2025 State Privacy Legislation and Regulation Roundup

July 31, 2025

Mike Signorelli | Venable | masignorelli@Venable.com

Allie Monticollo | Venable | ammonticollo@Venable.com

VENABLE LLP

Agenda

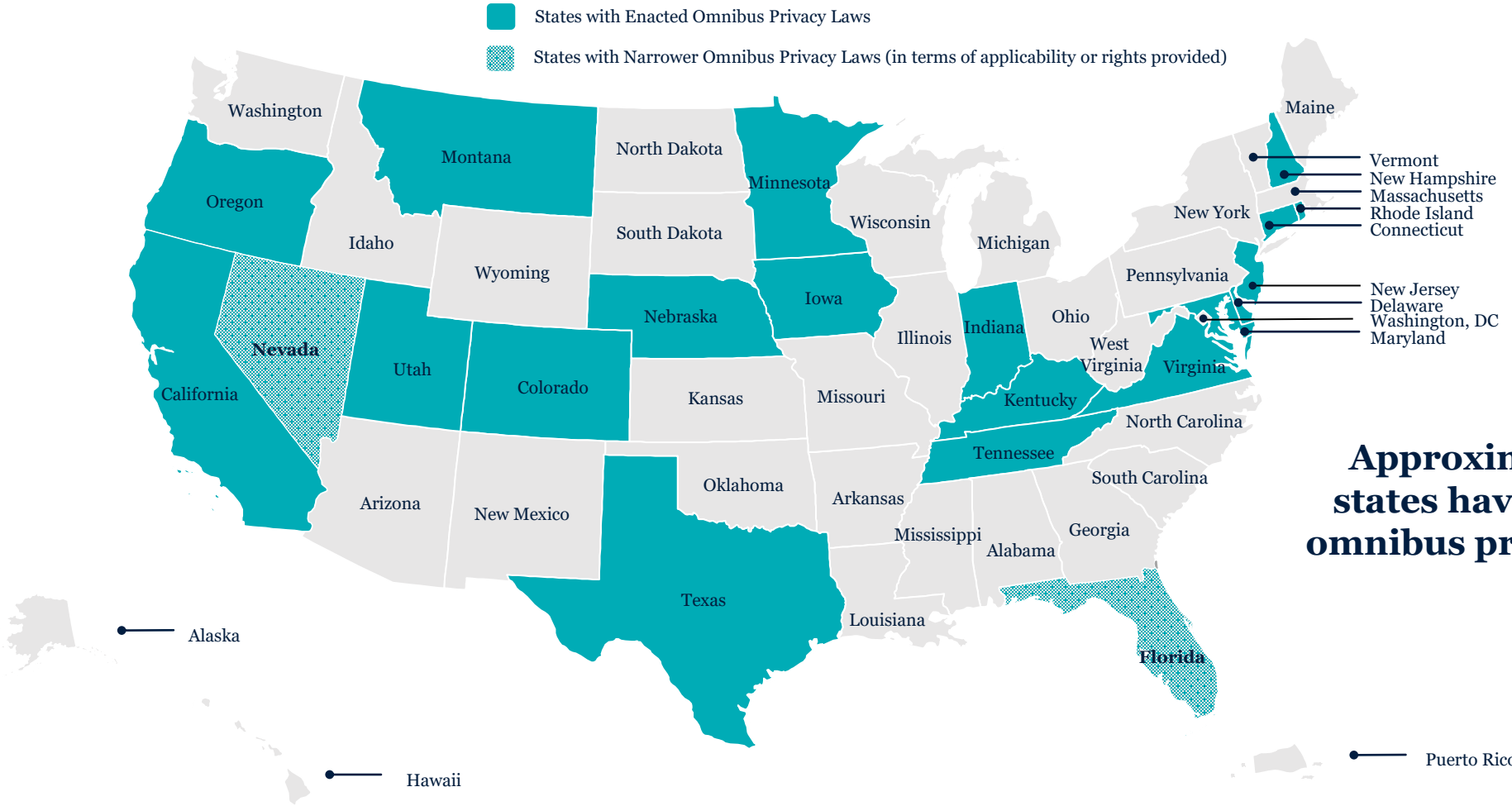
1. Baseline of Privacy Laws in the U.S.
2. 2025 Developments: Amendments, New Laws, and New Regulations
3. Lessons from Enforcement and Counseling

VENABLE LLP

Baseline of Privacy Laws in the U.S.

VENABLE LLP

Omnibus State Privacy Laws as of July 31, 2025

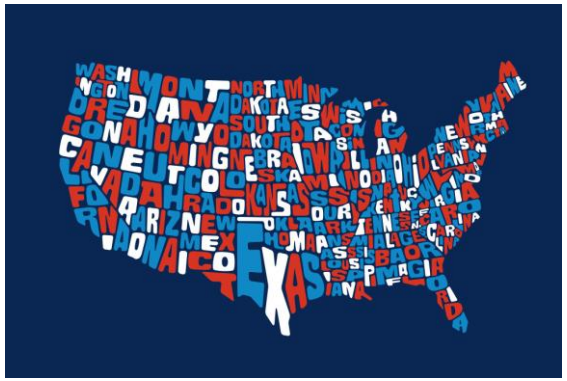


Approximately 21 states have enacted omnibus privacy laws.

