2026 State Privacy and AI Developments Round-Up

June 16, 2026

Mike Signorelli | masignorelli@Venable.com

Allie Monticollo | ammonticollo@Venable.com

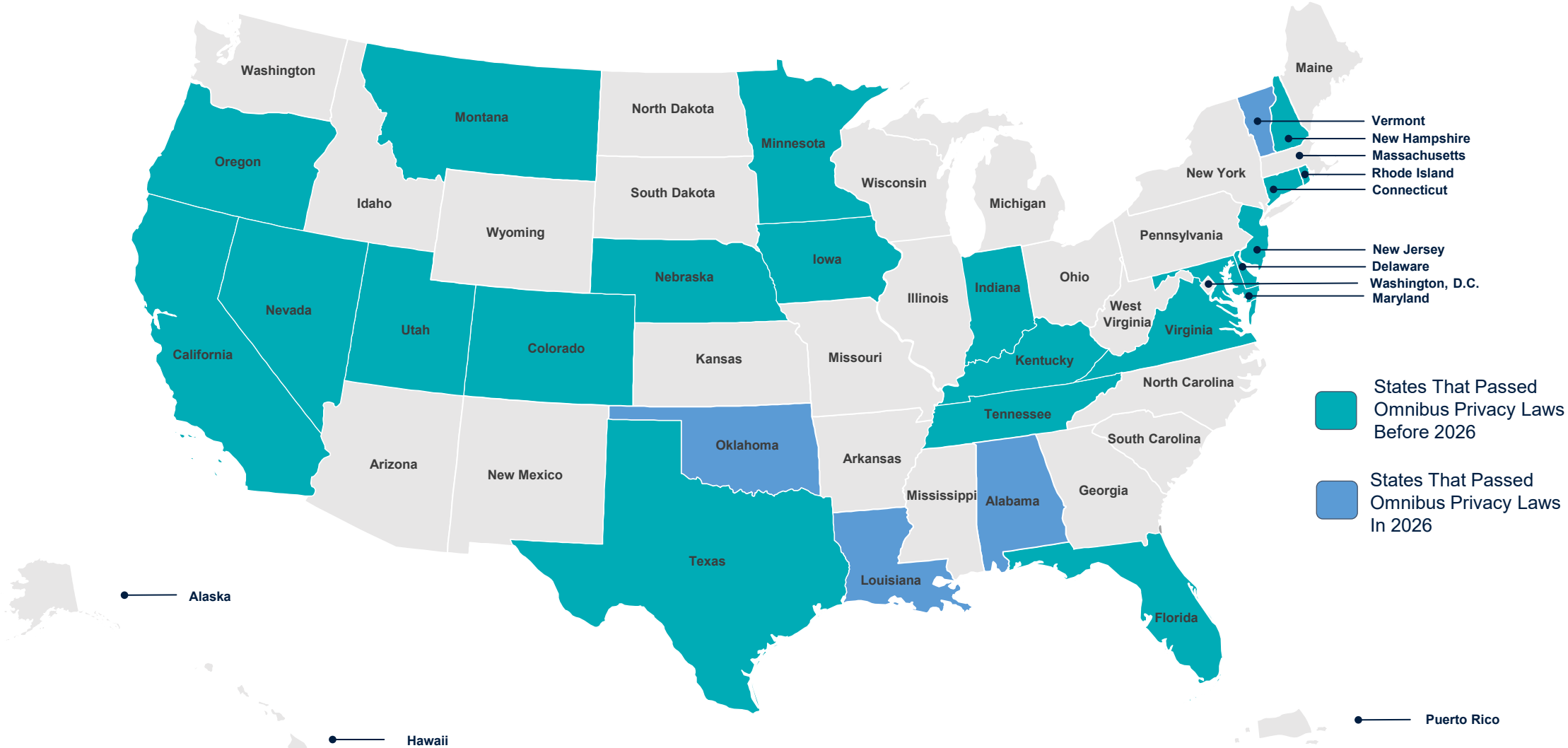
VENABLE LLP

Agenda

- New Omnibus Privacy Laws
- Notable Amendments to Omnibus Laws
- Data Brokers
- Kids and Minors
- AI
- “Surveillance Pricing”
- 2026 California Enforcement Spotlight

