SQUIRE PATTON BOGGS

Privacy World

Keeping you informed on the evolving law on data privacy, security and innovation.

State Privacy Law Patchwork Presents Challenges

By Alan Friel & Julia Jacobson on June 10, 2024

State legislatures across the country were busy in 2023 and so far this year passing comprehensive consumer privacy laws and creating a vexing patchwork of compliance obligations.

Legislatures in Iowa, Indiana, Tennessee, Montana, Florida, Texas, Oregon, Delaware, New Jersey, New Hampshire, Kentucky, Maryland, Nebraska and Minnesota all enacted consumer privacy laws of their own with an additional consumer privacy law in Vermont awaiting action by the Governor. The fifteen laws passed in 2023 and 2024 join laws in California, Virginia, Colorado, Utah, and Connecticut which already are in effect. A chart at the end of this blog post notes each law's effective date, **three of which** are effective at the end of this month.

While inspired by the EU General Data Protection Regulation and the California Consumer Privacy Act ("CCPA"), the new state consumer privacy laws take materially different approaches in many ways. States also have passed more targeted privacy laws pertaining specifically to **consumer health data** (beyond treating it as a category of sensitive personal data), the protection of children (beyond limiting the use of personal data), **AI-specific laws** (not part of a comprehensive consumer data regime) and laws regulating data brokers (typically controllers that sell personal data they do not directly collect from consumers). Congress continues to consider a **federal law** that would mostly preempt the state consumer privacy laws, as well as other laws specific to children's online safety with partial preemption. In the meantime, data controllers (and to a lesser degree processors) face the challenge of determining which state consumer privacy laws apply and whether to apply applicable laws based on consumer residency or to apply a national highest standard to all consumers.

The SPB privacy team has developed a comprehensive guide on state consumer privacy laws, including comparison charts on key issues to help determine which laws apply and tips for enhancing information governance. Most of the new state consumer privacy laws require controllers to conduct and retain documentation of data privacy impact or risk assessments. Minnesota's new consumer privacy law also requires a documented privacy compliance program reasonably designed to ensure compliance and data inventories. The most recent draft of the federal privacy law mandates privacy-by-design.

Following are some highlights of the emerging 'high water mark' (strictest requirement) for key aspects of consumer privacy in the United States:

Sensitive Personal Data:

- Most of the state consumer privacy laws require opt-in (rather than opt-out as in CCPA) consent for sensitive personal data processing except for processing necessary for certain permitted uses (e.g., to provide a requested product or service, comply with law or legal process, etc.). The state consumer privacy laws of Utah and Iowa require a controller to provide consumers with clear notice and an opportunity to opt out before processing

sensitive data. California offers consumers a "limit processing of sensitive personal information" right.

- The state consumer privacy laws of Texas and Florida require an affirmative statement, clearly and conspicuously given, when a controller/website sells sensitive personal data.
- The Maryland Online Data Privacy Act bans the sale of sensitive personal data of minors (under the age of 18). Vermont's pending[1] state consumer privacy law bans all sales of sensitive personal data.
- The following categories of sensitive personal data are recognized by the CCPA/CPRA:
    - Government Issued Identification Numbers (e.g., social security, driver's license, state identification card or passport number)
    - Financial Data (a consumer's account log-in, financial account, debit card or credit card number in combination with any required security or access code, password or credentials allowing access to an account)
    - Precise Geolocation (data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet)
    - Personal Characteristics/Protected Classes (racial or ethnic origin, religious or philosophical beliefs, citizenship or immigration status or union membership)
    - Communication Content (the contents of a consumer's mail, email and text messages unless the Business[2] is the intended recipient of the communication)
    - Genetic Data
    - Biometric Information processed for the purpose of uniquely identifying a consumer
    - Health Information (i.e., personal information collected and analyzed concerning a consumer's health[3])
    - Sex Life/Sexual Orientation (i.e., personal information collected and analyzed concerning a consumer's sex life or sexual orientation)
- The other state privacy laws include various new sensitive personal data categories:
    - Children's Data: personal data collected from a known "child." The standard for knowledge and, as more fully explained below, the age of a "child" varies under state laws, i.e., under the age of 16, 17 or 18. Based on the federal Children's Online Privacy Protection Act ("COPPA"), all state privacy laws treat a minor under the age of 13 as a child subject to parental consent for online personal data collection. Unlike COPPA,

however, the state privacy laws apply to personal data *about* the child collected *offline* and online. Some states limit the processing of children's data regardless of the consent of the minor or his/her parent[4].