VENABLE LLP

State Privacy Law Effective Dates

Omnibus State Privacy Laws: Currently in Effect (17)

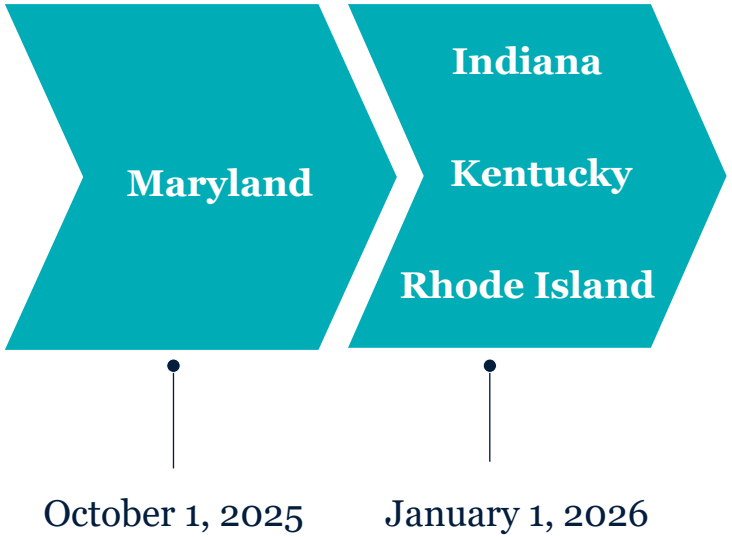


2020:	**CCPA**
2021:	**Nevada**
2022:	**N/A**
2023:	**CPRA, Virginia, Colorado, Connecticut, Utah**
2024:	**Florida, Oregon, Texas, Montana**
2025:	**Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee**
Today:	**Minnesota**

VENABLE LLP

Upcoming Effective Dates

Omnibus State Privacy Laws: Upcoming Effective Dates (4)



VENABLE LLP

Common Themes and Key Differences

- All are “rights-based” laws that focus on notice for consumers as well as rights like:
  - Access, Deletion, Correction, Portability
  - Opt-out of sales/sharing/targeted advertising
  - Opt-in/opt-out from sensitive data processing
- All grant enforcement authority to the state attorney general

- BUT there are also numerous differences:
  - Certain states like CA, CO, and TX require adherence to universal opt-out mechanisms
  - CA regulates cross-context behavioral advertising; other states regulate targeted advertising
  - Certain states, like MN, CT, OR, and RI, require specific disclosures (e.g., list of specific third parties)
  - MD data minimization provisions and ban on sensitive data sales
  - Detailed and prescriptive regulations in CA, CO, and soon NJ

VENABLE LLP

Elements of Omnibus Laws Taking Effect Soon

	Minnesota	Maryland	Indiana	Kentucky	Rhode Island
Rights-based	✓	✓	✓	✓	✓
Opt-out for sales, targeted advertising, profiling	✓	✓	✓	✓	✓
Opt-in for sensitive data processing	✓	✗ (strictly necessary processing standard; ban on sales)	✓	✓	✓
Global privacy controls	✓	✓	✗	✗	✗
PRA	✗	✗	✗	✗	✗
Regulatory authority	✗	✗	✗	✗	✗

VENABLE LLP

Unique Features of Omnibus Laws Taking Effect Soon

- **Minnesota**
  - "A consumer has a right to obtain a **list of the specific third parties** to which the controller has disclosed the consumer's personal data."
  - "**Specific geolocation data**" means "information derived from technology, including… latitude and longitude coordinates or other mechanisms, that **directly identifies the geographic coordinates of a consumer or a device linked to a consumer with an accuracy of more than three decimal degrees of latitude and longitude** or the equivalent in an alternative geographic coordinate system, or a street address derived from the coordinates."
- **Rhode Island**
  - "Any commercial website or internet service provider… shall designate a controller. If a commercial website or internet service provider collects, stores, **and sells** customers' personally identifiable information, then the controller shall, in its customer agreement or incorporated addendum, or **in another conspicuous location on its website or online service platform** where similar notices are customarily posted:…(2) **Identify all third parties to whom the controller has sold or may sell customers' personally identifiable information**…."

