Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Colorado Adds Wrinkle To Emerging State Privacy Law Quilt

By **Allison Grande**

Law360 (June 18, 2021, 12:01 PM EDT) -- Colorado is on the brink of becoming the third U.S. state to enact comprehensive consumer privacy legislation, a move that's set to throw a curveball at companies' compliance plans and give further ammunition to the push for a unified nationwide framework.

The Colorado Privacy Act, which Gov. Jared Polis is expected to sign in the coming days and would take effect on July 31, 2023, has much in common with the privacy laws already on the books in California, Virginia and the European Union, which similarly aim to give consumers more access to and control over how companies handle their personal information.

At the same time, the new legislation also introduces some important nuances that set it apart from its predecessors, such as establishing heightened protections for the processing of sensitive data and prohibiting the use of "dark patterns" that websites use to trick consumers into making unintended choices.

"It's interesting how the Colorado Legislature seems to have watched the landscape and watched how these different laws were being implemented, and then cherry-picked the provisions they wanted to include, which of course makes it more difficult for companies to figure out how to comply," said Jacqueline Cooney, a senior director of privacy and cybersecurity at Paul Hastings LLP.

But while the new twists in the Colorado law are likely to pose compliance challenges, companies may be able to derive some benefits from the core privacy principles that run across the three state regimes, Cooney noted.

"There are a lot of similarities when it comes to elements such as access, deletion, data portability and opting out of the sale of data that companies should be making sure that they understand and that they can apply to create an overarching approach that meets the requirements of all three states," Cooney said. She added that since the Colorado, Virginia and California laws have all been considered and passed around the same time, they contain some similar concepts "that may make it easier to impose an enterprise-wide approach for data subjects to exercise their rights."

Colorado's embrace of these common privacy principles also solidifies their place as essentially bedrock provisions that companies should expect to see featured prominently in other state laws that are likely to emerge in the next few years. Additionally, Congress is likely to use these core principles as a guide in its long-running efforts to answer calls from businesses and consumer advocates to institute a federal standard to counteract the emerging state patchwork, attorneys say.

"We're starting to see patterns in these laws that are being passed on the state level, and they're creating somewhat of a standard that might make adopting a federal law a little easier, since states and lobbyists have done a lot of the work so far," said Amy Pimentel, a partner at McDermott Will & Emery LLP.

The Colorado Senate voted 34-1 to send the privacy bill to the governor's desk on June 8, a day after the state's House approved the measure in a 57-7 vote. The legislation requires businesses to give consumers the ability to access, correct, delete and opt out of the sale of their personal information or processing of this data for targeted advertising and profiling purposes.

The law enables the state's attorney general as well as district attorneys to enforce the law and doesn't include a private right of action that would have allowed consumers to sue for alleged violations.

The bill's passage came just over three months after Virginia's governor in March signed into law a sweeping consumer privacy bill that's slated to take effect Jan. 1, 2023. Like the Colorado legislation, the Virginia Consumer Data Protection Act will hand consumers the ability to access, correct and delete their personal information and to opt out of the processing of this data for targeted advertising purposes, while also giving the state's attorney general exclusive authority to enforce the law.

The Virginia law is scheduled to go live on the same day as the California Privacy Rights Act, a ballot measure that voters approved in November to strengthen the state's landmark Consumer Privacy Act, which has been in effect since the beginning of 2020. The CPRA builds on the existing privacy statute in several ways, including by creating a new agency dedicated to data privacy, allowing consumers to correct inaccurate information and opt out of the sharing of their data, and establishing a new category of "sensitive" personal information that is afforded heightened safeguards.

Companies that do business across the U.S. were already gearing up to fall into step with the Virginia and revamped California frameworks by the start of 2023. With the latest and somewhat surprising move by Colorado, which wasn't on many privacy experts' radar as a contender to pass the nation's next privacy law, companies will now have additional considerations to factor into these compliance plans, attorneys say.

"Businesses made significant investments to comply with the California Consumer Privacy Act," which the state Legislature passed in 2018, noted Hogan Lovells partner Bret S. Cohen. "Now, with revisions to that law in the California Privacy Rights Act, along with new laws in Virginia and Colorado, it will become much more difficult to build a single, effective, U.S.-wide compliance program."