VENABLE LLP

Omnibus Privacy Laws



VENABLE LLP

New Omnibus Privacy Laws and Notable Amendments

- **New Laws**
  - **Louisiana** – effective January 1, 2027
  - **Oklahoma** – effective January 1, 2027
  - **Alabama** – effective May 1, 2027
  - **Vermont** – effective January 1, 2028

- **General Approach of New Laws**
  - Rights-based (access, correction, deletion, portability, opt-out)
  - Transparency requirements (privacy policy)
  - Data minimization (must limit collection of personal data to what is adequate, relevant, and reasonably necessary in relation to purposes for which personal data is processed, as disclosed to the consumer)
  - Enforcement vested in state AG; no PRA

VENABLE LLP

New Omnibus Privacy Laws – Notable Provisions

- Louisiana – effective January 1, 2027
  - **NOTICE requirements for sales of sensitive personal data and biometric data**
  - **Authentication** required for all consumer rights (including opt-outs)
  - **Cure period available until July 31, 2027**

- Oklahoma – effective January 1, 2027
  - **Pseudonymous data qualifier in definition of personal data.** "The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual."
  - **Authentication** required for all consumer rights (including opt-outs)
  - **Mandatory 30-day cure period** (no sunset)

VENABLE LLP

New Omnibus Privacy Laws – Notable Provisions (cont.)

- **Alabama** – effective May 1, 2027
  - "Sales" do not include disclosures to a third party **for the purpose of providing analytics services or marketing services "solely" to the controller**
  - **No assessment requirements**
  - **Mandatory 45-day cure period** (no sunset)
- **Vermont** – effective January 1, 2028
  - **Profiling**: If personal data is processed for profiling in furtherance of an automated decision that produces legal or similarly significant effects, consumers may **question the result**, **be informed of the reason** the profiling resulted in the decision, **review the personal data** processed for the profiling, and **correct the personal data if it is used for a housing decision**; additional impact assessment requirements for profiling in furtherance of decisions that produce legal effects
  - Right to obtain a **list of third parties** to which a controller has sold personal data
  - **Limit on disclosing certain information in response to an access request** (e.g., SSN and other government-issued ID numbers, financial account number, biometric data, etc.)
  - **Privacy notice** must include a statement disclosing whether the controller collects, uses, or sells personal data for the purpose of **training large language models**
  - **Cure period available until June 30, 2029**

VENABLE LLP

Notable Amendments to Omnibus Privacy Laws

Notable Amendments

- **Maryland** – effective July 1, 2026
  - Precise geolocation data = information derived from technology that can precisely and accurately identify, within a radius of 1750 feet, the specific location of a consumer, *a mobile device, or a vehicle*
  - Publicly available information = information lawfully obtained from a government entity record *if the person complies with each restriction or term of use the government entity imposes as a condition for providing the information*
  - Prohibits knowing sales of personal data to a government unit that, within the prior 6 months, has engaged in or supported civil immigration enforcement through provision of personnel or material resources
- **Virginia** – effective July 1, 2026
  - Prohibits controllers from selling or offering for sale precise geolocation data
- **Connecticut** – effective October 1, 2026
  - Facial recognition technology terms
  - Amendments to publicly available information definition and extension of deletion right to certain publicly available information
  - Ban on controller and third-party sales of precise geolocation data