VENABLE LLP

Maryland-Specific Provisions

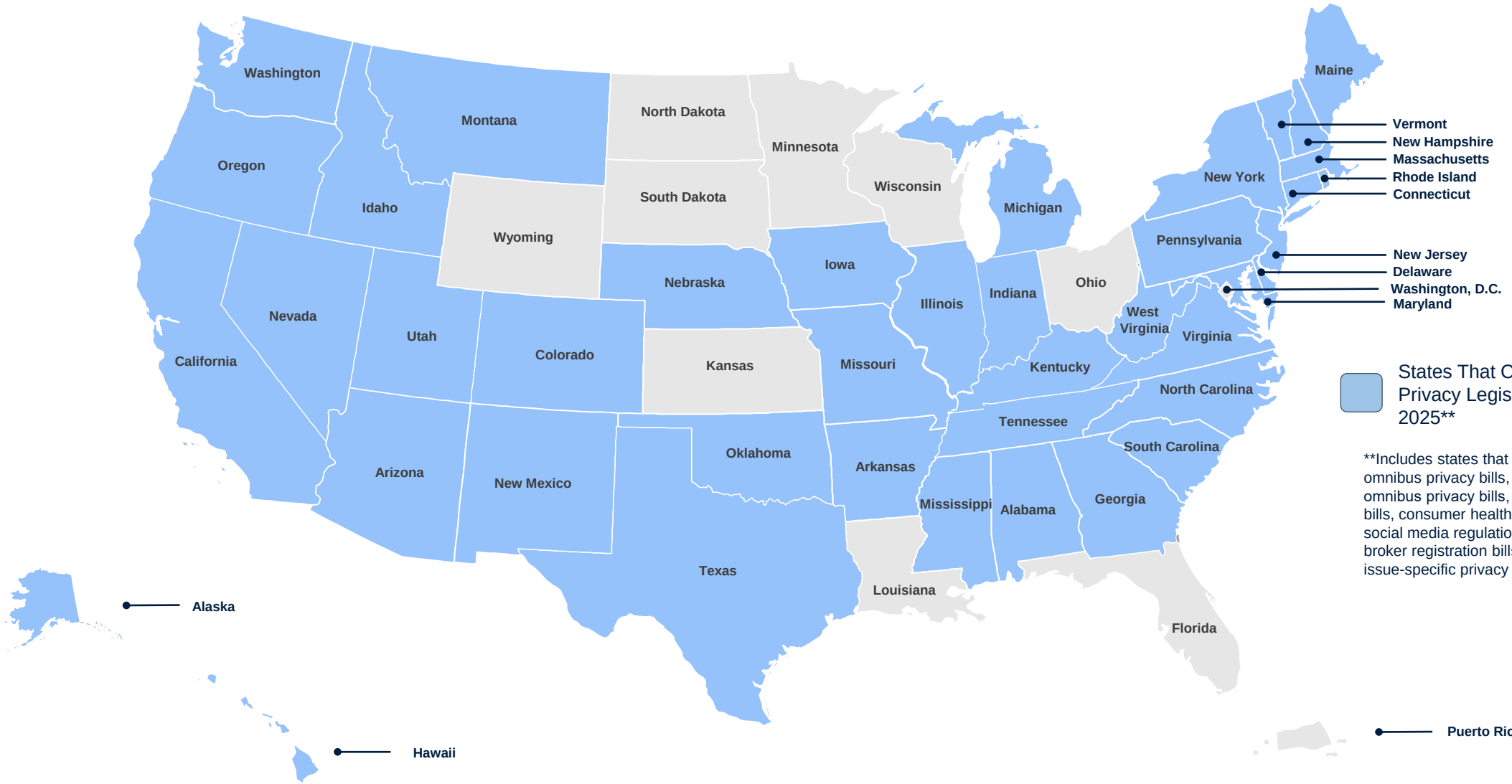
- **Data minimization (personal data):** Personal data collection must be limited to what is *reasonably necessary and proportionate* to provide or maintain a *specific product or service requested* by the consumer.
  - Targeted advertising is permissible subject to an opt-out.
  - How to understand these provisions together, in context?
- **Data minimization (sensitive personal data):** Collection, processing, and sharing must be limited to what is *strictly necessary* to provide or maintain a *specific product or service requested* by the consumer.
- **Ban on sensitive data sales:**
  - Sensitive data includes race or ethnic origin, religious beliefs, consumer health data, sex life, sexual orientation, status as transgender or nonbinary, national origin, citizenship or immigration status, genetic or biometric data, personal data related to a known child, precise geolocation data.
  - Precise geolocation data is "information *derived from technology* that can precisely and accurately identify the *specific location of a consumer* within a radius of 1,750 feet."

VENABLE LLP

2025 Developments: Amendments, New Laws, and New Regulations

VENABLE LLP

States That Have Considered Privacy Legislation in 2025



**Includes states that considered omnibus privacy bills, amendments to omnibus privacy bills, minors' privacy bills, consumer health data bills, social media regulation bills, data broker registration bills, and other issue-specific privacy bills

VENABLE LLP

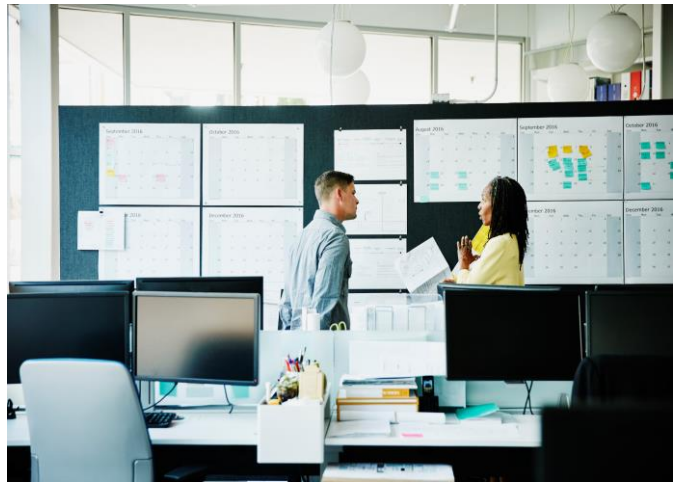
Amendments to Omnibus Privacy Laws

- **Montana** SB 297 (effective October 1, 2025):
  - **Changes applicability thresholds** (law applies to persons who produce products or services targeted to residents of the state and control or process personal data of not less than ~~50,000~~ 25,000 consumers, or ~~25,000~~ 15,000 consumers and derive more than 25% of gross revenue from the sale of personal data)
  - **Narrows the law's nonprofit exemption** to include only those nonprofits established to detect and prevent fraudulent acts in connection with insurance
  - **Removes GLBA entity exemption** and replaces it with a GLBA data exemption
  - **Removes cure period** upon effective date (cure period that would have lasted through April 1, 2026 will now be cut short by 6 months)
- **Kentucky** HB 473 (effective January 1, 2026): Amends health information exemptions in Kentucky Privacy Act.
- **Connecticut** SB 1295 (effective July 1, 2026):
  - **Changes applicability thresholds** (law applies to persons who produce products or services targeted to residents of the state and during the previous calendar year controlled or processed personal data of not fewer than ~~100,000~~ 35,000 consumers~~, or 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data~~; control or process sensitive data; or offer personal data for sale in trade or commerce)
  - **Removes GLBA entity exemption** and replaces it with a GLBA data exemption
  - **New privacy notice requirements**, including requirement to disclose whether the controller collects, uses, or sells personal data for the purpose of training large language models
  - **Adds right to obtain list of third parties** to whom a controller sold personal data
  - **New impact assessment and other requirements** for profiling in furtherance of decisions that produce any legal or similarly significant effect concerning a consumer

