Processing Consumers' Personal Data.

A federal privacy law should place meaningful limits on businesses that handle consumers' personal data and require them to handle that data responsibly.

These limits must reflect the company's role in handling consumers' personal data. Specifically, they must reflect whether the company decides why and how to collect a consumer's data or instead processes that data on behalf of another company and pursuant to the company's instructions. The distinction between these two types of companies — often referred to as controllers and processors — is critical to privacy laws worldwide and is incorporated in all comprehensive state privacy laws. Both types of businesses have important responsibilities to protect consumers' data, but their obligations should fit their roles. If legislation does not reflect these different roles, it can end up undermining the goal of improving consumer privacy by creating obligations that inadvertently pose new privacy and security risks for consumers.

We strongly recommend a federal privacy law: (1) define controllers and processors, and (2) assign strong but different obligations to each type of entity, reflecting their different roles in

[2] BSA, "Models of State Privacy," April 3, 2025 (last updated), https://www.bsa.org/policy-filings/us-2025-models-of-state-privacy-legislation.

handling consumers' personal data.[3] This creates better protections for consumers, by ensuring all companies who handle their personal data protect it.

Controllers decide how and why to process a consumer's personal data — and they should be responsible for obligations related to those decisions. For example, if a law requires consent to process certain types of data, the controller should be obligated to obtain that consent. This ensures that a controller adjusts its decisions about how and why to collect personal data in light of its legal obligations. Similarly, when laws create data minimization requirements, those obligations should fall on controllers — so that their decisions about how and why to collect consumers' data minimize the collection and use of that data. Controllers are also typically the companies interacting directly with consumers, so consumers usually expect them to carry out consumer-facing obligations like asking for consent and providing notice.

Many comprehensive state consumer privacy laws assign a common set of obligations to controllers, including:

- Responding to consumer rights requests, including requests to access, correct, delete, and port personal data.
- Honoring requests to opt out of certain processing, including targeted advertising, sale of personal data, and certain types of profiling.
- Obtaining consent to process sensitive personal data.
- Complying with data minimization obligations.
- Adopting reasonable data security measures.
- Providing privacy notices to consumers about how and why personal data is processed.
- Conducting data protection assessments, to assess potential impacts of specific activities.

Processors handle data on behalf of a controller and pursuant to its instructions — and they should be obligated to handle data confidentially and subject to contractual limitations.[4]

Many comprehensive state consumer privacy laws assign a common set of obligations to processors, including:

- Processing personal data pursuant to a contract with the controller.
- Deleting or returning personal data at the end of services.
- Providing information to the controller as necessary for the controller to conduct data protection assessments.
- Requiring any subprocessors engaged by the processor to meet the processor's obligations and to notify the controller that a subprocessor is engaged.
- Imposing a duty of confidentiality on persons processing personal data.
- Adopting reasonable data security measures.

---

[3] BSA, "Controllers and Processors: A Longstanding Distinction in Privacy," April 2, 2025, https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy, and BSA, "The Global Standard in Privacy Legislation: Distinguishing Between Controllers and Processors," June 12, 2025, https://www.bsa.org/policy-filings/the-global-standard-in-privacy-legislation-distinguishing-between-controllers-and-processors.

[4] If a company agrees to handle personal data as a processor but then breaks that agreement and begins independently deciding to process the data for its own purposes it would no longer fall within the definition of a processor. In that scenario, the entity should be treated as a controller and be subject to the obligations placed on controllers, because it is deciding how and why to process personal data.

These roles reflect the modern economy, where one company may rely on many processors to provide services to consumers. For example: A grocery store may decide to collect information from its customers and store that information in the cloud. The grocery store acts as a controller, because it decides what information to collect from consumers — and when, how, and why to use that information. The cloud storage provider acts as a processor, because it stores the data on behalf of the grocery store and processes it pursuant to the grocery store's instructions.

The concepts of controllers and processors have existed for more than 40 years and are reflected in all 20 comprehensive state consumer privacy laws.[5] Nineteen of the comprehensive state consumer privacy laws use the terms controller and processor, while California uses the terms business and service provider. Controllers and processors are also key to privacy and data protection frameworks worldwide, including the OECD Privacy Guidelines, the APEC Privacy Framework, and ISO 27701.[6]

b. Consumers Should Have New Rights Over Their Personal Data.

A federal privacy law should give consumers new rights over their personal data, including the right to access their personal data, the right to correct personal data that is inaccurate, the right to delete their personal data, and the right to port their personal data. There is widespread agreement that these rights are core components of effective privacy laws.