VENABLE LLP

State Omnibus Privacy Laws

- **Sensitive data / precise geolocation data sales**
  - *See, e.g.*, Maryland, Oregon, Virginia, Connecticut
- **Sectoral law and other exemptions**
  - *See, e.g.*, Montana, Connecticut
- **Data minimization**
  - *See, e.g.*, Maryland
- **Applicability thresholds**
  - *See, e.g.*, Montana
- **Sensitive data consent**
  - *See, e.g.*, Delaware HB 380 (not yet enacted)
- **Outlier Proposals:**
  - Duty of loyalty requirements
  - "Original" data collector contact information requirements
  - Extension of rights/protections to *all individuals when data is collected about them in the relevant jurisdiction* (not just state residents or consumers)

VENABLE LLP

Data Brokers

- **Connecticut enacts new data broker registration requirements and DELETE Act.** *See* CT SB 4 (2026), as amended by CT HB 5222 (2026). *Effective October 1, 2026.*
  - **$2,500** annual registration fee
  - Commissioner of Consumer Protection (DCP) required to establish an accessible deletion mechanism program not later than **July 1, 2028**
  - DCP required to verify consumer requests by **August 15, 2028**
    - DCP or DCP's "authorized agent" to verify deletion requests
    - Unverified deletion requests must be treated as opt-out requests
  - Registered data brokers required to comply and access the mechanism at least once every 45 days beginning on **October 1, 2028**
  - Law contemplates giving consumers the option to exclude individual data brokers from the scope of their requests
  - **Exemptions** for several processing activities, e.g., compliance with laws; cooperation with law enforcement; preventing, detecting, protecting against, or responding to security incidents, identity theft, fraud; assisting other persons in performing such exempt activities
  - **Exemptions** for entities engaged in activities under certain sectoral laws
  - **Regulatory authority for DCP**

VENABLE LLP

Data Brokers

- **Vermont amends data broker regime.** *See* HB 211 (2026) (here and here).
  - Amendment to "brokered personal information" definition; adopts California definition of "direct relationship"
  - New disclosures required, including:
    - Whether the data broker **collects precise geolocation**, reproductive healthcare data, biometric data, immigration status, sexual orientation, union membership, name, DOB, zip, email address, phone number, account login or account number in combination with required security code/access code/password, DLN, SSN, passport number, or other unique ID number issued on a government document, **mobile ad ID number**, **CTV ID number**, **VIN**, or the three most common types of personal information the data broker collects if the data broker does not collect such data points
    - Whether the data broker in the past year **shared or sold** "consumers' data" to a foreign actor, the federal government, other state/local governments, law enforcement (unless pursuant to subpoena or court order), a **developer of a GenAI system or model**
  - NO centralized DELETE Act mechanism, but requires **Secretary of State study of DELETE Act mechanism**
    - Interim report due December 1, 2027 and final report due December 1, 2028
  - Adds **data broker deletion right** (authentication required), with a requirement to provide a link to part of data broker's website that allows a consumer to submit a deletion request and informs consumers of opt-out rights
  - AG rulemaking; $20,000 bond requirement that shall run to the state for any liability arising under subchapter
- **California data brokers are required to begin processing Delete Request and Opt-Out Platform requests beginning August 1, 2026.**

VENABLE LLP

Kids and Minors

- States continue to move beyond COPPA by regulating data pertaining to both children and teens (often under age 18). Key features of state legislation include:
  - Restrictions on targeted advertising to minors
  - Data minimization and privacy-by-default/design requirements
  - Age assurance and age verification mechanisms
  - Limits on addictive design features and harmful content exposure
- **Notable State Approaches**
  - **Age-Appropriate Design Codes** (e.g., California, Maryland, Nebraska) require online services likely accessed by minors to assess and mitigate privacy and safety risks.
  - **Social Media and Online Safety Laws** increasingly require parental consent, age verification or age assurance, or limits on certain platform features.
  - Legislatures are extending requirements to emerging technologies, including **AI-powered services and chatbots**.

