



# MAKING SENSE OF THE PATCHWORK OF U.S. STATE CONSUMER PRIVACY LAWS



**BY  
ALAN L.  
FRIEL**



**&  
SASHA  
KIOSSE**

Alan Friel is the Chair of Squire Patton Boggs' Global Data Practice, based in Los Angeles, and Sasha Kiosse is an associate in the firm's New York office.

### A WIN FOR EUROPEAN REGULATORS ON DIGITAL PRIVACY

By Mark MacCarthy



### THE GDPR: THE GOOD, THE BAD, THE UGLY

By Cedric Burton, Laura Brodahl & Hattie Watson



### MAKING SENSE OF THE PATCHWORK OF U.S. STATE CONSUMER PRIVACY LAWS

By Alan L. Friel & Sasha Kiosse



### COOKIE CONSENT IS BROKEN: TIME FOR A NEW PRIVACY PROTECTION MODEL

By Omar Vasquez Duque



### PERSONAL DATA EXPLOITATION AS EXCESSIVE PRICING: A REVIEW OF THE BUNDESKARTELLAMT FACEBOOK CASE

By Sebastián Cañas



### MAKING SENSE OF THE PATCHWORK OF U.S. STATE CONSUMER PRIVACY LAWS

By Alan L. Friel & Sasha Kiosse

California was the first state to enact comprehensive consumer privacy legislation in 2018. Since then, 19 other states have done so, but have added to or subtracted from California's approach. California has also amended its law, and has and continues to promulgate regulations that add obligations for businesses and rights for consumers. Enterprises need to determine which of these laws apply to them, and how to reconcile the differences between the laws, or adopt a high-water mark approach. As enterprises prepare their annual privacy notice updates, a requirement under the California law, now is a good time to confirm what additional state laws apply and ensure compliance with those that are, or will become in 2025, applicable.

Visit [www.competitionpolicyinternational.com](http://www.competitionpolicyinternational.com)  
for access to these articles and more!

**Scan to Stay Connected!**

Scan here to subscribe to CPI's  
**FREE** daily newsletter.





## INTRODUCTION

As of the date of this article, 19 states have followed the lead of California and passed consumer privacy laws. While there are many similar aspects to these laws, they also diverge from each other, creating a compliance challenge for organizations. Federal legislative efforts to create a federal floor or ceiling have not been successful; however, this may change with the Republicans gaining control of the House, Senate and Presidency. In the meantime, this article outlines key aspects of U.S. comprehensive state consumer personal information/data<sup>2</sup> privacy laws (collectively, “state consumer privacy laws”<sup>3</sup>), but does not discuss other privacy laws pertaining specifically to consumer health data,<sup>4</sup> laws specific to children’s and minors’ personal data and not part of a comprehensive consumer privacy law,<sup>5</sup> AI-specific laws,<sup>6</sup> or laws, including part of overall consumer privacy laws, regulating data brokers.<sup>7</sup>

The key aspects of state consumer privacy laws are summarized by topic below and comparison charts are included at the end of the article. Since California requires annual privacy notice updates many companies will be updating their policies for 2025, which is a good time to address the laws that became effective in 2024 or will come into effect next year.

**Jurisdictional Scope and Applicability:** Organizations should consider whether each of the state consumer privacy laws apply to them. Some state consumer privacy laws include high thresholds that may cause them to be inapplicable to many organizations. Texas and Nebraska have the lowest thresholds, applying regardless of the number affected residents, but applying fewer terms to small businesses. Florida’s thresholds are particularly high, though certain of its provisions relating to sensitive personal data may apply to organizations that do not meet such thresholds. Table 2 out-

lines basic applicability thresholds, but the state consumer privacy laws also include various data-level and entity-level exemptions that vary.

**Effective Dates, Enforcement, Rulemaking, etc.:** The newer of the twenty state consumer privacy laws go into effect between July 1, 2024, and early 2026. See Table 1 for more details.

**HR and B-to-B Data:** Human resources (“HR”) and business to business (“B-to-B”) personal information have been in scope under the California Consumer Privacy Act (“CCPA”) since January 1, 2023. So far, the CCPA is the only state consumer privacy law that requires compliance for these types of data subjects. The remaining state consumer privacy laws provide various exemptions or exceptions as to this kind of data, the effect of which is to exclude HR and B-to-B data from their scope.

**Privacy Policies and Notice at Collection:** Privacy policies that were drafted to address compliance with the CCPA or Colorado Law will generally suffice for compliance with the other state consumer privacy laws, since these laws are the two most prescriptive in terms of privacy policy content requirements. However, there are notices required by a few states that go beyond the California/Colorado requirements and updates may be needed to address new requirements under other state consumer privacy laws, such as with respect to consumer rights. Rhode Island has specific online privacy policy requirements that apply to online service providers even if other provisions of the law do not, and also requires website notice of the parties to which personal data is or may be sold. Texas and Florida require enhanced notice of sensitive personal data sales on controllers’ websites. The CCPA is the only state privacy law that includes prescriptive and specific notice at collection requirements, though the other state consumer privacy laws likely implicitly require a similar practice.

**Consumer rights:** Oregon, Delaware, Minnesota, and Maryland include a consumer right that is not found in the other

2 The California Consumer Privacy Act uses the term “personal information” whereas the other state consumer privacy laws use the term “personal data.” Although the definitions vary somewhat, these terms are used interchangeably in this article.

3 Please see [Table 1](#) at the end of this article for an alphabetical list of the state consumer privacy laws and their effective dates.

4 For example, Washington’s My Health My Data Act and a similar Nevada law. See <https://www.privacyworld.blog/2024/04/are-you-ready-for-washington-and-nevadas-consumer-health-data-laws>.

5 For example, the California Age-Appropriate Design Code Act (“CA AADCA”). See <https://www.privacyworld.blog/2023/10/california-attorney-general-appeals-federal-court-ruling-that-online-child-safety-act-is-likely-unconstitutional/> and <https://www.privacyworld.blog/2023/07/texas-two-steps-into-the-childrens-privacy-dance-the-securing-children-online-through-parental-empowerment-act/>. A 9<sup>th</sup> Circuit federal Court of Appeals decision has struck down the risk assessment and abatement provisions of CA AADCA, and laws making favored and disfavored content distinctions for minors face similar challenges. See <https://www.privacyworld.blog/2024/08/are-data-practice-risk-assessments-at-risk-in-the-us/>.