At the state level, all 20 comprehensive state consumer privacy laws create rights for consumers over their personal data. These include:

- Right to access personal data (20 states)
- Right to correct personal data (19 states)
- Right to delete personal data (20 states)
- Right to data portability (20 states)

States also create rights for consumers to opt out of certain types of processing. These include:

- Right to opt out of sale of personal data (20 states)
- Right to opt out of targeted advertising (19 states)
- Right to opt out of certain types of profiling (17 states)

A federal law should build on these existing rights. It should also contain practical limits on exercising those rights, as state privacy laws recognize. For example, a consumer's right to delete data should contain limits so that the consumer cannot require a business to delete data that the business is legally required to retain. A federal privacy law should also recognize other appropriate limits on consumer rights, so that honoring the rights of one consumer does not

---

[5] *Id.*

[6] OECD, "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," Part 1(a) (defining "data controller"), 1980, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188; APEC, "Privacy Framework," Part II.10 (defining "personal information controller" as part of a privacy framework for controllers), 2015, https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015); APEC, "Privacy Recognition for Processors ("PRP") Purpose and Background" (explaining the APEC PRP creates requirements for processors, complementing the APEC Privacy Framework for controllers), August 2020, https://cbprs.org/wp-content/uploads/2020/08/PRP-Purpose-and-Background-4.pdf; Int'l Org. for Standardization, International Standard ISO/IEC 27701 Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines 1, 4-5, 49-55, (creating standards for both controllers and processors), 2019, https://www.iso.org/standard/71670.html.

create privacy or security risks to other consumers or to the company's services. In addition, the primary obligation to respond to consumer rights requests should be assigned to the controller, since it decides how and why to collect and process that information and will be in a position to know if a consumer's rights (or any exceptions to those rights) apply. This approach will also ensure consumers know which organization to contact to exercise their rights.

c. A Privacy Law Should Create a Strong, Consistent Enforcement System.

Effective enforcement is important to protect consumers' privacy, ensure that organizations meet their commitments and legal obligations, and deter potential violations.

A federal privacy law should be enforced by federal and state officials working together.

At the federal level, the Federal Trade Commission (FTC) has a long history of enforcing consumer protections, including bringing more than 180 privacy and data security enforcement actions under Section 5 of the FTC Act.[7] The FTC is therefore an appropriate choice for the primary federal agency to enforce consumer privacy protections. To serve this function, though, the FTC may need new authorities, including the ability to fine first-time violators and targeted rulemaking authority.

At the state level, empowering state attorneys general to enforce a federal privacy law will maintain an important pathway for states to continue to promote and protect privacy. All 20 comprehensive state consumer privacy laws create a role for the state's attorney general to enforce the privacy law. Nineteen of these state privacy laws also created a right for businesses to cure privacy violations, with 10 states ending that right to cure after a certain period of time. Notably, none of the 20 comprehensive state consumer privacy laws create a private right of action for privacy violations.[8] Working together, the FTC and state attorneys general can create a strong and consistent approach to enforcing federal privacy protections, ensuring that organizations meet their obligations under a federal privacy law.

II. A Federal Law Should Bring Consistency to Existing Privacy Obligations.

A comprehensive federal consumer privacy law can bring consistency to existing state protections. It can also help to guard against a worst-case scenario, in which 50 states adopt privacy laws with conflicting obligations. We are not yet in that scenario, but there are signs that the current consistent approach to state privacy protections may not last.

The wave of state consumer privacy laws began in 2018, when California adopted its state privacy law. Since then, states have steadily adopted new privacy laws, with two adopted in 2021 (in CO and VA), two adopted in 2022 (in UT and CT), eight adopted in 2023 (in DE, FL, IN, IA, MT, OR, TN, TX) and seven adopted in 2024 (in KY, MD, MN, NE, NH, NJ, RI). Those laws emerged from a much broader set of bills. Specifically:

---

[7] Federal Trade Commission, "2023 Privacy and Data Security Update," March 21, 2024, https://www.ftc.gov/system/files/ftc_gov/pdf/2024.03.21-PrivacyandDataSecurityUpdate-508.pdf.

[8] California is the only state to include a private right of action in its privacy law, but it does not allow consumers to sue for violations of the law's privacy protections. Instead, it only allows consumers to bring suit for a narrow set of data security breaches. Cal. Civ. Code Sec. 1798.150 (creating a private right of action for certain breaches of nonencrypted and nonredacted personal information, but defining that information narrowly, as a subset of "personal information" covered by the state's Customer Records law, rather than the broader set of "personal information" defined in the CCPA).

- In 2019, at least 25 comprehensive privacy bills were introduced across 17 states.
- In 2020, at least 46 comprehensive privacy bills were introduced across 19 states.
- In 2021, at least 54 comprehensive privacy bills were introduced across 26 states.
- In 2022, at least 70 comprehensive privacy bills were introduced across 29 states.
- In 2023, at least 70 comprehensive privacy bills were introduced across 30 states; another nine bills were introduced to amend existing privacy laws.
- In 2024, at least 60 comprehensive privacy bills were introduced across 25 states; another 25 bills were introduced to amend existing privacy laws.
- In 2025, at least 49 comprehensive privacy bills have been introduced across 19 states; at least another 31 bills have been introduced to amend existing privacy laws.