VENABLE LLP

App Store Accountability Laws

State	Law	Effective Date
Texas	App Store Accountability Act (SB 2420)	Jan. 1, 2026 (currently subject to litigation; stay on injunction issued in early June)
Alabama	App Store Accountability Act (HB 161)	Jan. 1, 2027
California	Digital Age Assurance Act (AB 1043)	Jan. 1, 2027
Utah	App Store Accountability Act (SB 142, as amended by HB 498)	May 6, 2027
Louisiana	HB 570, as amended by HB 977	July 1, 2027

VENABLE LLP

Colorado AI Act

- **Original Law – SB 24-205 | Signed May 2024**
  - One of the first states to pass comprehensive AI regulation
  - Focused on preventing algorithmic discrimination by high-risk AI systems
  - Applies to developers (creators) and deployers (users) of AI systems
  - "High-risk" = systems making consequential decisions in employment, education, financial services, housing, insurance, and government services
  - Key obligations: impact assessments, risk management, transparency, consumer notification, AG reporting
  - Originally scheduled to take effect February 1, 2026, then delayed to June 30, 2026

- **Amendment – SB 26-189 | Signed May 2026**
  - Significant amendments to original Act
  - Delays effective date to **January 1, 2027**
  - Applies to use of automated decision-making technology to "materially influence" a "consequential decision"
  - Requires developer documentation; deployer record-keeping (at least 3 years after date of consequential decision); deployer disclosures to individuals; access and correction rights and meaningful human review for adverse decisions
  - Enforceable by CO AG; includes a 60-day cure period for non-knowing or repeated violations; includes safe harbor provisions / affirmative defense for entities demonstrating good-faith compliance
  - AG rulemaking required before law's effective date

VENABLE LLP

AI Disclosure/Labeling Example: Generative AI Disclosures

WA HB 1170 (2026)

- **Requires covered providers of GenAI systems to offer a no-cost provenance detection tool.**
- **Disclosure Requirements:**
  - Manifest - Must offer an option for a clear, conspicuous visible disclosure on AI-generated or AI-modified media.
  - Latent - Must include an embedded disclosure where feasible (provider, model/version, timestamp, unique ID). Latent disclosure must be detectable, aligned to widely accepted standards, and hard to remove/recoverable where feasible.
- **Enforcement:** Enforceable by WA attorney general under the Consumer Protection Act; effective date **January 1, 2028**.

VENABLE LLP

AI Synthetic Performer Example: NY Synthetic Performer Act S8420A (2025)

- **Applicable to any person or entity that produces or creates advertising content featuring a "synthetic performer" created or modified by generative AI/algorithmic tools.**
  - Focuses on synthetic humans not recognizable as an "identifiable natural performer" (i.e., not a specific real person).
- **Conspicuous disclosure requirement**, provided the advertiser has **actual knowledge** of the synthetic performer's inclusion**.**
- **Carve-out.** For advertisements and promos of expressive works (e.g., film/TV/streaming/video games) when use matches the underlying work; audio-only ads; use of AI for language translation of a human performer; mediums/outlets such as newspapers, magazines, TV networks and stations, streaming services, cable TV systems, transit advertisements, or billboards.
- **Enforcement:** Civil penalties ($**1k** for first violation; $**5k** for subsequent).
- **Effective Date: June 9, 2026.**

VENABLE LLP

“Surveillance Pricing”

- **Maryland** – effective October 1, 2026
  - Targets food retailers and third-party delivery service providers
  - Prohibits use of personal data to set a higher price for a single consumer or to set a higher personalized price ("dynamic pricing") based on personal data about a consumer
  - Prohibits use of "protected class data" to deny members of that legally protected group a privilege other groups may receive
  - Does not apply to promotional pricing offers, loyalty program benefits, and other temporary discounts or changes to pricing related to retention of existing customers, rewards programs, and cost-based differences, among other exceptions
  - AG enforcement with 45-day cure period; no PRA

VENABLE LLP

“Surveillance Pricing”(cont.)

