

CLIENT ALERT

Additional States Plan for the Implementation of Data Privacy Laws

March 1, 2022

Earlier this month, Crowell & Moring issued an alert regarding the robust enforcement of the California Consumer Privacy Act (“CCPA”) since its 2020 effective date. Other states and state consortiums, such as the Attorney General Alliance, continue to focus on the perceived need for consumer data privacy, which maintains bipartisan appeal. Currently, Colorado is preparing for the July 1st, 2023 effective date for the Colorado Privacy Act (“CPA”), various other states are working toward passing consumer data privacy legislation, and some states are attempting to pass measures of protection against “big data” that are different from California, Virginia or Colorado’s data privacy acts.

The Attorney General Alliance (“AGA”), a cooperative organization that hosts bipartisan forums in the Attorney General community, held a conference in early February titled “Colorado Privacy Act: Rights, Obligations, and Next Steps” as part of the “Ginsburg/Scalia Initiative.” The conference provided a forum for robust discussion on the implementation of consumer data privacy legislation, the states currently considering legislation, namely Alaska, Connecticut, Indiana, Minnesota, Ohio, Oklahoma, and Washington and held a fireside chat with Attorney General Weiser and Wyoming Attorney General Hill. Additionally, Paul Ohm, a Georgetown Law professor, privacy expert, and former advisor to the FTC, was a keynote speaker and announced that he would join the Colorado AG’s office to advise the implementation of the CPA.

The CPA was passed in June 2021 and became the United States’ third comprehensive consumer data privacy law passed at the state level after the CCPA and the Virginia Consumer Data Protection Act (“VCDPA”). Though not identical, those familiar with the CCPA and VCDPA will recognize many aspects of the CPA. While the law itself does not go into effect until July 1, 2023, AG Weiser recently announced that his office will be soliciting feedback in order to “fully understand the concerns and needs of Coloradoan’s and Colorado businesses.” The precise timeline for the upcoming notice and comment period has not yet been announced, but AG Weiser indicated that a formal Notice of Proposed Rulemaking would be posted during Fall 2022. AG Weiser also indicated that he expects his office to adopt final rules around February, 2023.

Regarding the substance of the CPA, the statute provides Colorado consumers with six main rights with respect to their personal data:

1. **Right of access.** Consumers have “the right to confirm whether a controller is processing personal data concerning the consumer and to access the consumer’s personal data.”
2. **Right to correction.** Consumers have “the right to correct inaccuracies in the consumer’s personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer’s personal data.”
3. **Right to delete.** Consumers have “the right to delete [their] personal data.”
4. **Right to data portability.** Consumers have “the right to obtain a personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance.”
5. **Right to opt out.** Consumers have “the right to opt out of the processing of [their] personal data ... for purposes of:

- a. targeted advertising;
- b. the sale of personal data, or
- c. profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.”
- d. Notably, the CPA’s opt-out mechanism requirement diverges significantly from its counterparts in the CCPA and VCDPA. Under the CPA, a controller must provide consumers with the right to opt out and a universal opt-out option so a consumer can click one button to exercise all opt-out rights. What this means from a technical standpoint is currently unclear, but we anticipate guidance from the Colorado Attorney General before July 1, 2023.

6. **Right to appeal.** Consumers have the right to appeal a business’ denial to act within a reasonable time period. In such instances, a business must respond to a consumer request within 45 days of receipt. However, that deadline may be extended by an additional 45 days when reasonably necessary.

In addition to these rights, the CPA also imposes new obligations for businesses. These obligations include new data minimization and technical safeguards requirements in conjunction with new mandates requiring that companies implement data processing agreements, conduct data protection assessments, and restrict their processing activities with respect to personal data.

Given the similarities between the VCDPA, CCPA, and CPA, companies should be able to build upon the existing privacy infrastructure developed for CCPA and VCDPA compliance purposes. However, companies should note that compliance with either the CCPA or VCDPA does not necessarily mean a company’s practices are CPA compliant as each law contains different exemptions, timeframes, and scopes of applicability. Given its potential impact, we encourage companies to consider participating in the notice and comment period. If you wish to remain apprised of rulemaking activities, a mailing list sign up link can be found [here](#). We recommend companies conduct a review of their data practices with respect to Colorado Consumers’ data prior to July 1, 2023.

As Colorado, and Virginia and California, continue to implement their individual consumer data privacy acts, many other states are considering or have considered their own implementation of consumer data privacy legislation. Around thirty states and the District of Columbia have officially considered consumer data privacy legislation through the introduction of a bill in at least one legislative chamber. Many of those bills died in committee or have been postponed. Two states, [Indiana](#) and [Oklahoma](#), have proposed consumer data privacy legislation that has passed in one chamber and is currently under consideration in the second chamber. The Indiana and Oklahoma bills passed their original chambers either unanimously or with a substantial majority and could become the next two states to enact consumer data privacy legislation.

However, consumer data privacy legislation is not the only way states are attempting to address “big data.” Some states are considering biometric privacy bills, while others are considering data broker bills. For example, the Oregon House is considering [HB 4017](#). HB 4017 requires data brokers—companies that knowingly collect and sell consumer profiles of American citizens that may include demographic information, internet use history, and other personal data to third parties with whom the consumer has no relationship— to register with the Oregon Department of Consumer and Business Services, essentially creating a “data broker registry.” Oregon Attorney General Rosenblum requested the introduction of the bill and testified before the Oregon House Business and Labor Committee in February. AG Rosenblum testified “It’s one thing for a consumer to willingly turn over data for a specific purpose. But the widespread sale of data, often done without our knowledge or our consent, gives data

brokers broad latitude to do whatever they want with it.” The bill calls on businesses that operate data brokerage services to “operate with transparency and responsibility.” Data brokers would pay a fee to support the registry program and Oregon consumers could use the registry to make inquiries of data brokers or request that the data brokers no longer sell their personal information. Delaware and Massachusetts are considering similar bills and California and Vermont have already passed data broker legislation and require registry of such companies.

Data privacy remains a prevalent, bipartisan consumer protection issue. Without federal movement, the states via legislation and subsequent attorney general enforcement are seeking varied ways to address consumer data privacy, which will likely lead to further piecemeal legislation and implementation. Corporations should remain aware of the development of consumer data privacy laws in various states to ensure compliance of any interstate commerce activity.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Toni Michelle Jackson

Partner – Washington, D.C.
Phone: +1.202.624.2723
Email: tjackson@crowell.com

Matthew B. Welling

Partner – Washington, D.C.
Phone: +1.202.624.2588
Email: mwelling@crowell.com

Sarah Rippy

Associate – Denver
Phone: +1.303.524.8634
Email: srippy@crowell.com

Roy Abernathy

Associate – Washington, D.C.
Phone: +1.202.654.6722
Email: rabernathy@crowell.com