6 For example, Colorado’s Artificial Intelligence (AI) law (C.R.S. 6-1-1701).

7 A data broker is typically a controller that sells personal data that the controller did not collect directly from consumers. CA, NV, VT, OR and TX all regulate data brokers. VT and NV do not have broad consumer privacy laws and do so on a separate basis.

state consumer privacy laws. This new right requires controllers to provide consumers with a list of third-party recipients of personal data (in effect parties to which the personal data is sold since processors are not within the definition of a third party), though the requirements vary across these states' laws. The Oregon 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 (i.e., a generic list that is not specific to the consumer)." The Minnesota Law adds a similar consumer right. However, rather than the choice between a list of specific third-party recipients receiving the specific consumer's personal data or *any* personal data, based on the controller's election, the Minnesota Law requires providing the specific third parties that receive the consumer's personal data, if the controller maintains the personal data in a particular format that allows for the identification of the specific third-party data recipients for each requesting consumer. Under the Delaware Law, consumers are entitled to receive from controllers the categories of third parties to which personal data is made available. Under the Maryland Law, a consumer can request a list of the categories of third parties to which the controller has disclosed the specific 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 any consumer's personal data. As noted above, Rhode Island requires information on third party recipients in the privacy notice rather than as a consumer request right.

The state consumer privacy laws also vary as to the processing of consumer rights requests, including verification standards, timing, and requirements to provide appeal rights. Table 3 summarizes consumer rights and corresponding controller / business obligations.

**Data Processing Agreements and Third-Party Accountability / Risk Management:** The European Union's General Data Protection Regulation ("GDPR")-inspired controller/processor scheme in the non-California state consumer privacy laws that came into effect in 2023 was likely new for organizations that were not required to comply with the GDPR and, in some respects, involves a different analysis than the business/service provider construct of the CCPA—requiring significant work on the vendor management aspect of compliance. Thankfully, the more recently passed state consumer privacy laws do not materially differ from the original four in respect of contracting or other requirements for controller / processor relationships.

California is the only state privacy law that effectively requires specific contract terms be in place when personal data is sold or shared (for cross-context behavioral advertising) with third parties. Note that this is a different requirement from the

contractual language required under the state consumer privacy laws with respect to service providers/processors. It is clear from many of the state consumer privacy laws (and also recent enforcement by the Federal Trade Commission) that, in addition to entering into agreements with specific provisions, organizations must demand accountability from vendors, partners, and other data recipients. For example, the CCPA provides that businesses that do not invoke audit provisions with data recipients may not be able to afford themselves of a safe harbor from liability if the recipient uses its personal data in violation of law. Moreover, the Data Assessment requirements clearly require input from external stakeholders, such as vendors and other recipients of personal data. Put simply, contractual provisions are not enough to mitigate privacy and security risk with respect to data recipients.

---

***The state consumer privacy laws also vary as to the processing of consumer rights requests, including verification standards, timing, and requirements to provide appeal rights"***

---

**Opt-Out Preference Signals / Universal Opt-Out Mechanisms:** By January 1, 2025, eight states will require controllers to receive and process opt-out preference signals / universal opt-out mechanisms – browser signals that express opt-out preferences. By Jan. 1, 2026, at least four more states will require this.

**Sensitive Personal Data:** Some of the new state consumer privacy laws have expanded the categories of personal data which are considered sensitive, and some provide heightened obligations or restrictions as to sensitive personal data, including Maryland's prohibition on the sale of sensitive data with no consent exception. Some of the material changes regarding sensitive personal data are listed immediately below.

- Most state consumer privacy laws require opt-in consent for processing sensitive personal data. California, Utah, and Iowa each, however, provide for an opt-out regime. The opt-in and opt-out requirements do not apply to processing for certain exempt purposes, which vary across the state laws.
- The Texas Law and Florida Law each require a specifically worded notice if the controller sells sensitive personal data.
- The Maryland Law prohibits sales of sensitive personal data.

- The other state consumer privacy laws include various new sensitive personal data categories:<sup>8</sup>
- Children's Data: personal data of, or collected from, a known child.<sup>9</sup> Based on the federal Children's Online Privacy Protection Act ("COPPA"), all state consumer privacy laws treat any consumer under age 13 as a child subject to parental consent; unlike COPPA, however, the state consumer privacy laws apply to personal data collected from a child both online and offline, as opposed to personal data collected from a child online. Moreover, the Florida Law defines "child" as under 18, and the Delaware, Maryland, and Oregon Laws define as sensitive data personal data collected both from a child and of a child.<sup>10</sup> Maryland prohibits the sale and targeted advertising involving minor personal data, and Delaware has limits on online marketing of certain age-limited products to minors, with no consent exceptions.<sup>11</sup>
- Under the majority of state consumer privacy laws, health related data is a sub-set of sensitive data; some of the state laws require such data to "reveal" a consumer's mental or physical health condition or diagnosis, while the CCPA defines as sensitive personal information "personal information collected and analyzed concerning a consumer's health." Connecticut, Nevada and Washington have taken a drastically different approach than the state consumer privacy laws, providing a defined term "consumer health data" in their respec-

tive laws, with broader and more restrictive obligations on regulated entities processing the same.<sup>12</sup>

- Data revealing a person's status as a victim of a crime.<sup>13</sup>
- Precise Geolocation (the non-CCPA state laws designate a 1,750 foot radius, and the CCPA has a radius of 1,850 feet. However, Minnesota's definition is "information derived from technology, including but not limited to, global positioning level latitude and longitude coordinates or other mechanisms, that directly identifies the geographic coordinates of a consumer or device linked to a consumer with an accuracy of more than three (3) decimal degrees of latitude and longitude (e.g. 360 feet) or the equivalent in an alternative geographic system, or street address derived from those coordinates.)
- Transgender or nonbinary status.

