BURR FORMAN LLP

Summary and Comparison of U.S. Data Privacy Laws Since California's CCPA and CPRA

Article
11.15.2022

California started the process of individual U.S. states enacting individual privacy laws with its California Consumer Privacy Act ("CCPA"), which currently is in effect, as supplemented and amended by the California Consumer Rights Act ("CPRA"), with general effect on January 1, 2023. There have been various revisions to the accompanying Regulations and many analyses and publications examining CCPA/CPRA, their meaning, and their effects on businesses.

After California, next came Virginia, Colorado, Utah, and Connecticut in passing their own similar but different privacy laws. Tracking compliance with each of these states' individual data privacy laws can be challenging for businesses that collect, use, retain, sell and/or share personal data, and engage in targeted advertising and profiling because there is no generally applicable federal law at this time.

This article sets out some of the key similarities and differences between and among the individual states' privacy laws following California's CCPA/CPRA.

Virginia – After California, Virginia enacted its data privacy law, the Consumer Data Protection Act ("CDPA" or "VCDPA"), which goes into effect on January 1, 2023. The CDPA applies to entities that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that either:

1. Control or process the personal data of at least 100,000 consumers during a calendar year, OR

RELATED PROFESSIONALS

Elizabeth B. Shirley, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

2. Control or process the personal data of at least 25,000 consumers and derive at least 50% of its gross revenue from the sale of personal data.

With regard to (a) above, this is the same 100,000 threshold that is contained in the CPRA, which doubled the 50,000 threshold that is set out in the CCPA.

Pursuant to the VCDPA, the "sale of personal information" is defined as "the exchange of personal data for monetary consideration by the controller to a third party." Thus, unlike California's privacy laws, where a sale is defined beyond only monetary sales and also encompasses "valuable consideration," Virginia's privacy law requires that the consideration for the sale to be monetary.

Under Virginia's CDPA, the definition of a sale contains certain exclusions:

- Disclosures to processors;
- Disclosures to a third party for purposes of providing products or services requested by the consumer;
- Disclosures to controller's affiliate;
- Disclosures of information that consumers:
- Intentionally made available to the general public via mass media, and
- Does not restrict a specific audience.

Virginia's CDPA provides consumers with the following primary rights:

- Right to access. Right to confirm whether a controller is processing the consumer's personal data and to access such personal data.
- Right to correct. Right to correct inaccuracies in personal information, considering the nature of the personal information and the purposes of the processing of the consumers' personal information.
- Right to delete. Right to delete personal information provided by or obtained about the consumer.
- Right to data portability. Right to obtain a copy of the consumer's personal information that the consumer previously provided in a portable format and, to the extent technically possible, readily usable format that allows the consumer to transmit the data to another entity without hindrance.
- Right to opt out. Right to opt out of the processing of their personal data for purposes of targeted advertising, the sale of personal information, and profiling that advances decisions that produce legal or similarly significant effects concerning the consumer.
- Right to appeal. A business must respond to a consumer request within 45 days of receipt of the request. Where reasonably necessary, the business may then extend the response deadline by an additional 45 days as long as they notify the consumer within the initial response window. Consumers have a right to appeal a business's denial to act within a reasonable time, and businesses must establish a process for such appeals. If the appeal is denied, businesses must inform consumers how they can submit a complaint to the attorney general.

Summary and Comparison of U.S. Data Privacy Laws Since California's CCPA and CPRA

Additionally, businesses have certain affirmative obligations pursuant to VCDPA:

- Limits on collection. The CDPA provides that businesses shall limit the collection of data to that which is "adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed."
- Limits on use. Once the personal information has been collected, businesses must "not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent." Also, the CDPA imposes limits on processing sensitive personal information such that doing so is prohibited absent consumer consent.
- Technical safeguards. In addition to imposing obligations on the business's processing activities, CDPA requires that businesses establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.
- Data protection assessments. Controllers are required to conduct data protection assessments evaluating the risks associated with personal information processing activities. No timeframe is provided for the frequency of these assessments.
- Data processing agreements. Processing activities by a processor on behalf of a controller must be governed by a data processing agreement. These agreements must clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. There are various terms that must be included in such agreements, which are set out in the CDPA.
- Privacy notice. The VCDPA requires controllers to provide consumers with a privacy notice. The notice must state:
  - The categories of personal information processed by the controller.
  - The purpose for processing personal information.
  - How consumers may exercise their consumer rights and appeal a controller's decision regarding the consumer's request.
  - The categories of personal information that the controller shares with third parties, if any.
  - The categories of third parties, if any, with whom the controller shares personal data.