VENABLE LLP

Amendments to Existing Laws

- **Texas** SB 2121 and SB 1343 (effective September 1, 2025). Recasts the definition of "data broker" in Texas and adds notice requirements for disclosures through the data broker registry.
  - "**Data broker**" means a business entity **that collects, processes, or transfers** ~~whose principal source of revenue is derived from the collecting, processing, or transferring of~~ personal data that the **business** entity did not collect directly from the individual (TX resident) linked or linkable to the data.
  - [T]his chapter **applies only to a data broker** that, in a 12-month period, derives (1) more than 50 percent of the data broker's revenue **directly** from processing or transferring personal data ~~that the data broker did~~ not **collected by the data broker** ~~collect~~ directly from the individuals to whom the data pertains; or (2) revenue **directly** from processing or transferring the personal data of more than 50,000 individuals ~~that the data broker did~~ not **collected by the data broker** ~~collect~~ directly from the individuals to whom the data pertains.



VENABLE LLP

Amendments to Existing Laws

- **Colorado** SB 25-276 (effective October 1, 2025). Adds a definition of "precise geolocation data" to the Colorado Privacy Act and deems such data "sensitive data." States that a controller may not process *or sell* sensitive data with out first obtaining consent.
    - 6.1.1303. Definitions. As used in this part 13, unless the context otherwise requires: **(17.4) "Precise geolocation data" means information derived from technology that accurately identifies the present or past location of a device that links or is linkable to an individual within a radius of 1,850 feet, including (I) GPS coordinates within a radius of 1,850 feet; or (II) any data derived from a device that is used or intended to be used to locate a consumer within a geographic area within a radius of 1,850 feet.**
    - **Colorado Privacy Act regulations:** "**Revealing**" includes Sensitive Data Inferences. "While precise geolocation information at a high level may not be considered Sensitive Data, *precise geolocation data which is used to infer an individual visited a mosque and is used to infer that individual's religious beliefs* is considered Sensitive Data…. Similarly, *precise geolocation data which is used to infer an individual visited a reproductive health clinic and is used to infer an individual's health condition or sex life is considered Sensitive Data*…." **NOTE**: This provision is subject to potential removal through proposed updates to existing Colorado regulations.
- **Oregon** HB 2008 (effective January 1, 2026). Bans sales of precise geolocation data and sales of personal data associated with U-16s.

VENABLE LLP

New Issue-Specific Laws

- **Virginia** SB 754 (currently effective). Makes obtaining, disclosing, selling, or disseminating any **personally identifiable reproductive or sexual health information** without consumer **consent** a violation of the Virginia Consumer Protection Act, subject to a **PRA**.
    - "Reproductive or sexual health information" means "information relating to the past, present, or future reproductive or sexual health of an individual, including:
        1. Efforts to research or obtain reproductive or sexual health information services or supplies, **including location information that may indicate an attempt to acquire such services or supplies**;
        2. Reproductive or sexual health conditions, status, diseases, or diagnoses, **including pregnancy**, menstruation, ovulation, **ability to conceive a pregnancy**, whether an individual is sexually active, and whether an individual is engaging in unprotected sex;
        3. Reproductive and sexual health-related surgeries and procedures, **including termination of a pregnancy**;

            …

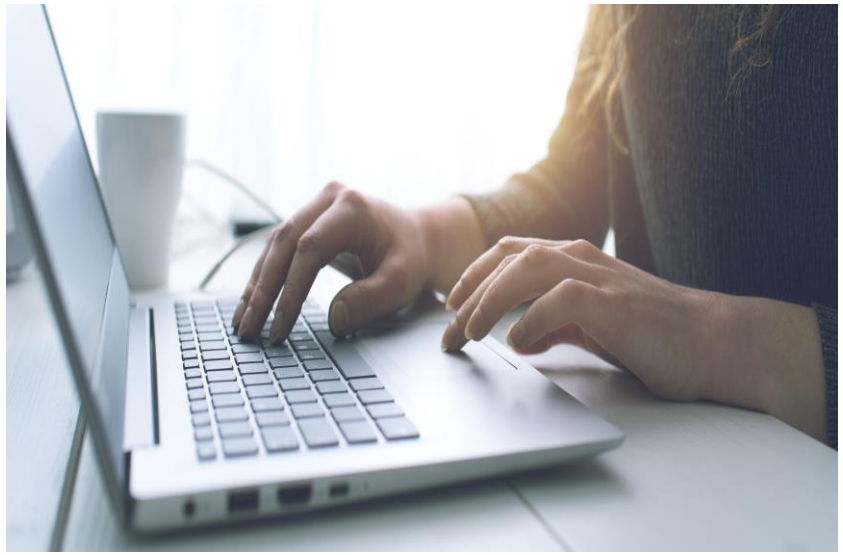
        7. Any information described in [other subsections] that is **derived or extrapolated from non-health related information such as proxy, derivative, inferred, emergent, or algorithmic data**."