**Children / Teens:** Since its inception in 1998, the Children's Online Privacy Protection Act ("COPPA") has been the cornerstone of protecting the personal data of minors under the age of 13 in the United States. COPPA imposes various requirements, including parental consent, notice and transparency, and data minimization, among other things, on online services that are "directed to children [under 13]" and "mixed audience" online services, or those that have actual knowledge that they have collected personal data from a child [under 13] online.

Many organizations that previously did not have to worry about COPPA or COPPA-based standards as applied to

8 The following categories of sensitive personal data are recognized by the CCPA:

- Government Issued Identification Numbers (e.g., social security, driver's license, state identification card, or passport number)
- Account Access 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 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)
- Sex Life/Sexual Orientation (i.e., personal information collected and analyzed concerning a consumer's sex life or sexual orientation)

9 Recognized category in Colo. Rev. Stat. § 6-1-1311 (24)(c), Conn. Gen. Stat. § 42-515 (38)(D), Del. Code § 12D-101 (30)(c), Fla. § 501.701, Ind. Code 24-15 (28)(3), Iowa Code § 715D.1, Ky. Rev. Stat. 367 § 28(c), Md. Ann. Code § 14-4601 (GG)(X), Minn. Stat. 5 § 325O.02 (v)(c), Mont. Code Ann. § 30-14-2801, Neb. L.B. 1074, 108<sup>th</sup> 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), Tex. Bus. & Com. Code Ann. § 541.001, Va. Code § 59.1-571 (3), and RI. S 2500 6-48.1-2(26).

10 Florida defines "child" as under 18, while the remaining state laws align with COPPA's under 13 standard, at least as it concerns to definitions of sensitive data. The Delaware, Maryland, and Oregon Laws cover children's data more broadly than the other state laws, also including personal data of *or about a child* (rather than just collected from) in their definitions of sensitive data.

11 The Maryland Law prohibits the sale and targeted advertising involving personal data of consumers under age 18. In Delaware, controllers cannot process sensitive data concerning a known child (under age 13) without first obtaining consent from the child's parent or guardian, and complying with another Delaware law (§ 1204C of Chapter 12C of title 6). § 1204C generally restricts an operator of a website, online or cloud computing service, online application or mobile application directed to minors (under age 18) from marketing or advertising, or engaging in other activities that would result in the marketing or advertising, of products or services related to alcohol, tobacco, firearms, drugs, piercings and tattoos, lotteries and other similar products or services to minors (under age 18).

12 Per above, this article does not go into detail into laws or amendments covering consumer health data.

13 Recognized category in Or. Rev. Stat. § 180.095 (18)(a)(C).


state consumer privacy laws should be aware of the trend in state consumer privacy laws to expand restrictions and obligations beyond COPPA's under age 13 standard, to minors that are at least 13 and under the age of 18 ("Teens"). This trend began in 2020 with the CCPA requiring consent for sale of personal information of consumers at least age 13 but younger than 16 years of age (the CPRA expanded that requirement to sharing as well). Consent must be given by the Teen or, if the consumer is under age 13, by the parent, using COPPA verification standards. Other relevant aspects regarding this trend, of which organizations should be aware, include:

- **There are now ten state consumer privacy laws that provide specific requirements and obligations as to Teens' personal data.** Ten state consumer privacy laws expand the treatment of minor data beyond COPPA's under 13 standard to Teens. These laws provide various ranges from 13 to 17 years of age (e.g., at least age 13 but younger than 16, 17 or 18).
- **Controller's actual knowledge of age is not required in many of these states.** Many of these states notably do not require a controller to have actual knowledge of age for the obligations to apply. Rather, they apply a "willful disregard" and/or a "knew or should have known" standard that prohibit businesses from turning a blind eye to the collection and processing of Teens' personal data. Provisions in privacy policies and terms of service stating that a website or service is not intended for, or restricting the use of the website or service by, users under 18 will likely not prevent organizations from violating these new requirements where a company willfully disregards or knew or should have known that it had Teen users or customers. This is reflective of how the FTC determines, for COPPA purposes, if an online service is directed at children under 13, or a general audience site – the latter having an actual knowledge standard and the former requiring a presumption that users are under 13.
- **Maryland prohibits the sale and targeted advertising involving minor (consumers under age 18) personal data, with no consent exceptions.**
- **The remaining states require consent for sale and targeted advertising involving Teens' personal data; Connecticut's SB3 provides additional consent requirements.** The general trend in many of these states is to require consent for certain processing involving Teens' personal data, such as for sale or targeted advertising. Consent must be obtained from the minors themselves unless the minor is under 13, in which case COPPA's "verifiable parental consent" standard applies. Connecticut's SB3, which amends its general consumer privacy law (*and notably contains provisions that went into effect on July 1 and October 1, 2024*), provides restrictive data minimization provisions that

require consent in other contexts, including for any processing of minor data beyond what is required to provide a product or service requested by a consumer.

- **The Scope of Child / Teen Personal Data Varies.** The states are broader in scope than COPPA as to both Teens' and children's (under 13) personal data. California and other state consumer privacy laws have anchored certain of their consumer privacy rights and obligations regarding personal data about children, regardless of from whom the personal data is collected (rather than regulating only personal data collected from a child as set forth in COPPA). Moreover, the state privacy laws regulate personal data collected offline, whereas COPPA only applies to personal data collected online.

---

 ***There are now ten state consumer privacy laws that provide specific requirements and obligations as to Teens' personal data"***

---

Profiling and Automated Decision-Making: With the exception of Utah and Iowa, profiling and automated decision-making are or will become regulated to some degree under state consumer privacy laws. Forthcoming CCPA regulations<sup>14</sup> will likely provide the most onerous restrictions and obligations on this topic.

Assessments and Data Inventories: Most of the 2023 and 2024 state consumer privacy laws (excluding the Iowa Law and Utah Law) require formal, documented privacy impact assessments to be conducted for various "high risk" data practices, and that a controller make assessments available for inspection. The California Privacy Protection Agency has proposed regulations requiring that assessments are filed in abridged form with its office. The Minnesota Law goes a step further, requiring documented personal data inventories and a documented privacy compliance program sufficient to reasonably ensure compliance.