This year, no state without a comprehensive consumer privacy law has adopted one. Instead, there has been a significant focus on amending existing state privacy laws, with seven states amending their comprehensive consumer privacy laws this year. These amendments revise and expand the rights and obligations in existing laws, including:

- **Colorado** expanded the definition of sensitive data and adopted new obligations for processing sensitive data.[9]
- **Connecticut** adopted broad amendments, including to expand certain consumer rights, broaden key definitions, and revise the law's data minimization standard.[10]
- **Kentucky** changed thresholds for applying the law and revised obligations on profiling.[11]
- **Montana** adopted broad amendments that change the thresholds for applying the law, broaden certain consumer rights, and remove a right for businesses to cure violations.[12]
- **Oregon** adopted new rules on sensitive data and kids data.[13]
- **Utah** added a right to correct inaccurate data and rules on social media.[14]
- **Virginia** adopted new obligations for social media platforms.[15]

As states continue to amend, expand, and update their existing privacy laws, it will create more variation among the state laws.

New state privacy obligations are also imposed through rulemakings to implement existing laws. In California, the California Privacy Protection Agency (CPPA) began initial rulemaking activities in 2021 to implement new obligations created by a ballot initiative passed in 2020.[16] That agency finalized one set of rules in March 2023 and voted earlier this month to formally adopt

---

[9] Colorado SB 276, https://leg.colorado.gov/bills/sb25-276, takes effect on Oct. 1, 2025.
[10] Connecticut SB 1295, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2025&bill_num=1295, takes effect July 1, 2026.
[11] Kentucky HB 473, https://apps.legislature.ky.gov/record/25RS/hb473.html, takes effect January 1, 2026.
[12] Montana SB 297, https://bills.legmt.gov/#/laws/bill/2/LC0372?open_tab=sum, takes effect October 1, 2025.
[13] Oregon HB 2008, https://olis.oregonlegislature.gov/liz/2025R1/Measures/Overview/HB2008, takes effect January 1, 2026.
[14] Utah HB 418, https://le.utah.gov/~2025/bills/static/HB0418.html, takes effect July 1, 2026.
[15] Virginia SB 854, https://lis.virginia.gov/bill-details/20251/SB854, takes effect January 1, 2026.
[16] California Privacy Rights Act of 2020 (CPRA), passed via Proposition 24, https://cppa.ca.gov/regulations/pdf/prop24_text.pdf. The CPPA held public comment periods on implementing rules in September 2021, July 2022, and November 2022, before the rules took effect in March 2023. CCPA Regulations, March 2023, https://cppa.ca.gov/regulations/consumer_privacy_act.html.

another lengthy set of rules on topics including cybersecurity audits, risk assessments, and automated decision-making technology.[17] In New Jersey, the Attorney General is also developing draft rules to implement the state's privacy law, which took effect six months ago.[18]

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, making it easier for businesses to understand when their obligations change and extending consumer safeguards to all Americans. Like many other companies, BSA members don't operate in just one state — and enacting a federal privacy law can help them invest in strong compliance programs that serve customers across the country.

III. A Federal Privacy Law Should Be Worthy of Preemption.

A federal privacy law should preempt existing comprehensive state consumer privacy laws and create a single, national standard that protects consumers nationwide.

We recognize that states have been leaders in adopting new privacy protections. However, navigating a growing number of state-level obligations creates significant challenges for companies that operate nationwide and creates confusion for consumers about how and when their rights apply. 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.

Importantly, the aim of a consistent national standard is not to weaken privacy protections already provided by state laws. A federal law should replace, but not undermine, comprehensive state consumer privacy laws — and extend the protections already adopted in 20 states to consumers across the country. A federal law should also ensure that states continue to be leaders in enforcing privacy protections, by ensuring that a federal privacy law empowers state attorneys general to enforce its obligations.

IV. A Strong Federal Privacy Law Is Good for American Consumers, American Businesses, and American Leadership.

Creating a strong national standard for consumer privacy has significant benefits.

For American businesses, the advantages 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 strong federal privacy law would replace this fragmented approach to privacy with a single, nationwide standard.

---

[17] The CPPA voted on July 24, 2025, to submit a new 119-page set of rules for formal approval, after public comment periods in February 2023, November 2024, and May 2025. Proposed Regulations, https://cppa.ca.gov/regulations/ccpa_updates.html.

[18] New Jersey Attorney General Division of Consumer Affairs, Press Release, June 2, 2025, https://www.njconsumeraffairs.gov/News/Pages/06022025.aspx. The New Jersey Data Privacy Act took effect January 15, 2025.

A federal privacy law that aligns with leading global privacy frameworks can also strengthen the ability of American companies to do business worldwide. Many existing state privacy laws already include core elements found in global privacy laws, such as strong consumer rights and clear obligations for both controllers and processors. Building on those core elements at the federal level would allow American companies to develop robust, interoperable compliance programs that meet key legal obligations across jurisdictions. That not only improves the consistency and quality of consumer protections but also facilitates cross-border data transfers — an essential component of the modern digital economy. A federal law that is interoperable with leading global frameworks can further support data transfers, helping American businesses compete globally while upholding high standards for privacy.