VENABLE LLP

New Issue-Specific Laws

- **Arkansas** HB 1717 (effective July 1, 2026). **COPPA 2.0** analog.

- **Nebraska** LB 504 (effective January 1, 2026). **Age-Appropriate Design Code** legislation.



VENABLE LLP

State Legislation – Areas of Focus

- **Amendments to existing omnibus privacy laws**.
- **Location Data**. A California bill would ban collection or use of precise geolocation information of an individual unless doing so is necessary to provide goods or services requested by that individual.
- **Reproductive and Sexual Health Data**. In the wake of the *Dobbs* decision, states are examining ways to protect individuals' access to reproductive and sexual health services. **Some of these bills may have implications for companies aiming to target advertising to new parents as well as companies that collect and process location data**.
- **Surveillance Pricing**. Bills that were considered (or are actively being considered) in California, Colorado, Georgia, and Illinois this year would prohibit setting a price offered to a consumer based, in whole or in part, upon personal information gathered through an electronic surveillance technology.
- **Data Broker Registration and Taxation**. Washington and Maryland bills would have created data broker registries and subject registering companies to new taxes.
  - Massachusetts: "By January 1, 2027, the Office of Consumer Affairs and Business Regulation shall either **partner with the California Privacy Protection Agency** to make available California's accessible deletion mechanism for Massachusetts consumers, in which case a data broker's compliance with said mechanism for Massachusetts consumers shall satisfy the requirements of this paragraph, **or establish an accessible deletion mechanism**…."

VENABLE LLP

Changing Definitions of Data Broker

- **Traditional Definition** (e.g., **Vermont**):
  - "**Data broker**" means a business, or unit or units of a business, separately or together, that knowingly **collects and sells** or licenses to third parties the brokered personal information of a **consumer (VT resident) with whom the business does not have a direct relationship**.
    - **Examples of a consumer with a direct relationship** include a past or present: (i) customer, client, **subscriber, user, or registered user**; (ii) employee, contractor, or agent; (iii) investor; or (iv) donor.
  - "**Brokered personal information**" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:
    - Name of the individual or of a member of their immediate family or household;
    - Address of the individual or of a member of their immediate family or household;
    - Date or place of birth;
    - Mother's maiden name;
    - Biometric data;
    - SSN or other government-issued identification number; or
    - **Other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the individual with reasonable certainty.**

VENABLE LLP

Changing Definitions of Data Broker

- **Traditional Definition** (e.g., **Oregon**):
- "**Data broker**" means a business entity or part of a business entity **that collects and sells** or licenses brokered personal data to another person.
  - A "**data broker" does not include** a business entity that collects information about an individual who is (i) a customer, client, **subscriber, user, or registered user**; (ii) an employee, contractor, or agent; (iii) an investor; (iv) a donor; or (v) in a similar relationship with the business.
- "**Brokered personal data**" means any of the following computerized data elements about an OR resident, if categorized or organized for sale or licensing to another person:
  - Individual's name or name of a member of their immediate family or household;
  - Individual's address or address of a member of their immediate family or household;
  - Individual's date or place of birth;
  - Maiden name of individual's mother;
  - Biometric information about the individual;
  - Social Security number (SSN) or other government-issued ID number;
  - **Other information that, alone or in combination with other information that is sold or licensed, can reasonably be associated with the individual.**

VENABLE LLP

California – Statutory Data Broker Definition

- "**Data broker**" means a business that knowingly **collects and sells** to third parties the personal information of a **consumer (CA resident) with whom the business does not have a direct relationship**.
- This definition appeared in the bill initially passed in 2019 (AB 1202) to establish CA's data broker registry and continues to be CA's statutory definition (as of July 2025).
- Legislative findings in AB 1202 demonstrate that the California legislature **understood an important distinction between businesses with direct relationships with consumers vs. others**:
  - "There are important differences between data brokers and businesses with whom consumers have a direct relationship. Consumers who have a direct relationship with traditional and e-commerce businesses, which could have formed in a variety of ways such as by visiting a business' premises or internet website, or by affirmatively and intentionally interacting with a business' online advertisements, may have some level of knowledge about and control over the collection of data by those businesses, including: the choice to use the business' products or services, the ability to review and consider data collection policies, the ability to opt out of certain data collection practices, the ability to identify and contact customer representatives, and the knowledge necessary to complain to law enforcement.
  - By contrast, consumers are generally not aware that data brokers possess their personal information, how to exercise their right to opt out, and whether they can have their information deleted, as provided by California law."

VENABLE LLP

California – Regulatory Change to "Direct Relationship" (2024)

- The California Privacy Protection Agency (CPPA) promulgated new rules implementing the data broker registration law (which was amended by the Delete Act in 2023). These rules became effective in December 2024.
- The 2024 regulations **fundamentally expand the term's scope by redefining "direct relationship."**
  - "'**Direct relationship**' means that a consumer intentionally interacts with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services within the preceding three years. . . . **A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer**." (emphasis added)

VENABLE LLP

California – Newly Proposed Regulations in 2025

- Through regulations to implement the Delete Request and Opt-Out Platform (DROP) under the California Delete Act, the CPPA has proposed amendments to the regulations to implement CA's data broker registration law.
- These 2025 proposed changes would further expand the scope of "data broker" by again amending the definition of "direct relationship," adding the following:
  - "A business does not have a 'direct relationship' with a consumer simply because it collects personal information directly from the consumer; **the consumer must intend to interact with the business**. **A business is still a data broker and does not have a direct relationship with a consumer as to personal information it sells about the consumer that it collected outside of a 'first party' interaction with the consumer**[.] " (emphasis added)
  - "**First party**" means a consumer-facing business with which the consumer intends and expects to interact.
- This express reference to an intentional, expected interaction could expand the sweep of "data broker" to entities that otherwise may have been able to argue they had a direct relationship.