Data Minimization and Secondary Use: Excepting Utah, Iowa, and Rhode Island, the state consumer privacy laws include both data minimization and secondary use provisions. Specifically, Utah only has secondary use requirements, while both Iowa and Rhode Island only have data minimization requirements. Data minimization provisions prohibit controllers from collecting personal data (and in the case of California, collecting and processing personal

---

<sup>14</sup> See <https://www.privacyworld.blog/2024/11/navigating-californias-evolving-privacy-landscape-key-updates-from-the-november-8th-cppa-board-meeting-on-rulemaking-and-what-it-means-for-you/>.



information) beyond certain purposes or purposes that are reasonably necessary and proportionate to such purposes. There are varying standards in the state consumer privacy laws, with Maryland having the most restrictive. Secondary use is a related concept and generally prohibits controllers from processing personal data for purposes that were not disclosed to the consumer unless the controller obtains consent. Note that California requires consent if sensitive personal information is used outside of permitted processing purposes enumerated under regulations.

**Data Retention:** Data retention schedules are explicitly required under the CCPA and are necessary for compliance more generally with the state consumer privacy laws that both do and do not explicitly require them. Data retention schedules must be understood and disclosed on a category-by-category basis for CCPA. Minnesota requires a description of data retention programs in a controller's privacy notice, and all of the states' data minimization requirements implicate the need for retention and defensible destruction programs. As a result, covered businesses will need to develop very detailed retention schedules that include purposes of processing and which are tied to categories of data, as well as a defensible destruction program. This differs from what public organizations must maintain as it relates to retention programs and schedules under Securities and Exchange Commission regulations and other laws which require organizations to maintain certain records for legal compliance purposes (like OSHA accident records or tax-related records), though these are a good starting point. The CCPA requires such retention schedules be available for consumers to review at the point of data collection, which can be satisfied by a deep link to a compliant privacy policy schedule. Therefore, it will be apparent to enforcement authorities which organizations have insufficient retention schedules by merely sweeping website privacy notices or other pre-collection notices. While published retention schedules are not required by the other state consumer privacy laws, their purpose limitation and data minimization principles make such a tool helpful, if not essential, in ensuring personal data is not retained longer than needed for each purpose stated at collection or processed for purposes beyond those that were disclosed to data subjects.

**Documentation of Data Privacy Programs:** Minnesota requires a defined and documented data privacy compliance program under the supervision of a chief privacy officer or other individual with primary responsibility for directing the program, and Tennessee offers a limited safe harbor if a company's privacy program is consistent with the NIST or other equivalent privacy program approaches.

**Enforcement:** Other than the CCPA in relation to security breaches, none of the state consumer privacy laws provide for a private right of action. The state consumer privacy laws are generally enforceable by the respective states' attorneys general and, in some cases, other state regulators.

**Regulations:** So far, only California and Colorado have promulgated regulations under their state consumer privacy laws, but other states may (and in some cases must) do so. California's rulemaking is ongoing, including regarding assessments, cybersecurity audits, automated decision making, profiling and proposed amendments to the existing regulations.

Enterprises need to determine which of these laws apply to them, and how to reconcile the differences between the laws, or adopt a high water mark approach. As enterprises prepare their annual privacy notice updates, a requirement under the California law, now is a good time to confirm what additional state laws apply and ensure compliance with those that are, or will become in 2025, applicable. The charts that follow can assist in doing so. For more information, contact the authors.

---

***Data retention schedules are explicitly required under the CCPA and are necessary for compliance more generally with the state consumer privacy laws that both do and do not explicitly require them***

---

Table 1

State Name and Link to Law	Consumer Privacy Law Title	Effective Date	
<a href="#">California</a>	California Consumer Privacy Act, as amended by the California Privacy Rights Act ( <b>CPRA</b> ) (collectively, <b>CCPA</b> )	Initial CCPA Effective Date: January 1, 2020 CPRA amendments Effective Date: January 1, 2023	
<a href="#">Colorado</a>	Colorado Privacy Act ( <b>Colorado Law</b> )	July 1, 2023	
<a href="#">Connecticut</a> <sup>15</sup>	Connecticut Data Privacy and Online Monitoring Act ( <b>Connecticut Law</b> )	July 1, 2023	
<a href="#">Delaware</a>	Delaware Personal Data Privacy Act ( <b>Delaware Law</b> )	January 1, 2025	
<a href="#">Florida</a>	Florida Digital Bill of Rights ( <b>Florida Law</b> )	July 1, 2024	
<a href="#">Indiana</a>	Indiana Consumer Data Protection Act ( <b>Indiana Law</b> )	January 1, 2026	
<a href="#">Iowa</a>	Act Relating to Consumer Data Protection ( <b>Iowa Law</b> )	January 1, 2025	
<a href="#">Kentucky</a>	Kentucky Consumer Data Protection Act ( <b>Kentucky Law</b> )	January 1, 2026	
<a href="#">Maryland</a>	Maryland Online Data Privacy Act ( <b>Maryland Law</b> )	October 1, 2025	
<a href="#">Minnesota</a>	Minnesota Consumer Data Privacy Act ( <b>Minnesota Law</b> )	July 31, 2025*	
<a href="#">Montana</a>	Montana Consumer Data Privacy Act ( <b>Montana Law</b> )	October 1, 2024	
<a href="#">Nebraska</a>	Data Privacy Act ( <b>Nebraska Law</b> )	January 1, 2025	
<a href="#">New Hampshire</a>	Act Relative to the Expectation of Privacy ( <b>New Hampshire Law</b> )	January 1, 2025	
<a href="#">New Jersey</a>	Act Concerning Online Services, Consumers, and Personal Data ( <b>New Jersey Law</b> )	January 15, 2025	
<a href="#">Oregon</a>	Oregon Consumer Privacy Act ( <b>Oregon Law</b> )	July 1, 2024	**
<a href="#">Rhode Island</a>	Rhode Island Data Transparency and Privacy Protection Act ( <b>Rhode Island Law</b> )	January 1, 2026	
<a href="#">Tennessee</a>	Tennessee Information Protection Act ( <b>Tennessee Law</b> )	July 1, 2025	
<a href="#">Texas</a>	Texas Data Privacy and Security Act ( <b>Texas Law</b> )	July 1, 2024	
<a href="#">Utah</a>	Utah Consumer Privacy Act ( <b>Utah Law</b> )	December 31, 2023	
<a href="#">Virginia</a>	Virginia Consumer Data Protection Act ( <b>Virginia Law</b> )	January 1, 2023	

<sup>15</sup> The General Statutes of Connecticut are supplemented as of January 1, 2024 [here](#).