For consumers, a national privacy law will ensure their personal data is protected regardless of where they live. A consumer should not lose privacy protections simply because she moves from Tennessee to South Carolina. All Americans deserve to have their personal data protected, regardless of the state they live in. Adopting a single 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.

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, 144 countries had national-level privacy laws, up from 120 countries with such laws in 2017, according to the International Association for Privacy Professionals.[19] The United States will have a stronger voice on digital issues globally if it enacts a federal privacy law that is uniquely American and creates clear rules for companies that handle consumers' personal data.

V. The Path Forward

BSA members are leaders in providing privacy-protective technologies to other companies. But they operate in a global environment that is increasingly complex, both in terms of technology and regulation. A federal consumer privacy law that sets strong standards and brings consistency to existing protections would help protect consumers' privacy, create a clear standard for businesses, and contribute to US leadership on privacy issues globally. BSA strongly supports these goals, and we look forward to working with Congress to achieve them.

* * *

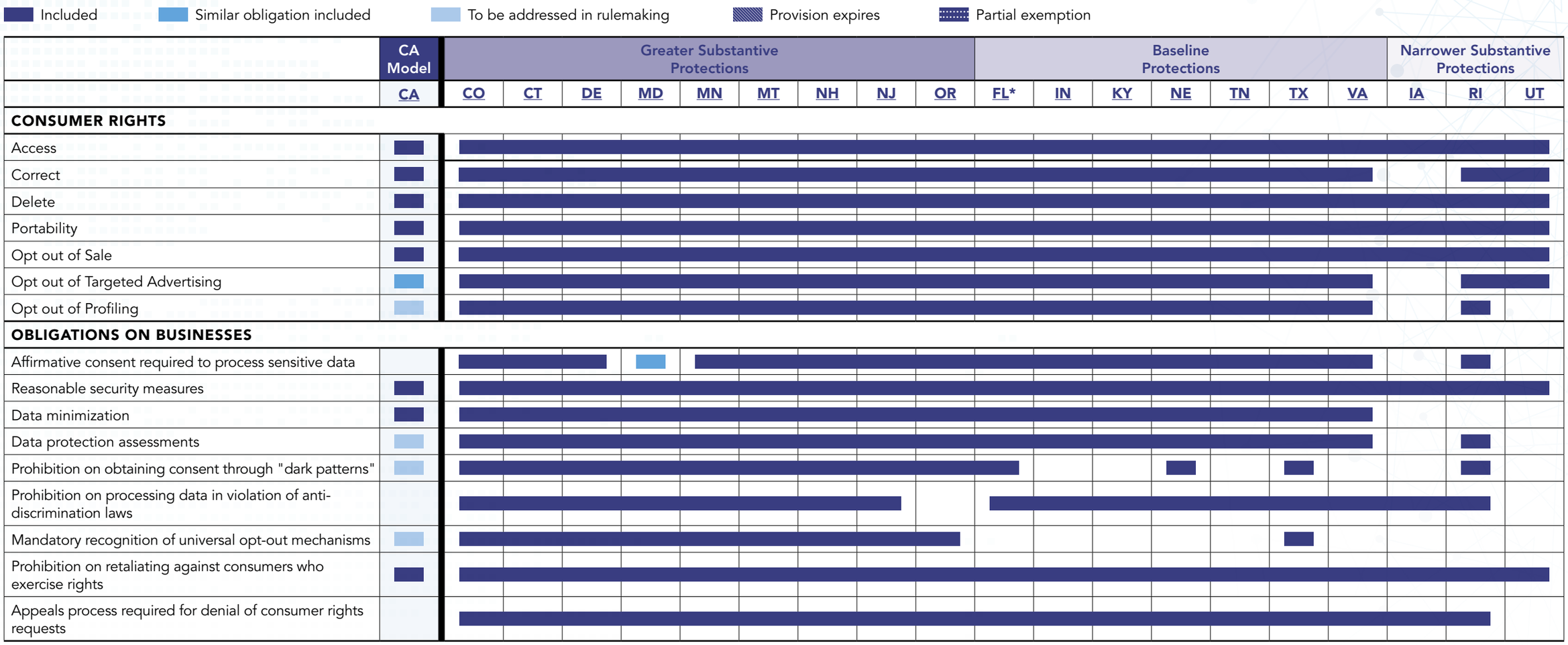
We appreciate this Committee's focus on the importance of protecting Americans' privacy. Thank you and I look forward to your questions.

[19] Aly Apacible-Bernardo and Kayla Bushey, Data Protection and Privacy Laws Now in Effect in 144 Countries, IAPP, January 28, 2025, https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries.