VENABLE LLP

Maryland (2025 Legislation)

2025 MD legislative proposals that *did not pass* (HB 1089/SB 904) would have taken a different broad approach to defining "data broker" that would have likely swept in even entities that have direct, first-party relationships with consumers.

- "**Data broker**" means any business entity that engages in data brokering.
- "**Data brokering**" means the act of collecting, aggregating, analyzing, **buying, selling, and sharing brokered personal data**.
- "**Brokered personal data**" means any of the following computerized data elements about a MD resident if categorized or organized for sale or licensing to another entity:
  - Individual's name or name of a member of their immediate family or household;
  - Individual's address or address of a member of their immediate family or household;
  - Individual's date or place of birth;
  - Maiden name of individual's mother;
  - Personal data (i.e., any information that is linked or reasonably linkable to an identified/identifiable natural person) about the individual;
  - SSN or other government-issued ID number;
  - **Other information that, alone or in combination with other information that is sold or licensed, can reasonably be associated with the individual.**

VENABLE LLP

Washington (2025 Legislation)

A 2025 WA legislative proposal that *did not pass* (HB 1887) would have taken a different broad approach to defining "data broker" that would have likely swept in even entities that have direct, first-party relationships with consumers.

- "**Data broker**" means any business entity that engages in data brokering (except for (A) consumer reporting agencies, furnishers of consumer reports, or users of consumer data under FCRA, and (B) financial institutions, affiliates, or nonaffiliated third parties to the extent they are subject to regulation under Title V of GLBA).
- "**Data brokering**" means the act of collecting, aggregating, analyzing, **buying, selling, and sharing brokered personal data, irrespective of the business entity's relationship with the resident individual whose data is being brokered**.
- "**Brokered personal data**" means any of the following computerized data elements about a WA resident if categorized or organized for sale or licensing to another entity:
  - Individual's name or name of a member of their immediate family or household;
  - Individual's address or address of a member of their immediate family or household;
  - Individual's date or place of birth;
  - Maiden name of individual's mother;
  - Biometric information about the individual;
  - SSN or other government-issued ID number;
  - **Other information that, alone or in combination with other information that is sold or licensed, can reasonably be associated with the individual.**