Colorado – Colordo was the next state after Viringia to enact a data privacy law, which is Colorado Privacy Act ("CPA"). The CPA goes into effect on July 1, 2023. Colorado's law is consistent in many ways with Virginia's data privacy law. The CPA applies to entities that conduct business in Colorado, or produce or deliver commercial products or services that are intentionally targeted to residents of Colorado, and

1. Control or process the personal data of at least 100,000 consumers or more during a calendar year; OR

2. Derive revenue or receive a discount on the price of goods or services from the sale of personal information and process or control the personal data of 25,000 consumers or more.

As to (a), this is the same standard as set out in Virginia's data privacy law.

Additionally, the CPA defines the "sale of personal information" as the exchange of personal data for monetary "or other valuable consideration" by a controller to a third party. Thus, the CPA is consistent with CCPA/CPRA and is not as restrictive in the definition of a sale as is Virginia's data privacy law.

Similar to Virginia's CDPA, however, the CPA also excludes certain types of disclosures from the scope of a sale. More specifically, the CPA contains the following exclusions:

- Disclosures to a processor that processes personal information on behalf of a controller;
- Disclosures to a third party for purposes of providing a product or service requested by the consumer;
- Disclosures or transfer to a controller's affiliate;
- Disclosures or transfer to a third party as an asset in a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets; and
- Disclosures:
  - That a consumer directs the controller to make by using the controller to interact with a third party; or
  - Intentionally made available by a consumer to the general public via mass media.

The CPA generally provides the same consumer rights as does the VCDPA—right of access, right to correction, right to delete, right to data portability, right to opt out of targeted advertising, the sale of personal data, and profiling in that affects decisions that produce legal or similarly significant effects concerning a consumer. However, with regard to a consumer's right to opt-out, controllers must honor opt-out signals as a method for consumers to exercise their opt-out rights.

The CPA also generally contains the same controller obligations as the VCDP – duty of transparency (including through use of a privacy notice), duty of purpose specification, duty of data minimization, duty to avoid secondary use, duty of care with regard to technical safeguards, duty regarding processing sensitive personal data only after obtaining consent, and the requirement of data processing contracts between controllers and processors.

Utah – After Colorado, Utah enacted its privacy law, the Utah Consumer Privacy Act ("UCPA") on March 24, 2022. The UCPA goes into effect on December 31, 2023. Utah's law contains some provisions that are more favorable to businesses, and it is not as encompassing in data privacy rights as Virginia and Colorado's laws.

Summary and Comparison of U.S. Data Privacy Laws Since California's CCPA and CPRA

The UCPA applies to any controller or processor that:

1. Conducts business in Utah or produces products or services that are targeted to Utah residents as consumers;
2. Has annual revenue of $25,000,000 or more; AND
3. Meets one or more of the following thresholds:

-
  - During a calendar year, controls or processes personal data of 100,000 or more consumers; or
  - Derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

Thus, Utah's data privacy law is more restrictive and favorable for businesses than CCPA/CPRA, VCDPA and CPA, as Utah's law provides that (a), (b), and one of the factors in (c) above apply for a controller or processor to fall within the scope of the UCPA.

Additionally, the UCPA's definition of a "sale" is similar to the more restrictive definition set out in Virginia's privacy law, whereby a sale involves an exchange of personal information for "monetary consideration by a controller to a third party."

The UCPA also contains similar exclusions to VCDPA and CPA with regard to certain types of disclosures from the definition of sale, e.g., disclosures to a processor or a controller's affiliates; disclosures to a third party to provide a product or service requested by the consumer, and the like. The UCPA, however, contains an exclusion that is not written into Virginia's and Colorado's privacy laws – the UCPA excludes from the definition of a sale "a controller's disclosure of personal data to a third party if the purpose is consistent with a consumer's reasonable expectations."