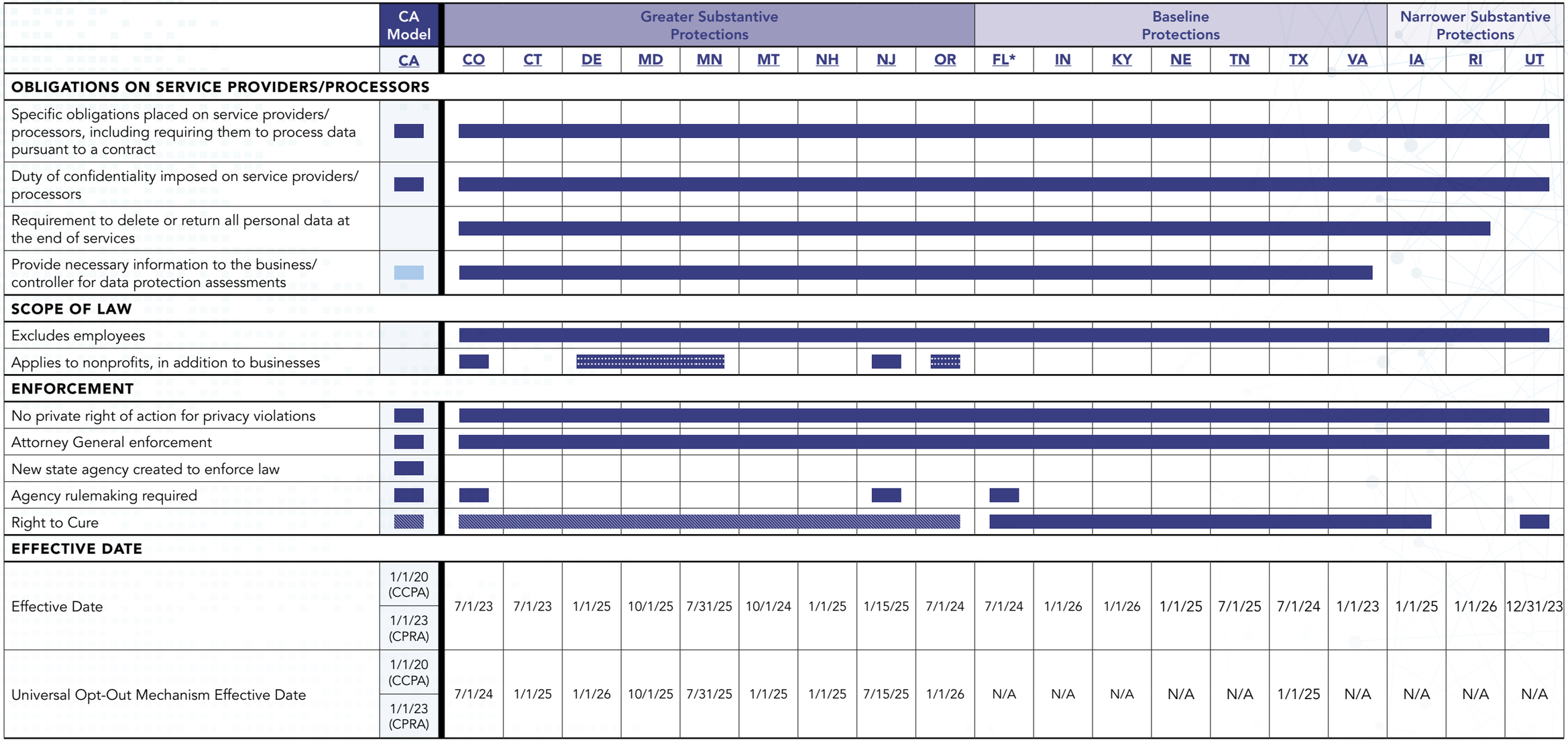
Business Software Alliance

Models of State Privacy Legislation

Twenty states have enacted comprehensive consumer privacy laws that create new rights for consumers, impose obligations on businesses that handle consumers' personal data, and create new mechanisms to enforce those laws. Nineteen of those states adopt the same basic structural model to protect consumer privacy. Some of those states have added greater substantive protections to that basic structural model while other states have adapted the same model to create narrower substantive protections, as reflected in the chart below. In contrast, California adopted a legislative model that creates a new state privacy agency charged with issuing regulations on more than 20 topics, including on issues addressed by statute in other states.



Included | Similar obligation included | To be addressed in rulemaking | Provision expires | Partial exemption