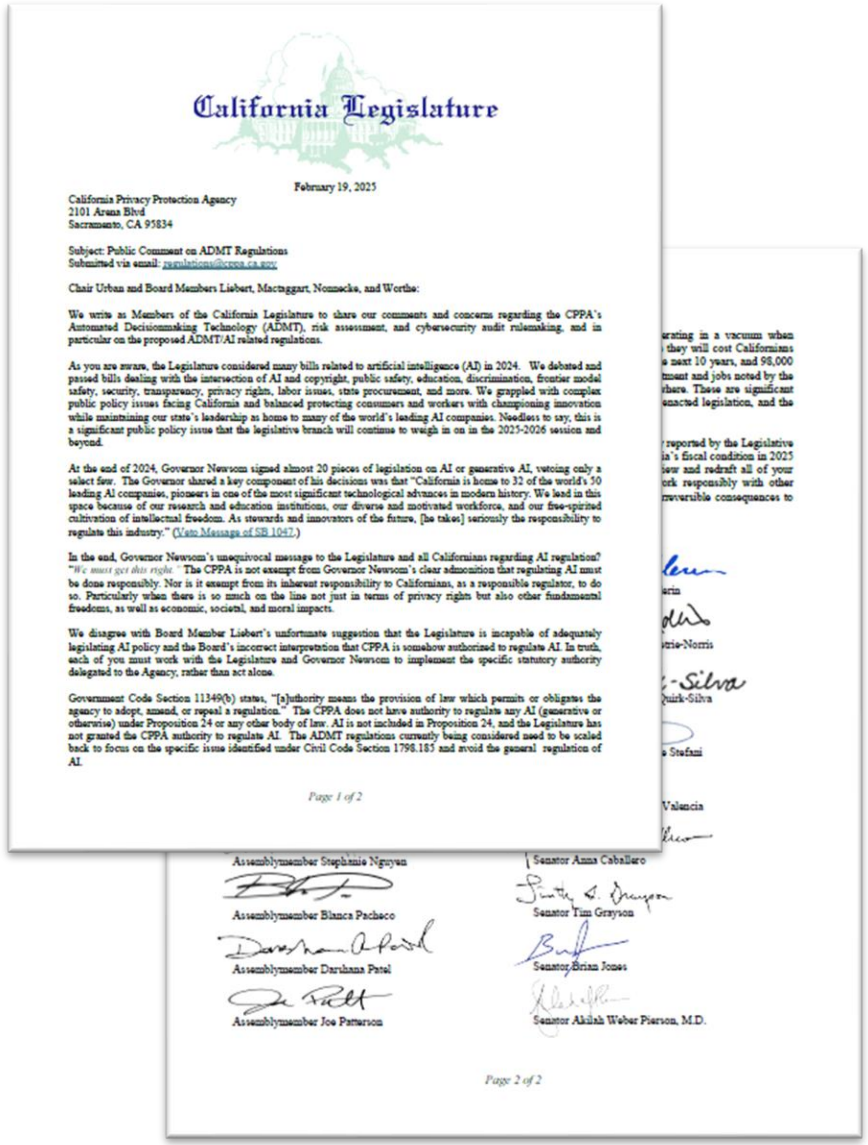
VENABLE LLP

State Regulatory Processes

- **California Privacy Protection Agency** (here and here)
  - Automated Decisionmaking Technology (ADMT)
  - Risk Assessments (sales, sharing, presence in sensitive locations, etc.)
  - Cybersecurity Audits, Insurance Companies, Amendments to Existing CCPA Regulations
  - Delete Request and Opt-Out Platform (DROP)
  - Updating definition of "direct relationship," impacting the state's data broker definition
  - *On July 24, 2025, the CPPA voted to **advance the ADMT/CCPA regulations rules to the CA OAL** and **advance an updated version of the proposed DROP regulations for comment**.*

- **Colorado Department of Law** (here and here)
  - Proposed updates to regulations implementing the Colorado Privacy Act regarding data associated with minors.
  - *Comments in response to the proposed updates are due September 10, 2025.*

- **New Jersey Division of Consumer Affairs** (here)
  - Notice at collection requirements
  - Consent required for use of personal data in AI (no definition for AI)
  - "Immediate" deletion button option
  - *Comments on regulatory proposal are due September 2, 2025.*



California Legislature

February 19, 2025

California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

Subject: Public Comment on ADMT Regulations
Submitted via email: regulations@cppa.ca.gov

Chair Urban and Board Members Liebert, Mactaggart, Nonnecke, and Worthe:

We write as Members of the California Legislature to share our comments and concern regarding the CPPA's Automated Decisionmaking Technology (ADMT), risk assessment, and cybersecurity audit rulemaking, and in particular on the proposed ADMT/AI related regulations.

As you are aware, the Legislature considered many bills related to artificial intelligence (AI) in 2024. We debated and passed bills dealing with the intersection of AI and copyright, public safety, education, discrimination, frontier model safety, security, transparency, privacy rights, labor issues, state procurement, and more. We grappled with complex public policy issues facing California and balanced protecting consumers and workers with championing innovation while maintaining our state's leadership as home to many of the world's leading AI companies. Needless to say, this is a significant public policy issue that the legislative branch will continue to weigh in on in the 2025-2026 session and beyond.

At the end of 2024, Governor Newsom signed almost 20 pieces of legislation on AI or generative AI, vetoing only a select few. The Governor shared a key component of his decisions was that "California is home to 32 of the world's 50 leading AI companies, pioneers in one of the most significant technological advances in modern history. We lead in this space because of our research and education institutions, our diverse and motivated workforce, and our free-spirited cultivation of intellectual freedom. As stewards and innovators of the future, [he takes] seriously the responsibility to regulate this industry." (Veto Message of SB 1047.)

In the end, Governor Newsom's unequivocal message to the Legislature and all Californians regarding AI regulation? "*We must get this right.*" The CPPA is not exempt from Governor Newsom's clear admonition that regulating AI must be done responsibly. Nor is it exempt from its inherent responsibility to Californians, as a responsible regulator, to do so. Particularly when there is so much on the line not just in terms of privacy rights but also other fundamental freedoms, as well as economic, societal, and moral impacts.

We disagree with Board Member Liebert's unfortunate suggestion that the Legislature is incapable of adequately legislating AI policy and the Board's incorrect interpretation that CPPA is somehow authorized to regulate AI. In truth, each of you must work with the Legislature and Governor Newsom to implement the specific statutory authority delegated to the Agency, rather than act alone.

Government Code Section 11349(b) states, "[a]uthority means the provision of law which permits or obligates the agency to adopt, amend, or repeal a regulation." The CPPA does not have authority to regulate any AI (generative or otherwise) under Proposition 24 or any other body of law. AI is not included in Proposition 24, and the Legislature has not granted the CPPA authority to regulate AI. The ADMT regulations currently being considered need to be scaled back to focus on the specific issue identified under Civil Code Section 1798.185 and avoid the general regulation of AI.

Page 1 of 2

Assemblymember Stephanie Nguyen
Senator Anna Caballero
Assemblymember Blanca Pacheco
Senator Tim Grayson
Assemblymember Darshana Patel
Senator Brian Jones
Assemblymember Joe Patterson
Senator Akilah Weber Pierson, M.D.

Page 2 of 2

VENABLE LLP

Lessons from Enforcement and Counseling

VENABLE LLP

State Enforcement: California

- Recent enforcement actions against **Healthline**, **Todd Snyder**, and **Honda** provide useful compliance lessons.
  - **Honda** (Mar. 7, 2025): **CPPA** issued a decision requiring Honda to change its business practices and pay a **$632,500** fine.
  - **Todd Snyder** (May 1, 2025): **CPPA** issued a decision requiring Todd Snyder to change its business practices and pay a **$345,178** fine.
  - **Healthline** (July 1, 2025): **California attorney general** settled with website publisher Healthline, including **$1.55 million** in civil penalties and injunctive terms prohibiting Healthline from sharing article titles that reveal that a consumer may have already been diagnosed with a medical condition (banning the company from engaging in these types of data transmissions).