- Consumer Health Data, which is a term that applies to a broader set of personal data or is subject to greater restriction than the CCPA's definition of health data, such as gender-affirming health data and reproductive or sexual health data.
- Data revealing a person's status as a victim of a crime[5].
- Inferences from non-sensitive data that can reveal data that is sensitive data[6].
- Precise Geolocation (the new state laws designate a radius that is within 1,750 feet of the data subject, and Minnesota has an expansive definition that goes beyond a mere area radius.)
- Transgender or nonbinary status.

Children / Teens:

All of the state consumer privacy laws require verified parental consent to process personal data for targeted advertising of children under age 13. California requires consent of a consumer at least age 13 but under age 16 for processing personal data. Other states apply more stringent standards:

- Consent for targeted advertising, sale and/or profiling: Oregon (under age 16) and New Jersey (under age 17)
- Consent for processing and/or selling of sensitive personal data: Florida (under age 18)
- Consent for targeted advertising or sale: Delaware (under age 18)
- Prohibition of targeted advertising or sale: Maryland (under age 18)

Vermont's pending privacy law includes data minimization requirements for processing of minors (under age 18) personal data by online services.

Several states also have **online child and teen safety laws** that go beyond data privacy, several of which are facing First Amendment challenges.

Consumer rights:

The Oregon consumer privacy law includes a consumer right allowing individuals to obtain, at a controller's option, "a list of specific third parties, other than natural persons, to which the controller has disclosed: (i) the consumer's personal data; or (ii) any personal data." Like Oregon's law, the state consumer privacy laws of Minnesota and Vermont each add a consumer right to obtain a list of personal data disclosure recipients, but, unlike the Oregon law, neither the Minnesota law nor the Vermont law include the option of a consumer-specific list (if/as possible).

Delaware's consumer privacy law entitles consumers to information on the third parties to which their personal data is sold on a category basis, rather than a list of specific third parties. Maryland's consumer privacy law grants a consumer the right to request a list of the categories of third parties to which the controller has disclosed the consumer's personal data or, if the controller does not maintain this information on a consumer-specific basis, the categories of third parties to which the controller has disclosed the consumer's personal data.

The state privacy laws also vary as to the methods of processing consumer rights requests, including verification standards, timing and appeals.

The pending Vermont law adds a limited private right of action applicable to data brokers and large data handlers related to sensitive personal data or its processing without consent. This private right of action is currently effective on January 1, 2027 and expires two years later. CCPA also has a private right of action which is limited to claims for certain data security incidents attributable to failure to maintain reasonable security. Watch Privacy World for a more in-depth analysis of the new laws in Minnesota and Vermont.

For more information or to inquire about our guidance resources for client, please contact the authors.

	Effective Date	**Enforcement Date**	**Rulemaking Details/Status of Regulations**
CCPA / CPRA	January 1, 2020/January 1, 2023	July 1, 2023	**Regulations** were finalized by the California Privacy Protection Agency (CPPA). The CPPA also published **draft regulations** about cybersecurity audits, risk assessments and automated decision-making

	Effective Date	Enforcement Date	Rulemaking Details/Status of Regulations
			but has not completed the formal rulemaking process.
Virginia Law	January 1, 2023	January 1, 2023	None. No statutory rulemaking authority granted.
Colorado Law	July 1, 2023	July 1, 2023	Final CPA Rules were finalized by the Colorado Attorney General and filed with the Secretary of State on March 15, 2023. The CPA Rules went into effect on July 1, 2023.
Utah Law	December 31, 2023	December 31, 2023	The Utah law requires the Attorney General to compile a report by July 1, 2025, that evaluates liability and enforcement provisions and details a summary of data protected (and not) by the Utah Law but otherwise does not provide explicitly for rulemaking.
Connecticut Law	July 1, 2023	July 1, 2023	None yet, but potentially coming.
Iowa Law	January 1, 2025	January 1, 2025	Seemingly none. No statutory rulemaking authority granted.
Indiana Law	January 1, 2026	January 1, 2026	Seemingly none. No statutory rulemaking authority granted.