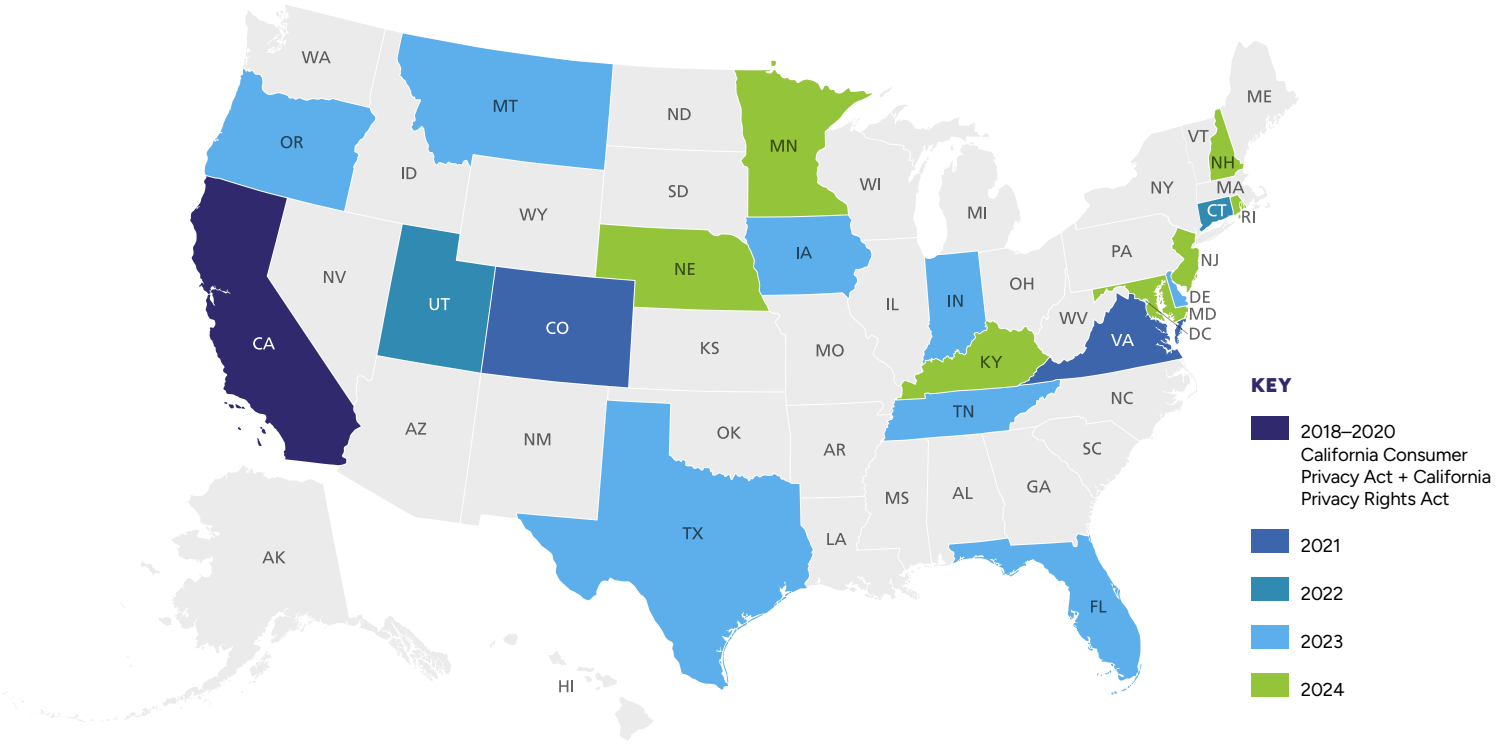
	CA Model	Greater Substantive Protections									Baseline Protections							Narrower Substantive Protections		
	CA	CO	CT	DE	MD	MN	MT	NH	NJ	OR	FL*	IN	KY	NE	TN	TX	VA	IA	RI	UT
OBLIGATIONS ON SERVICE PROVIDERS/PROCESSORS																				
Specific obligations placed on service providers/ processors, including requiring them to process data pursuant to a contract																				
Duty of confidentiality imposed on service providers/ processors																				
Requirement to delete or return all personal data at the end of services																				
Provide necessary information to the business/ controller for data protection assessments																				
SCOPE OF LAW																				
Excludes employees																				
Applies to nonprofits, in addition to businesses																				
ENFORCEMENT																				
No private right of action for privacy violations																				
Attorney General enforcement																				
New state agency created to enforce law																				
Agency rulemaking required																				
Right to Cure																				
EFFECTIVE DATE																				
Effective Date	1/1/20 (CCPA)	7/1/23	7/1/23	1/1/25	10/1/25	7/31/25	10/1/24	1/1/25	1/15/25	7/1/24	7/1/24	1/1/26	1/1/26	1/1/25	7/1/25	7/1/24	1/1/23	1/1/25	1/1/26	12/31/23
	1/1/23 (CPRA)																			
Universal Opt-Out Mechanism Effective Date	1/1/20 (CCPA)	7/1/24	1/1/25	1/1/26	10/1/25	7/31/25	1/1/25	1/1/25	7/15/25	1/1/26	N/A	N/A	N/A	N/A	N/A	1/1/25	N/A	N/A	N/A	N/A
	1/1/23 (CPRA)																			

* Florida's coverage thresholds are higher than those in other state privacy laws and apply to a more limited set of companies.

Business Software Alliance

Federal Privacy Legislation Can Build on State Privacy Laws

Twenty states have enacted their own privacy laws, but there remains no uniform federal law to safeguard consumers' personal data nationwide. A federal privacy law would bring consistency to existing protections, create broad and long-lasting privacy safeguards for consumers, and advance US leadership.



Congress can build on the work of states and adopt a federal privacy law that: (1) provides consumers rights over their personal data, (2) requires companies to handle personal data responsibly, and (3) adopts a strong, consistent approach to enforcement.