- **Connecticut** – effective October 1, 2026
  - Disclosure requirement for any business’s use of a “price setting device.” “THIS PRICE WAS INCREASED BY A PRICE SETTING DEVICE USING YOUR PERSONAL DATA.”
  - Ban on retailer sellers and third-party delivery service from engaging in “surveillance pricing,” with exemptions for:
    - Offering a discounted price for the purpose of retaining the consumer as a customer
    - Offering different prices due to justifiable differences in costs and temporal differences
    - Group-based discounts based on publicly disclosed terms and offered to all consumers who are members of a group, including loyalty programs
  - Exemptions for insurers and financial institutions subject to Title V of GLBA
  - UDAP violation; no PRA

“Surveillance Pricing” (cont.)

- **Colorado – VETOED**
  - Bans persons from engaging in “**individualized price setting**” and “**individualized wage setting**”
    - “Individualized price setting” = using a price- or wage-setting algorithm or the output of a price- or wage-setting algorithm in determining a price offered to a consumer
    - A “price- or wage-setting algorithm” or “PWSA” includes any technology, software, program, machine-based system, or computational process that uses statistical modeling, data analytics, AI, or data-processing techniques to analyze “surveillance data” and is a substantial factor in setting or determining a price or wage offered to an individual
    - “Surveillance data” = data obtained through observation, inference, or surveillance of a consumer or worker that is related to personal characteristics, online behaviors, or biometrics of the individual or a group, band, class, or tier to which the individual belongs, including information gathered, purchased, or otherwise acquired
  - **Exemptions:** Allows for differential prices based on cost or temporal differences; allows discounted prices offered on equal terms to all consumers who meet the criteria, discounts to members of broadly defined and publicly recognized groups, and discounts offered on equal terms (e.g., loyalty programs)
  - Requires **development and publication of reasonable procedures** to ensure the accuracy of all data considered by a price- or wage-setting algorithm
  - AG rulemaking and enforcement, *plus* a PRA

California Enforcement Spotlight: Enforcement Priorities

- Clear and Complete Privacy Notices
- Effective Consumer Choice Mechanisms
  - ✓ Opt-out Methods
  - ✓ GPC Signals
  - ✓ Opt-in Consent for U-16 Consumers
- End-to-End Opt-out Compliance
- Contracts and Third-Party Accountability/Controls
- Consumer Rights Processes
- Consumer Verification Processes
- Purpose Limitation Principle / Data Minimization
- Vendor Management and Testing Third-Party Tools
- Cookie Banners
- Heightened Protection for Children's and Teen Data

VENABLE LLP

California Enforcement Spotlight

Global Entertainment and Media Company (February 2026 – CA AG)

- The action resulted in a **$2.75 million fine** and focused on functionality of **opt-outs** and **directing consumers looking to opt out on apps to a web interface**.
- The company did not fully effectuate opt-out choices across devices and services.
    - The company works with third-party adtech partners to target ads for its products on external sites and services and operates its own ad platform for advertisers on the company's streaming services and websites. It provides a webform and toggle for opt-outs and states it honors GPC signals.
    - Opt-outs submitted through the webform were applied only to the company's own ad platform; the company continued sharing data about those consumers with third-party adtech partners.
    - Opt-outs submitted via the toggle or GPC stopped sharing with adtech partners, but only for the specific service and device used to submit the request, even if the consumer was logged into their account.
    - The company would not fully opt a consumer out unless the consumer (1) completed its opt-out webform and (2) individually used the opt-out toggle for *each* service and on *each* device the consumer used, even though the company knew which devices were associated with the user or connected to their account.
    - Citing vendor and technical limitations, the company did not offer in-app opt-outs in many CTV apps, instead directing consumers to its webform—which implemented opt-outs only incompletely.

VENABLE LLP

California Enforcement Spotlight (cont.)