**Table 2**

Who is Covered?	
<b>CCPA CPRA</b>	<p>For-profit “businesses” that meet thresholds, including affiliates, joint ventures, and partnerships that:</p> <ul style="list-style-type: none"> <li>(1) have a gross global annual revenue of &gt; U.S. \$25 million;</li> <li>(2) annually buy, sell, or “share” for cross-context behavioral advertising purposes PI of 100,000 or more California consumers or households; or</li> <li>(3) derive 50% or more of annual revenues from selling or “sharing” for cross-context behavioral advertising PI of California consumers.</li> </ul> <p>Non-profit exception from the term “Business.”</p>
<b>Virginia Law</b>	<p>Business entities, including for-profit and B-to-B entities, that conduct business in Virginia or produce products or services that target Virginia residents and, during a calendar year, either:</p> <ul style="list-style-type: none"> <li>(1) control or process personal data of at least 100,000 Virginia residents; or</li> <li>(2) derive 50% of gross revenue from the sale of personal data and control or process personal data of at least 25,000 Virginia residents.</li> </ul> <p>Full non-profit exception.</p>
<b>Colorado Law</b>	<p>Any legal entity that conducts business in Colorado or produces or delivers commercial products or services that intentionally target Colorado residents, and that satisfies one or both of the following:</p> <ul style="list-style-type: none"> <li>(1) during a calendar year, controls, or processes personal data of 100,000 or more Colorado residents; or</li> <li>(2) both derives revenue or receives discounts from selling personal data and processes or controls the personal data of 25,000 or more Colorado residents.</li> </ul>
<b>Utah Law</b>	<p>Controllers or processors who:</p> <ul style="list-style-type: none"> <li>(1) conduct business in Utah or produce a product or service targeted to Utah residents;</li> <li>(2) have annual revenue of U.S. \$25 million or more; and</li> <li>(3) (a) control or process data of 100,000 or more Utah residents in a calendar year; or</li> <li>(b) derive over 50% of gross revenue from the sale of personal data and control or process personal data of 25,000 or more Utah residents.</li> </ul> <p>Full non-profit exception.</p>
<b>Con- necticut Law</b>	<p>Individuals and entities that do business in Connecticut or produce products or services that are targeted to Connecticut residents, that in the preceding year either:</p> <ul style="list-style-type: none"> <li>(1) controlled or processed the personal data of at least 100,000 Connecticut residents (excluding for the purpose of completing a payment transaction); or</li> <li>(2) controlled or processed the personal data of at least 25,000 Connecticut residents and derived more than 25% of gross annual revenue from the sale of personal data.</li> </ul>
<b>Iowa Law</b>	<p>Persons conducting business in Iowa or producing products or services that are targeted to consumers who are residents of Iowa and that, during a calendar year, either:</p> <ul style="list-style-type: none"> <li>(1) control or process personal data of at least 100,000 consumers; or</li> <li>(2) both control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.</li> </ul> <p>Full non-profit exception.</p>
<b>Indiana Law</b>	<p>Persons that:</p> <ul style="list-style-type: none"> <li>(1) conduct business in Indiana or produce products or services that are targeted to Indiana residents; and</li> <li>(2) during a calendar year, (a) control or process the personal data of at least 100,000 consumers who are Indiana residents; or (b) control or process the personal data of at least 25,000 consumers who are Indiana residents and derive more than 50% of gross revenue from the sale of personal data.</li> </ul> <p>Full non-profit exception.</p>
<b>Tennes- see Law</b>	<p>Persons that conduct business in Tennessee producing products or services that target Tennessee residents and that:</p> <ul style="list-style-type: none"> <li>(1) exceed \$25 million in revenue; and</li> <li>(2) (a) control or process the personal information of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal information; or (b) during a calendar year, control, or process personal information of at least 175,000 consumers.</li> </ul> <p>Full non-profit exception.</p>

Who is Covered?	
Montana Law	<p>Persons that:</p> <p>(1) conduct business in Montana or produce products or services that are targeted to Montana residents; and</p> <p>(2) (a) control or process the personal data of at least 50,000 consumers, excluding personal data collected or processed solely for the purpose of completing a payment transaction; or (b) control or process the personal data of at least 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data.</p> <p>Full non-profit exception.</p>
Florida Law	<p>(1) Controllers, which are defined as any sole proprietorship, partnership, LLC, corporation, association, or legal entity that meets the following requirements:</p> <p>(a) is organized or operated for the profit or financial benefit of its shareholders or owners;</p> <p>(b) conducts business Florida;</p> <p>(c) collects personal data about consumers, or is the entity on behalf of which such information is collected;</p> <p>(d) determines the purposes and means of processing personal data about consumers or jointly with others;</p> <p>(e) makes in excess of \$1 billion in global gross annual revenues; and</p> <p>(f) satisfies at least one of the following:</p> <p>(i) derives 50% or more of its global gross annual revenues from the sale of advertisements online, including targeted advertising or the sale of ads online;</p> <p>(ii) operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation. For purposes of this sub-paragraph, a consumer smart speaker and voice command component service does not include a motor vehicle or speaker or device associated with or connected to a vehicle which is operated by a motor manufacturer or a subsidiary or affiliate thereof; or</p> <p>(iii) operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.</p> <p>(2) Any entity that controls or is controlled by a controller. As used in this paragraph, the term “control” means:</p> <p>(a) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a controller;</p> <p>(b) control in any manner the election of a majority of the directors, or of individuals exercising similar functions; or</p> <p>(c) the power to exercise a controlling influence over the management of a company.</p> <p>Full non-profit exception.</p>
Texas Law	<p>Persons that:</p> <p>(1) conduct business in Texas or produce a product or service consumed by Texas residents;</p> <p>(2) process or engage in the sale of personal data; and</p> <p>(3) are not a small business as defined by the U.S. Small Business Administration.</p> <p>Full non-profit exception.</p>
Oregon Law	<p>Persons that:</p> <p>(1) conduct business in Oregon, or provide products or services to residents of Oregon; and</p> <p>(2) during a calendar year, control, or process (a) the personal data of at least 100,000 consumers, other than personal data controlled or processed solely for the purpose of completing a payment transaction; or (b) the personal data of at least 25,000 consumers, while deriving at least 25% of annual gross revenue from the sale of personal data.</p> <p>Limited non-profit exception.</p>
Delaware Law	<p>Persons that:</p> <p>(1) conduct business in Delaware or produce products or services that are targeted to Delaware residents; and</p> <p>(2) during the preceding calendar year did any of the following:</p> <p>(a) controlled or processed the personal data of at least 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or</p> <p>(b) controlled or processed the personal data of at least 10,000 consumers and derived more than 20% of their gross revenue from the sale of personal data.</p> <p>Limited non-profit exception.</p>
New Jersey Law	<p>Controllers that:</p> <p>(1) conduct business in New Jersey or produce products or services that are targeted to New Jersey residents; and</p> <p>(2) during the calendar year did any of the following:</p> <p>(a) controlled or processed the personal data of at least 100,000 consumers (excluding personal data processed solely for the purpose of completing a payment transaction); or</p> <p>(b) controlled or processed the personal data of at least 25,000 consumers and derived revenue or received a discount on the price of any goods or services from the sale of personal data.</p>