Consumer Rights

A federal privacy law should give consumers important rights over their personal data, including to:

- Access, correct, delete, and port their personal data
- Opt out of:
  - sale,
  - targeted advertising, and
  - certain types of profiling

Obligations on Businesses

A federal privacy law should require companies that handle consumers' personal data to do so responsibly, including to:

- Obtain consent for processing sensitive data
- Adopt reasonable security measures
- Require impact assessments for specific activities

It should also reflect the different roles and responsibilities of controllers and processors.

Strong Enforcement

A federal privacy law should be enforced by federal and state agencies working together.

- The Federal Trade Commission has a long history of addressing consumer privacy.
- Allowing state attorneys general to enforce the law adds 50+ enforcement agencies.

How Can Federal Privacy Legislation Build on State Privacy Laws?

Nineteen of the 20 states with consumer privacy laws use the same structural model to protect consumer privacy. While states adapt this model by adding and removing substantive protections, these laws create a common framework that Congress can build on to create a uniform, nationwide privacy law.

CONGRESS CAN BUILD ON THE WORK OF STATES AND ADOPT A FEDERAL PRIVACY LAW THAT:

Provides consumers rights over their personal data,

Requires companies to handle personal data responsibly, and

Adopts a strong, consistent approach to enforcement.

Consumer Rights

All 20 state privacy laws create new rights for consumers in their personal data. These include:

- **Right to access personal data:** 20 states
- **Right to correct personal data:** 19 states
- **Right to delete personal data:** 20 states
- **Right to data portability:** 20 states
- **Right to opt out of sale:** 20 states
- **Right to opt out of targeted advertising:** 19 states
- **Right to opt out of certain types of profiling:** 17 states

Obligations on Businesses

All 20 state privacy laws create obligations for businesses to handle consumers' personal data responsibly. All 20 also reflect the fundamental distinction between controllers, which are the companies that decide when and why to collect a consumer's personal data, and processors, which handle that personal data on behalf of another company and pursuant to their instructions.

State privacy laws assign important—and distinct—obligations to both controllers and processors, based on their different roles.

CONTROLLERS MUST:

- **Obtain consent to process sensitive data:** 16 states
- **Adopt reasonable security measures:** 20 states
- **Conduct data protection assessments for certain activities:** 17 states
- **Recognize universal opt out mechanisms:** 11 states
- **Not retaliate against consumers who exercise their rights:** 20 states

PROCESSORS MUST:

- **Process data pursuant to a contract:** 20 states
- **Be subject to a duty of confidentiality:** 20 states
- **Delete or return all data at the end of services:** 18 states
- **Provide information a controller needs to conduct data protection assessments:** 16 states

Notably, state privacy laws focus on *consumer* privacy. Nineteen states expressly exclude employees.

Enforcement

All 20 laws create a role for the state's attorney general to enforce the privacy law. The laws have:

- **No private right of action for privacy violations:** 20 states
- **Right to cure violations:** 19 states (10 sunset)
- **Rulemaking required:** 4 states
- **New state agency created to enforce law:** 1 state

For more information comparing state privacy laws, see BSA's Models of State Privacy Legislation.

Business Software Alliance

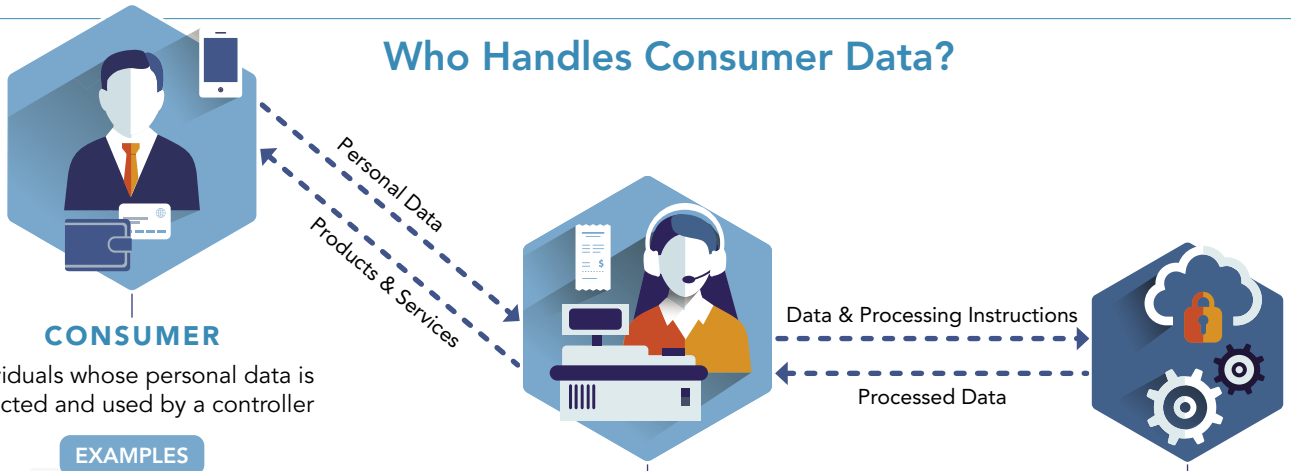
The Global Standard in Privacy Legislation: Distinguishing Between Controllers and Processors

Comprehensive privacy legislation must create strong obligations for all companies that handle consumer data. These obligations will only be strong enough to protect consumer privacy and instill trust, though, if they reflect how a company interacts with consumer data.