Youth Sports Media Company (March 2026 – CalPrivacy)

- The action resulted in a **$1.1 million fine** and focused on functionality of **opt-outs** and **compliant privacy notices**.
- The company allegedly "forced" Californians, including students, to click "agree" to tracking technologies before they could use their tickets on the platform or view the company's websites, without providing a "sufficient" way to opt out.
- The company allegedly did not fully provide consumer opt-out rights disclosures and effectuate opt-out choices across their websites/mobile apps.
- The company allegedly did not recognize and honor opt-out preference signals.
- The company allegedly did not provide consumers with privacy notices that accurately disclosed their sales of personal information, the consumer rights to opt out of sales/sharing of personal information, and compliant mechanisms for consumers to exercise rights.

VENABLE LLP

California Enforcement Spotlight (cont.)

Global Automotive Manufacturer (March 2026 – CalPrivacy)

- The action resulted in a **$375,703 fine** and focused on **friction in the opt-out process.**
- The company provided a single privacy rights form to consumers and required consumers to submit the same information for all rights, including verifiable consumer rights *and* opt-out rights.
- After a consumer submitted a request through the form, the company displayed a message stating, "One more step! Please confirm your request!" The company asked the consumer to check their email for confirmation, click "confirm," and, after those steps were taken, stated they would "start" the consumer's request.
- For consumers who did check their email, the company presented them with the following message: "We have received your request listed below. For us to complete this request, you must confirm your email and identity by clicking on the button below. Once we have confirmed your identity, we will respond to your request within the legally required time period." Then the company presented consumers with a "Confirm Email" button at the bottom of the message.
- **The company required consumers to verify their identity before they could opt out.**
- The company's practice of requiring consumers to confirm access and control over their email address before processing a request to opt out of sale/sharing impermissibly required consumers to submit a verifiable consumer request and resulted in "unnecessary friction" in the exercise of the opt-out right.
- The company also deemed as "expired" all requests to opt out submitted by consumers who did not click "Confirm Email" in the message. This resulted in the company not processing requests to opt out within the period required by the CCPA. The company therefore sold/shared personal information after consumers requested to opt out.

California Enforcement Spotlight (cont.)

Global Automotive and Mobility Company (May 2026 – CA AG)

- The action resulted in a **$12.75 million fine** and focused on **insufficient disclosures** under the Unfair Competition Law and the False Advertising Law, the CCPA's **purpose limitation principle**, the CCPA's **data minimization** rules, and **failure to provide required rights**.

Lessons Learned

- Disclose all sales of personal information and offer consumers the ability to opt out of such sales.
- Disclose all uses and disclosures of sensitive personal information, provide required notices (e.g., notice of the right to limit), and offer consumers the ability to limit such uses or disclosures, in line with the CCPA.
- **Purpose limitation principle: regulates why data is used or shared**. Use, retain, and/or share personal information in a manner that is reasonably necessary or proportionate to achieving the purposes for which the personal information was collected or processed or for another disclosed purpose that is compatible with the context in which the personal information was collected.
    - Don't collect data for one purpose and sell it for an entirely unexpected and undisclosed purpose.
    - Another "disclosed, compatible" purpose can *never* be a purpose that would violate California law.
- **Data minimization principle: asks whether some or all of the data is necessary in the first instance, or still needed if retained, to accomplish the purpose**.
    - Do not retain data longer than necessary to perform the disclosed purpose or share data for illegal purposes.
    - The action serves as the first time the CA AG has alleged a violation of the CCPA's data minimization terms.

VENABLE LLP

SECURE Data Act, H.R. 8413

What's Good for the States Is Also Good for America			
Core Provisions		**Consensus State Approach**	**H.R. 8413**
Responsible Uses of Data (i.e., Advertising, Fraud Prevention)		✓	✓
Consumer Rights	Access	✓	✓
	Correction	✓	✓
	Deletion	✓	✓
	Portability	✓	✓
Opt Out Rights	Targeted Advertising	✓	✓
	Sales	✓	✓
	Profiling	✓	✓
Data Minimization		✓	✓
State AG Enforcement		✓	✓
No Private Right of Action		✓	✓

VENABLE LLP

Questions?

VENABLE LLP