Who is Covered?	
<b>New Hampshire Law</b>	<p>Persons that:</p> <ul style="list-style-type: none"> <li>(1) conduct business in New Hampshire or produce products or services that are targeted to New Hampshire residents; and</li> <li>(2) during a one-year period did any of the following: <ul style="list-style-type: none"> <li>(a) controlled or processed the personal data of at least 35,000 unique consumers (excluding personal data processed solely for the purpose of completing a payment transaction); or</li> <li>(b) controlled or processed the personal data of at least 10,000 unique consumers and derived more than 25% of their gross revenue from the sale of personal data.</li> </ul> </li> </ul> <p>Full non-profit exception.</p>
<b>Kentucky Law</b>	<p>Persons that:</p> <ul style="list-style-type: none"> <li>(1) conduct business in Kentucky or produce products or services that are targeted to Kentucky residents; and</li> <li>(2) during a calendar year did any of the following: <ul style="list-style-type: none"> <li>(a) controlled or processed the personal data of at least 100,000 consumers; or</li> <li>(b) controlled or processed the personal data of at least 25,000 consumers and derived more than 50% of their gross revenue from the sale of personal data.</li> </ul> </li> </ul> <p>Full non-profit exception.</p>
<b>Maryland Law</b>	<p>Persons that:</p> <ul style="list-style-type: none"> <li>(1) conduct business in Maryland or produce products or services that are targeted to Maryland residents; and</li> <li>(2) during the preceding calendar year did any of the following: <ul style="list-style-type: none"> <li>(a) controlled or processed the personal data of at least 35,000 consumers (excluding personal data processed solely for the purpose of completing a payment transaction); or</li> <li>(b) controlled or processed the personal data of at least 10,000 consumers and derived more than 20% of their gross revenue from the sale of personal data.</li> </ul> </li> </ul> <p>Limited non-profit exception.</p>
<b>Nebraska Law</b>	<p>Persons that:</p> <ul style="list-style-type: none"> <li>(1) conduct business in Nebraska or produce products or services that are consumed by Nebraska residents; and</li> <li>(2) processes or engages in the sale of personal data; and</li> <li>(3) is not a small business, as determined by federal law.</li> </ul> <p>Full non-profit exception.</p>
<b>Rhode Island Law</b>	<p>For-profit entities that:</p> <ul style="list-style-type: none"> <li>(1) conduct business in Rhode Island or produce products or services that are targeted to Rhode Island residents; and</li> <li>(2) during the preceding calendar year did any of the following: <ul style="list-style-type: none"> <li>(a) controlled or processed the personal data of at least 35,000 Rhode Island residents (excluding personal data processed solely for the purpose of completing a payment transaction); or</li> <li>(b) controlled or processed the personal data of at least 10,000 Rhode Island residents and derive more than 20% of the gross revenue from the sale of personal data.</li> </ul> </li> </ul> <p>(Some sections of the law apply to any commercial website or internet service provider conducting business in Rhode Island or with customers in Rhode Island (or otherwise subject to Rhode Island jurisdiction) that collects, stores, and sells customer's personal data.)</p> <p>Full non-profit exception.</p>
<b>Minnesota Law</b>	<p>Legal entities (subject to exclusions, such as most government entities) that:</p> <ul style="list-style-type: none"> <li>During a calendar year, control or process the personal data of at least 100,000 consumers (excluding payments processing);</li> <li>Derive over 25% of gross revenues from the sale of personal data and process the personal data of at least 25,000 consumers.</li> </ul> <p>Limited non-profit exception.</p>



**Table 3**

The following chart demonstrates the similarities and differences among current U.S. consumer privacy laws of general application, compares them to the GDPR and notes differences between the original CCPA and the current version amended by the California Privacy Rights Act (“CPRA”).

**GDPR, CCPA, CPRA, Virginia Law & Colorado Law**

	GDPR	CCPA	CPRA	Virginia Law	Colorado Law
Right to Access	✓	✓	✓	✓	✓
Right to Confirm Personal Data is Being Processed	✓	Implied	Implied	✓	✓
Right to Data Portability	✓	✓	✓	✓	✓
Right to Delete <sup>16</sup>	✓	✓	✓	✓	✓
Right to Correct / Right to Rectification	✓	✗	✓	✓	✓
Right to Opt-Out of Sale	✓ <sup>17</sup>	✓ <sup>18</sup>	✓ <sup>17</sup>	✓ <sup>19</sup>	✓ <sup>17</sup>
Right to Opt-Out of Targeted / Behavioral Advertising <sup>20</sup>	✓	✗ <sup>21</sup>	✓	✓	✓
Right to Object or Opt-Out of ADM	✓	✗	✓ <sup>22</sup>	✗	✓ <sup>23</sup>
Right to Opt-Out of Profiling <sup>24</sup>	✓	✗	✓	✓	✓
Choice Required for Processing of “Sensitive” Personal Data	Opt-In	✗	Opt-Out <sup>25</sup>	Opt-In	Opt-In
Right to Object to or Restrict Processing Generally	✓	✗	✗	✗	✗

16 In California, Utah, and Iowa, deletion obligations are limited to PI collected from the consumer; all other state consumer privacy laws include PI collected about the consumer is in scope of the deletion right.