VENABLE LLP

State Enforcement: California

- Lessons from recent California enforcement:
  - **Consumer Verification**. Collect only what you need to verify and do not verify opt-out requests. *See* Honda, Todd Snyder.
  - **Contracting and Vendor Oversight**. Ensure contracts reflect required terms and conduct due diligence regarding vendors' compliance with opt-out signals. *See* Honda, Healthline.
  - **Functionality of Opt-Out Mechanisms**. Test opt-out methods and mechanisms to ensure they are functioning as intended. *See* Todd Snyder, Healthline.
  - **Observe Purpose Limitation Requirements**. Use of personal data should be consistent with the reasonable expectations of a consumer. *See* Healthline.
  - **Update Privacy Policies with Necessary Specificity**. Generic privacy policy disclosures may be insufficient for health targeting. *See* Healthline.

State Enforcement: California

Entity	Fine	Enforcement Entity and Claim
Accurate Append	$55,400	CPPA: Failure to register as data broker
Healthline Media LLC	$1.55 million	CA AG: CCPA violations
Jerico Pictures, Inc. d/b/a National Public Data	$46,000	CPPA: Failure to register as data broker
Todd Snyder, Inc.	$345,178	CPPA: CCPA violations
Honda Motor Co.	$632,500	CPPA: CCPA violations
Background Alert, Inc.	$50,000	CPPA: Failure to register as data broker
Key Marketing Advantage	$55,800	CPPA: Failure to register as data broker
PayDae, Inc. d/b/a Infillion	$54,200	CPPA: Failure to register as data broker
The Data Group	$46,600	CPPA: Failure to register as data broker
Growbots, Inc.	$35,400	CPPA: Failure to register as data broker
UpLead LLC	$34,400	CPPA: Failure to register as data broker
Tilting Point Media LLC	$500,000	CA AG: CCPA violations
Delivery Service	$375,000	CA AG: CCPA violations
Sephora	$1.2 million	CA AG: CCPA violations

VENABLE LLP

State Enforcement: Connecticut

- **TicketNetwork**: On July 8, 2025, the CT AG announced a settlement related to allegations that the company's privacy notice was largely unreadable, was missing key data rights, and contained rights mechanisms that were misconfigured or inoperable. TicketNetwork agreed to comply with CTDPA, maintain metrics for consumer rights requests received under the CTDPA, provide a report of these metrics to the CT AG, and pay **$85,000**.
- **Connecticut Updated Enforcement Report** (Apr. 17, 2025):
  - **Privacy Notices**: Suggests incorporation of CTDPA and specific reference to the law's consumer data rights.
  - **Marketing and Advertising**: Discusses cremation company sending mailer to a CT resident who recently completed chemotherapy. Signals focus on data services companies/analytics firms/data brokers that identify individuals for marketing lists.
  - **Connected Vehicles**: Discusses a cure notice the CT AG sent to a car manufacturer resulting in updates to the company's privacy notice to clarify personal data collected from consumers vs. employees; notes the CT AG has since expanded its review to include other car manufacturers, and those matters remain ongoing.
  - **Problematic Opt-Out Mechanisms/Dark Patterns**: Suggests focus on cookie banners and symmetry of choice (AGREE or ACCEPT ALL COOKIES button to opt in vs. SHOW PURPOSES button and additional choice points to opt out).
  - Other topics addressed include **facial recognition technology (FRT)**, **biometric data**, **genetic data**, **palm recognition**, **data associated with teens and minors**, **consumer health data**, and **UOOMs**.

VENABLE LLP

Cookies, Online Trackers, and Wiretapping Lawsuits

- Recent **surge in lawsuits alleging wiretapping claims** in the context of use of cookies, online tracking technologies, and session replay technology.
  - Two-party consent states; allegations are grounded in need for **consent** from both parties to a communication.
- State law requirements require **careful construction of cookie banners and related disclosures.**
  - Banner should be unavoidable and functional. *See* Healthline.
  - Symmetry of choice and "Accept all" button vs. multiple steps for opting out. *See* CT Enforcement Report, Honda.
  - Avoid dark patterns and consumer confusion; cookies should not fire before banner is presented. *See* CT Enforcement Report, Todd Snyder.
  - Off-the-shelf products and vendor solutions require review and **customization**. *See* Todd Snyder.
- California SB 690 (not yet enacted) would add a **commercial business purpose exception** to the California Invasion of Privacy Act to stem the tide of these lawsuits.

VENABLE LLP

Data Brokers

- **Enforcement consideration**: The CPPA has brought approximately 10 enforcement actions for data brokers' failure to register, with monetary penalties of up to $55,800 and at least one action resulting in an order for the company to "cease and desist from operating as a data broker" for three years or pay a $50,000 fine.
- **Compliance consideration**: What data is being provided? Each state's data broker law and data broker definition is different. Some state data broker laws apply to transfers of "brokered personal data." Other state laws apply to personal information or personal data more broadly.
- **Compliance consideration**: Definitions are beginning to encompass entities with **direct or first-party** consumer relationships. *See* California and New Jersey (proposed).
- California Delete Request and Opt-Out Platform (DROP) **rules related to treating deletion requests as opt-out requests** may result in broad application of requests. ("*If a data broker associates multiple consumers with a matched identifier from the consumer deletion list, the data broker* ***must opt each associated consumer out of the sale or sharing of their personal information***.")
  - A proposed amendment to California SB 361 (not yet enacted) would require disclosure of the "**unique identifiers** a data broker uses to **associate personal information with a consumer**."
- **Authorized agents** and submission of requests through the California DROP.
  - California SB 302 (not yet enacted) would require the CPPA to submit deletion requests on behalf of all **elected officials** and **judges**.

VENABLE LLP

Questions?

VENABLE LLP

VENABLE LLP