Consumer rights under the UCPA are consistent with those set out in Virginia and Colorado's data privacy laws, but more restricted. The UCPA provides the right to access, deletion, data portability, and opt-out of certain data processing for the purposes of targeted advertising or the sale of personal data.

Notably, consumers do not have the right to request deletion of all of the personal information that the controller retains. Instead, consumers only have the right to delete the personal data that they provided to the controller. Additionally, consumers do not have the right to opt out of profiling, and controllers do not have to recognize universal opt-out signals as a method for consumers to opt-out. And, under the UCPA, consumers do not have the right to correct inaccuracies in their personal information.

Consistent with VCDPA and CPA, Utah's CPA contains various controller obligations with regard to their collection, use, and retention of personal information. Under Utah's law, however, controllers' obligations are not as broad and extensive as their obligations under Virginia and Colorado's privacy laws.

Summary and Comparison of U.S. Data Privacy Laws Since California's CCPA and CPRA

In Utah, controllers have obligations of transparency (including a privacy notice); parental consent to process personal information of minors under age 13 years (consistent with COPPA); data security; responding to consumer requests; data processing contracts between controllers and processors; and, similar to CCPA/CPRA, non-discrimination with regard to consumers exercising their personal data rights. Further, there is no appeal process for consumers whose requests have been denied under Utah's privacy law.

Connecticut – Finally, Connecticut recently passed its data privacy law, An Act Concerning Personal Data Privacy and Online Monitoring ("CT law"). The CT law was signed on May 10, 2022, and it goes into effect on July 1, 2023. The CT law is more in line with Virginia's and Colorado's data privacy laws. Thus, it may be considered more restrictive on controllers' data processing activities than the more flexible Utah data privacy law.

The CT law applies to entities that conduct business in Connecticut or produce products or services targeted to Connecticut residents and that during the preceding calendar year either:

- Controlled or processed the personal data of at least 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing payment transactions; OR
- Controlled or processed the personal data of at least 25,000 consumers and derived over 25% of their gross revenue from the sale of personal data.

Connecticut's law has a lower threshold for revenue based on the control or processing of personal data than Virginia (25% of gross revenue in CT; 50% of gross revenue in VA), which operates to include more businesses in the scope of the law. Connecticut's law, however, contains a higher threshold for revenue based on the control or processing of personal data than Colorado's law (25% of gross revenue in CT; any % of gross revenue in CO), which operates to include fewer businesses in the scope of the law. Significantly, the CT law excludes consideration of personal information that is processed solely for the purpose of completing payment transactions, which can be favorable if a business seeks to stay outside the scope of the CT law.

The CT law defines the "sale of personal data" as "the exchange of personal data for monetary or other valuable consideration by the controller to a third party." Thus, the CT law includes the broader definition of a sale, similar to California and Colorado. Additionally, the CT law excludes certain disclosures, and these exclusions are substantially similar to Colorado's exclusions.

The CT law provides similar consumer rights to those in Colorado – (1) the right to access, where consumers can confirm whether the business has their personal data, as well as access to such personal data; (2) right of correction; (3) right to delete; (4) right to data portability, which applies to all personal data of the consumer, not just that personal data provided by the consumer; and (5) the right to opt out.

Summary and Comparison of U.S. Data Privacy Laws Since California's CCPA and CPRA

Under CT law, controllers are required to provide “clear and conspicuous” links on their websites allowing consumers to opt-out of various types of processing of their personal information. Starting January 1, 2025, the CT law also requires controllers to recognize universal opt-out preference signals that indicate the consumer’s intent to opt-out of targeted advertising and sales.

The CT law contains controller obligations that are similar to those in CCPA/CPRA, Virginia’s privacy law, and Colorado’s privacy law. More specifically, controllers have obligations to limit collection of personal information; limit the use of personal information to disclosed purposes; maintain reasonable security (administrative, technical and physical security); transparency (e.g., privacy policies); vendor contracts between controllers and processors; data protection assessments for activities that involve a heightened risk of harm to consumers; and obtain consent to the sale and targeted advertising of personal data from consumers aged 13-16 years, as well as compliance with the consent requirements set out in COPPA.