17 Selling personal data under the GDPR generally would require the consent of the data subject for collection and would be subject to the right to object to processing.

18 Any consideration sufficient, but cash consideration not required.

19 Cash consideration required.

20 Right to opt-out of cross-context behavioral advertising sharing for California; right to opt-out of targeted advertising in all other state consumer privacy laws.

21 However, certain data disclosures inherent in this type of advertising are arguably a “sale,” subject to opt-out rights. The CPRA Regulations combine the opt-out right for “sale” and “share.”

22 Subject to substantial expansion under the CPRA Regulations. Based on preliminary rulemaking activities, it appears that the CPPA is contemplating a GDPR-like approach for ADM and profiling.

23 Under the CPA Rules, if a consumer requests to opt out of human involved automated processing, organizations can reject the request, but must inform the consumer of the rejection within 45 days and include the following information or link to such information: the decision subject to profiling, the categories of PI used, the logic used in the profiling process, the role of human involvement, how profiling is used in the decision-making process, benefits and potential consequences of the decision, and how consumers can correct or delete the data used in the profiling.

24 The CPRA's concept of profiling subject to change under the regulations. The profiling concepts in the other 2023 state consumer privacy laws require legal or substantially similar effects.

25 Under the CPRA, the Sensitive PI opt-out right applies to certain processing activities beyond business purposes. Section 7027 of the CA Regs includes contextual but not cross-context behavioral advertising.

	GDPR	CCPA	CPRA	Virginia Law	Colorado Law
Required Opt-Out Links on Website or Elsewhere	No Explicit Requirement	DNS	DNSell, DN-Share, Sensitive PI Opt-Out <sup>26</sup>	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs
Right to Non-Discrimination <sup>27</sup>	Implied	✓	✓	✓	✓
Specific Privacy Policy Content Requirements	✓	✓	✓	✓	✓
Purpose, Use, and/or Retention Limitations	✓	Implied	✓	✓	✓
Privacy & Security Impact Assessments Sometimes Required	✓	✗	✓	✓	✓
“Reasonable” Security Obligation	✓	Implied	✓	✓	✓
Notice at Collection Requirement	✓	✓ (Statute + Regs)	✓	✗	✗
Honor Universal Opt-out Signals	✗	✗	✓	✗	✓

#### Utah Law, Connecticut Law, Nevada Law, Iowa Law & Indiana Law

	Utah Law	Connecticut Law	Nevada Law	Iowa Law	Indiana Law <sup>28</sup>
Right to Access	✓	✓	✗	✓	✓
Right to Confirm Personal Data is Being Processed	✓	✓	✗	✓	✓
Right to Data Portability	✓	✓	✗	✓	✓
Right to Delete	✓	✓	✗	✓	✓
Right to Correct / Right to Rectification	✗	✓	✗	✗	✓
Right to Opt-Out of Sale	✓ <sup>18</sup>	✓ <sup>17</sup>	✓ <sup>29</sup>	✓ <sup>18</sup>	✓ <sup>18</sup>
Right to Opt-Out of Targeted / Behavioral Advertising	✓	✓	✗	✓	✓
Right to Object or Opt-Out of ADM	✗	✗	✗	✗	✗
Right to Opt-Out of Profiling	✗	✓	✗	✗	✓
Choice Required for Processing of “Sensitive” Personal Data	Notice & Opp. to Opt-Out	Opt-In	✗	Notice & Opp. to Opt-Out	Opt-In
Right to Object to or Restrict Processing Generally	✗	✗	✗	✗	✗
Required Opt-Out Links on Website or Elsewhere	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	None	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs
Right to Non-Discrimination	✓	✓	✗	✓	✓

26 Businesses will be able to utilize “a single, clearly labeled link” to cover all opt-outs. The CA Regs permit titling the link “Your Privacy Choices” or “Your California Privacy Choices” plus an icon. It is not clear if organizations need to provide both sale/share and limit sensitive info opt-outs where it is not engaging in activities that necessitate both in order to use the alternative link. The former could work well to direct a consumer to the other state opt-outs too.

27 The CCPA (and the CPRA) take a more onerous approach to non-discrimination with respect to financial incentives and price/service differences, requiring businesses to prove that they are reasonably related to the value of the consumer’s data to the business.

28 Indiana Law also provides the right to obtain a copy or a representative summary of the consumer’s personal data provided to the controller.

29 In Nevada, website and online service operators are required to offer an “opt-out,” but only for limited disclosures of certain information and only if the disclosure is made in exchange for monetary consideration.

	Utah Law	Connecticut Law	Nevada Law	Iowa Law	Indiana Law <sup>28</sup>
Specific Privacy Policy Content Requirements	✓	✓	✓	✓	✓
Purpose, Use, and/or Retention Limitations	✗	✓	✗	✗	✓
Privacy and Security Impact Assessments Sometimes Required	✗	✓	✗	✗	✓
“Reasonable” Security Obligation	✓	✓	✓	✓	✓
Notice at Collection Requirement	✗	✗	✗	✗	✗
Honor Universal Opt-out Signals	✗	✓	✗	✗	✗