	Effective Date	Enforcement Date	Rulemaking Details/Status of Regulations
Tennessee Law	July 1, 2025	July 1, 2025	Seemingly none. No statutory rulemaking authority granted.
Montana Law	October 1, 2024	October 1, 2024	Seemingly none. No statutory rulemaking authority granted.
Florida Law	July 1, 2024	July 1, 2024	Statutory rulemaking granted to the Florida attorney general who is required to adopt rules to implement the Florida Law, including "standards for authenticated consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf."
Texas Law	July 1, 2024	July 1, 2024	Seemingly none. No statutory rulemaking authority granted.
Oregon Law	July 1, 2024	July 1, 2024	Seemingly none. No statutory rulemaking authority granted.
Delaware Law	January 1, 2025	January 1, 2025	Seemingly none. No statutory rulemaking authority granted.
New Jersey Law	January 15, 2025	January 15, 2025	Additional regulations necessary to enforce the purpose of the New Jersey Law may be forthcoming from the Director of the

	Effective Date	Enforcement Date	Rulemaking Details/Status of Regulations
			Division of Consumer Affairs, including rules and regulations regarding a universal opt-out mechanism which is as consistent as possible with the approach taken in other states. (§ 8.b.(2)(d)).
New Hampshire Law	January 1, 2025	January 1, 2025	No – no explicit requirement for rulemaking. The New Hampshire Attorney General has rule-making authority with respect to privacy notice requirements, which is the only rule-making authority available (§ 507-H:6, III).
Kentucky Law	January 1, 2026	January 1, 2026	Seemingly none. No statutory rulemaking authority granted.
Maryland Law	October 1, 2025	April 1, 2026	Seemingly none. No statutory rulemaking authority granted.
Nebraska Law	January 1, 2025	January 1, 2025	Seemingly none. No statutory rulemaking authority granted.
Vermont Law	July 1, 2025, with some aspects later effective, and the PRoA available only from 1/1/27 – 1/1/29	July 1, 2025	Limited rulemaking for data broker security breach provisions

	Effective Date	Enforcement Date	Rulemaking Details/Status of Regulations
Minnesota Law	July 1, 2025	July 1, 2025	Seemingly none. No statutory rulemaking authority granted.

Disclaimer: While every effort has been made to ensure that the information contained in this article is accurate, neither its authors nor Squire Patton Boggs accepts responsibility for any errors or omissions. The content of this article is for general information only, and is not intended to constitute or be relied upon as legal advice.

---

1. The Vermont Governor has until ~ June 13th to sign, veto or not take action on the Vermont Data Privacy Act as passed by the Vermont legislature. ↩
2. A defined term in CCPA ↩
3. The definition of "health data" varies among the state privacy laws, with other states adding specific subcategories. ↩
4. Recognized category in Colo. Rev. Stat. § 6-1-1311 (24)(c), Conn. Gen. Stat. § 42-515(38)(D), Del. Code § 12D-101 (30)(c),Ind. Code 24-15 (28)(3), Ky. Rev. Stat. 367 § 28(c), Md. Ann. Code § 14–4601 (GG)(X), Minn. Stat. 5 § 325O.02 (v)(c),Neb. L.B. 1074, 108th Leg. § (1)(30)(c),N.H. Rev. Stat. Ann. LII § 507-H:1 (XXVIII), N.J. Stat. Ann. 56 § 8-166.4 (1),Or. Rev. Stat. § 180.095 (18)(a)(B),Tenn. Code § 47-18-3302 (26)(C), Va. Code § 59.1-571 (3), and Vt. Stat. Ann. 9 § 2415 (54)(I). ↩
5. Recognized category in Or. Rev. Stat. § 180.095 (18)(a)(C) and Vt. Stat. Ann. 9 § 2415 (54)(D). ↩
6. Colorado, Montana. ↩