Privacy laws worldwide distinguish between two types of companies: (1) businesses that decide *how* and *why* to collect consumer data, which act as **controllers** of that data and (2) businesses that process the data *on behalf of* another company, which act as **processors** of that data.

This fundamental distinction is critical to a host of global privacy laws. It is also reflected in all 20 comprehensive consumer privacy laws enacted at the state level. Both types of businesses have important responsibilities and obligations, which should be set out in any legislation.

Who Handles Consumer Data?



CONSUMER

Individuals whose personal data is collected and used by a controller

EXAMPLES

Consumers who shop at retail stores, buy products online, or share information on social media platforms.

CONSUMERS SHOULD HAVE THE RIGHT TO:

- **Know** what type of data a controller collects — and why
- **Access** information about them
- **Correct** that information
- **Delete** that information
- **Opt out** of sale, targeted advertising, and certain profiling
- Have their data **securely protected**
- Have their data used **consistent with their expectations**

CONTROLLER

Decides whether and how to collect data from consumers, and the purposes for which that data is used

EXAMPLES

Companies that interact directly with consumers, such as hotels, banks, retail stores, travel agencies, and consumer-facing technology providers.

CONTROLLERS ARE RESPONSIBLE FOR:

Obtaining any consent needed to process a consumer's data

Responding to consumer requests like access, correction, or deletion

Using data consistent with the consumers' expectation

PROCESSOR

Processes data on behalf of a controller, pursuant to the controller's instructions

EXAMPLES

Companies that provide business-to-business products like cloud computing, and vendors like printers, couriers, and others that process data at the direction of another company.

PROCESSORS ARE RESPONSIBLE FOR:

Processing data consistent with a controller's instructions

Adopting appropriate safeguards designed to protect data security

Controllers and processors should have role-dependent responsibilities to ensure consumers' privacy and security are protected.

Privacy Laws Worldwide Distinguish Between Controllers and Processors

Privacy laws worldwide reflect the basic distinction between companies that decide to collect and use data about individuals and companies that only process such data.

CONTROLLERS	PROCESSORS
Companies that decide how and why to collect consumers' personal data.	**Companies that process consumers' personal data at the direction of others.**

Sometimes, a company may process personal data as a controller (for some products and services) and also process personal data as a processor (for other products and services). Distinguishing between these two roles is critical, so the company knows which obligations apply to each product and service.

The concepts of controllers and processors have existed for more than 40 years. These roles are key parts of global privacy and data protection frameworks including the OECD Privacy Guidelines, Convention 108, the APEC Privacy Framework, and ISO 27001.

EXAMPLE

A business contracts with a printing company to create invitations to an event. The business gives the printing company the names and addresses of the invitees from its contact database, which the printer uses to address the invitations and envelopes. The business then sends out the invitations.

The business is the controller of the personal data processed in connection with the invitations. The business decides the purposes for which the personal data is processed (to send individually-addressed invitations) and the means of the processing (mail merging the personal data using the invitees' addresses). The printing company is the processor handling the personal data pursuant to the business's instructions. The printing company cannot sell the data or use it for other purposes, such as marketing. If the printing company disregarded those limits and used the data for its own purposes, it would become a controller and be subject to all obligations imposed on a controller.

Why Is the Distinction Between Controllers and Processors Important to Protecting Consumer Privacy?

Distinguishing between controllers and processors ensures that privacy laws impose obligations that reflect a company's role in handling consumer data. This helps safeguard consumer privacy without inadvertently creating new privacy or security risks.

Data Security. Controllers and processors should both have strong obligations to safeguard consumer data.

- Placing this obligation on both types of companies ensures consumer data is protected.
- Controllers and processors should both employ reasonable and appropriate security measures, relative to the volume and sensitivity of the data, size, and nature of the business, and the cost of available tools.

Consumer Rights Requests. Responding to important consumer rights requests—such as requests to access, correct, or delete personal data—requires knowing what is in that data.

- Controllers interact with consumers and decide when and why to collect their data. For that reason, laws like those in Virginia, Colorado, and California require controllers to respond to consumer rights requests. Moreover, controllers must decide if there is a reason to deny a consumer's request, such as when a consumer asks to delete information subject to a legal hold.
- Processors, in contrast, often do not know the content of the data they process, and may be contractually prohibited from looking at it. It is not appropriate for processors to respond directly to a consumer's request—which creates both security risks (by providing data to consumers they do not know) and privacy risks (by looking at data they otherwise would not). Processors should instead provide controllers with tools the controller can use to collect data needed to respond to a consumer's request.