### Tennessee Law, Montana Law, Florida Law, Texas Law & Oregon Law

	Tennessee Law	Montana Law	Florida Law <sup>30</sup>	Texas Law	Oregon Law <sup>31</sup>
Right to Access	✓	✓	✓	✓	✓
Right to Confirm Personal Data is Being Processed	✓	✓	✓	✓	✓
Right to Data Portability	✓	✓	✓	✓	✓
Right to Delete	✓	✓	✓	✓	✓
Right to Correct / Right to Rectification	✓	✓	✓	✓	✓
Right to Opt-Out of Sale	✓ <sup>18</sup>	✓ <sup>17</sup>	✓ <sup>17</sup>	✓ <sup>17</sup>	✓ <sup>17</sup>
Right to Opt-Out of Targeted / Behavioral Advertising	✓	✓	✓	✓	✓
Right to Object or Opt-Out of ADM	✗	✗	✗	✗	✗
Right to Opt-Out of Profiling	✓	✓	✓	✓	✓
Choice Required for Processing of “Sensitive” Personal Data	Opt-In	Opt-In	Opt-In (with a right to opt out later)	Opt-In	Opt-In
Right to Object to or Restrict Processing Generally	✗	✗	✗	✗	✗
Required Opt-Out Links on Website or Elsewhere	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs
Right to Non-Discrimination	✓	✓	✓	✓	✓
Specific Privacy Policy Content Requirements	✓	✓	✓	✓	✓
Purpose, Use, and/or Retention Limitations	✓	✓	✓	✓	✓
Privacy and Security Impact Assessments Sometimes Required	✓	✓	✓	✓	✓
“Reasonable” Security Obligation	✓	✓	✓	✓	✓
Notice at Collection Requirement	✗	✗	✗	✗	✗
Honor Universal Opt-out Signals	✗	✓	✗	✓	✓

30 Florida Law also contains the rights to: (i) opt out of the collection or processing of sensitive data; and (ii) opt out of the collection of personal data through voice or facial recognition.

31 Oregon Law also contains the right to obtain a list of specific third parties to which the controller has disclosed the consumer’s personal data, OR any personal data (at the controller’s option).



## Delaware Law, New Jersey Law, New Hampshire Law, Kentucky Law & Minnesota Law

	Delaware Law <sup>32</sup>	New Jersey Law	New Hampshire Law	Kentucky Law	Minnesota Law <sup>33</sup>
Right to Access	✓	✓	✓	✓	✓
Right to Confirm Personal Data is Being Processed	✓	✓	✓	✓	✓
Right to Data Portability	✓	✓	✓	✓	✓
Right to Delete	✓	✓	✓	✓	✓
Right to Correct / Right to Rectification	✓	✓	✓	✓	✓
Right to Opt-Out of Sale	✓ <sup>17</sup>	✓ <sup>17</sup>	✓ <sup>17</sup>	✓ <sup>18</sup>	✓ <sup>17</sup>
Right to Opt-Out of Targeted / Behavioral Advertising	✓	✓	✓	✓	✓
Right to Object or Opt-Out of ADM	✗	✗	✗	✗	✓
Right to Opt-Out of Profiling	✓	✓	✓	✓	✓
Choice Required for Processing of “Sensitive” Personal Data	Opt-In	Opt-In	Opt-In	Opt-In	Opt-In
Right to Object to or Restrict Processing Generally	✗	✗	✗	✗	✗
Required Opt-Out Links on Website or Elsewhere	Targeted Ad & Sale Opt-Outs	Targeted Ad, Sale & Profiling Opt-Outs	Targeted Ad & Sale Opt-Outs	None	Not required, but noted as an approved method.
Right to Non-Discrimination	✓	✓	✓	✓	✓
Specific Privacy Policy Content Requirements	✓	✓	✓	✓	✓
Purpose, Use, and/or Retention Limitations	✓	✓	✓	✓	✓
Privacy and Security Impact Assessments Sometimes Required	✓	✓	✓	✓	✓
“Reasonable” Security Obligation	✓	✓	✓	✓	✓
Notice at Collection Requirement	✗	✗	✗	✗	✗
Honor Universal Opt-out Signals	✓	✓	✓	✗	✓

## Maryland Law, Nebraska Law & Rhode Island Law

	Maryland Law <sup>34</sup>	Nebraska Law	Rhode Island Law
Right to Access	✓	✓	✓
Right to Confirm Personal Data is Being Processed	✓	✓	✓
Right to Data Portability	✓	✓	✓
Right to Delete	✓	✓	✓
Right to Correct / Right to Rectification	✓	✓	✓

<sup>32</sup> Delaware Law also provides the right to obtain a list of categories of third-party recipients of the consumer’s personal data, by category of personal data.

<sup>33</sup> Under the Minnesota Law, 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. If the controller does not maintain the information in a format specific to the consumer, a list of specific third parties to whom the controller has disclosed any consumers’ personal data may be provided instead.

<sup>34</sup> Maryland Law also provides the right to obtain a list of the categories of third parties to which the controller has disclosed the consumer’s personal data, OR a list of the categories of third parties to which the controller has disclosed any consumer’s personal data IF the controller does not maintain this information in a format specific to the consumer.

	Maryland Law <sup>34</sup>	Nebraska Law	Rhode Island Law
Right to Opt-Out of Sale	✓ <sup>17</sup>	✓ <sup>17</sup>	✓ <sup>17</sup>
Right to Opt-Out of Targeted / Behavioral Advertising	✓	✓	✓
Right to Object or Opt-Out of ADM	✗	✗	✗
Right to Opt-Out of Profiling	✓	✓	✓
Choice Required for Processing of “Sensitive” Personal Data	Only when strictly necessary, no sale allowed	Opt-In	Opt-In
Right to Object to or Restrict Processing Generally	✗	✗	✗
Required Opt-Out Links on Website or Elsewhere	Targeted Ad & Sale Opt-Outs	Targeted Ad & Sale Opt-Outs	✗
Right to Non-Discrimination	✓	✓	✓
Specific Privacy Policy Content Requirements	✓	✓	✓
Purpose, Use, and/or Retention Limitations	✓	✓	✓
Privacy and Security Impact Assessments Sometimes Required	✓	✓	✓
“Reasonable” Security Obligation	✓	✓	✓
Notice at Collection Requirement	✗	✗	✗
Honor Universal Opt-out Signals	✓	✓	✗

# CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit [competitionpolicyinternational.com](https://competitionpolicyinternational.com) today to see our available plans and join CPI's global community of antitrust experts.

