Preparing For 5 State Data Privacy Laws Coming In 2023

By **Taylor Osher and Jeremy Beutler** (December 15, 2022)

Taylor Osher

Jeremy Beutler

Early next year, on Jan. 28, several countries, including the U.S., will observe Data Privacy Day, an internationally recognized day to commemorate the anniversary of the first legally binding international privacy treaty.[1]

The goal of Data Privacy Day is to promote awareness about the importance of respecting and safeguarding personal information. In the U.S., Data Privacy Day should hold special significance because five new data privacy laws come into effect in five states.

Beginning Jan. 1, Virginia's Consumer Data Protection Act, or VCDPA, and California's Privacy Rights Act, or CPRA, officially become operational. Just six months later, on July 1st, Connecticut's Data Privacy Act, or CDPA, and Colorado's Privacy Act, or CPA, go into effect, and California also begins enforcement of the CPRA.

Finally, the year is set to end with the effective date of Utah's Consumer Privacy Act, or UCPA, on Dec. 31, 2023.

All five of these privacy laws will provide consumers with the right to access, delete and request their personal information in a portable format. Some states will further allow consumers to request that inaccurate personal information be corrected.

Consumers will also have the right to opt out of targeted advertising and disclosures of personal information that may qualify as sales of personal information. And in some states, consumers will have the right to request that their personal information be restricted from use in connection with profiling.

Businesses under each privacy law will be obligated to provide notice and transparency about their information practices — often in the form of a privacy policy and other notices — and, in many states, will be prohibited from discriminating against a consumer who chooses to exercise one or more of these privacy rights.

Although many of these privacy laws share similarities, no two laws are identical, and so compliance with only one of these laws will not satisfy the new requirements across all five states.

For example, California, Virginia, Colorado and Connecticut each require data impact assessments for certain processing activities.[2] Utah, however, does not require such an assessment.

In addition, each of these laws have contractual requirements that a business must put into place with service providers that process personal information on behalf of the business.[3] Although the requirements under laws in Colorado, Connecticut, Utah and Virginia are somewhat similar, the draft regulations under the CPRA include additional requirements not present in the other state laws.

With Jan. 1 fast approaching, businesses should be updating their service provider contracts to comply with these laws.

One hurdle to managing compliance across all five states is the fact that common terms are sometimes defined differently. The word "sale" for instance has a different definition in the CPRA than in the VCDPA.

Under the CPRA a "sale" means any disclosure of personal information to a third party for monetary or other valuable consideration.[4]

Under the VCDPA a "sale" is limited to the exchange of personal data for monetary consideration.[5] The differences in meaning can have implications for how businesses implement and manage processes to honor consumers' opt-out requests.

Another hurdle to managing compliance is the lack of finalized regulations to help guide businesses on how to implement each of these new privacy laws. California[6] and Colorado[7] have released draft regulations under the CPRA and CPA, respectively.

The CPRA propose regulations are going through a second round of comments and will not likely be finalized until January or February of next year, at the earliest.

Colorado published its first draft of proposed rules in October and a public hearing on the draft will be held in February, so it will likely be many months before businesses will know what will be included in the final regulations. This is one area for businesses to continue to monitor to see if the goal posts for privacy compliance shift.

Although a lack of finalized regulations can create uncertainty when it comes to complete compliance, the draft regulations provide some insight on how to prepare for 2023.

For example, like the regulations that were issued under the California Consumer Privacy Act, drafts of the CPRA regulations have consistently included requirements for businesses to honor opt-out preference signals,[8] like the Global Privacy Control.[9]

Colorado's draft CPA regulations have a similar requirement for businesses to honor universal op-out mechanisms as an indication of a consumer's decision to opt out of targeted advertising.[10]

This is an important requirement of which businesses should take note because, in the only CCPA enforcement action to date that resulted in financial penalties, the failure to honor such a signal was among the list of violations identified by the California Attorney General.[11]

With only days until the VCDPA and CPRA take effect, the time to start planning for privacy is now. Enforcement of the VCDPA begins Jan. 1, but, fortunately for businesses, includes a requirement that the Virginia Attorney General provide alleged violators with a 30-day cure period before bringing an enforcement action.[12]

Although a similar notice-and-cure provision under the CCPA sunsets with the effective date of the CPRA, enforcement of the CPRA will not begin until July 1, 2023. Still, businesses should keep in mind that the California attorney general will continue to enforce the CCPA in the interim.

Businesses that have not begun compliance efforts should begin now and those that have

should keep an eye on this space. We will likely see finalized regulations under the CPRA and CPA in the first half of the year, and we may even see other states pass similar privacy laws next year.

Taylor Osher and Jeremy C. Beutler are associates at Stubbs Alderton & Markiles LLP.

[1] https://staysafeonline.org/programs/data-privacy-week/about/.

[2] VCDPA Section 59.1-576, CPRA Section 1798.185(a)(15), and CPA 6-1-1309.

[3] VCDPA Section 59.1-575 and CPRA Section 1798.100(d).

[4] CPRA Section 1798.140(t).

[5] VCDPA Section 59.1-571.

[6] https://cppa.ca.gov/regulations/.

[7] https://coag.gov/resources/colorado-privacy-act/.

[8] CPRA Draft Regulations as of 11/3/22 Section 7025.

[9] https://globalprivacycontrol.org/.

[10] CPA Section 6-1-1306.

[11] Compl. ¶ 5, California v. Sephora USA, Inc., No. CGC-22-601380 (Cal. Sup. Ct. Aug. 24, 2022).

[12] VCDPA Section 59.1-584(A).