In general, Colorado's bill shares some key principles with the CPRA and the Virginia law, including establishing similar rights of access, correction, deletion, data potability, special protections for sensitive data and the ability for consumers to opt out of the sale of their personal information.

But the Colorado law hews more closely to the model established by Virginia, which departs from the California framework by adopting language and data assessment requirements that are more on par with the EU's General Data Protection Regulation and leaving it completely up to the state attorney general rather than consumers to enforce the law.

The Colorado bill also borrows from and builds on the Virginia law and the GDPR by taking steps such as requiring opt-in consent for the processing of sensitive personal information, creating an obligation to

respond to universal opt-out signals and requiring companies to insert certain language for contracts involving processors, subprocessors and data that has been stripped of identifiers that can be used to link it to specific individuals.

"The major differences are in the details," noted Kirk Nahra, co-chair of the privacy and cybersecurity group at WilmerHale.

For example, the three laws all define "sensitive data" as well as the relevant exemptions that may apply to companies differently, Nahra said. The Colorado law also exempts personal information generated within the employment and business-to-business contexts, consistent with the Virginia law but a departure from California's regime, attorneys noted.

Additionally, the Colorado law "may apply to a slightly broader set of companies than the Virginia law," noted Greg Szewczyk, a partner at Ballard Spahr LLP who's based in Denver.

Both laws contain two coverage thresholds, including an identical one that applies to companies that collect the personal data of 100,000 of their consumers annually, Szewczyk said. However, the laws differ with respect to the second threshold, with Colorado's law extending to companies that derive any revenue from data sales plus collect the personal data of 25,000 Colorado consumers, and Virginia limiting liability to companies that derive 50% of their gross revenue from the sale of personal data plus collect the personal data of 25,000 consumers in the state, Szewczyk added.

The Colorado bill is also "the first of the state privacy laws to apply to nonprofits, which, for the first time, must consider how they will comply with comprehensive privacy laws in the U.S," noted Cohen, the Hogan Lovells partner.

The CPRA offers a third coverage model, extending to businesses that buy, sell or share personal information of more than 100,000 California consumers or households, have a gross revenue over $25 million, or derive at least 50% of annual revenue from sharing or selling the personal information of California consumers.

"The number one step for companies to take is figuring out the scope of these laws and whether it applies to them, since that analysis is going to differ from state to state," said Cooney, the Paul Hastings attorney.

The compliance stakes are particularly high due to the Colorado law's enforcement structure. While lawmakers declined to allow consumers to bring lawsuits, as they're allowed to do under the California law's limited private right of action for data breach-related claims, they empowered not only the state's attorney general to enforce the law, but also district attorneys, who aren't given such authority under any other privacy regime and whose new ability is likely to broaden the scope of potential enforcement.

"This means that enforcement can be local in nature as opposed to statewide," Cooney said. "The attorney general only has so much bandwidth to bring enforcement actions, so as a result of making it a little more decentralized, enforcement might end up being more aggressive in Colorado."

The enforcers will also be able to collect higher penalties under the Colorado law than their counterparts in California and Virginia. Colorado's lawmakers elected to make any violations of the new privacy statute actionable under the state's existing consumer protection statute, which carries fines of up to $20,000 per violation, while the California and Virginia regimes cap penalties at $7,500 per

violation.

"This means there could be some potentially significant financial consequences for folks caught violating the Colorado statute," said Ed Hopkins, a partner in Fisher Phillips LLP's data security and workplace privacy practice.

Hopkins, who works in the firm's Denver and Phoenix offices, added that Colorado Attorney General Phil Weiser, who was instrumental in pushing the law through the state Legislature, is likely to be an active enforcer and at least at first focus his office's limited resources on situations where companies had either completely shirked their new obligations or where a vast quantity of Colorado residents have been impacted.

"AG Weiser may be one of the most well-studied attorneys general when it comes to the privacy practice, and he has a reputation for balancing consumers' rights with the needs of the business community," Hopkins said. "So the expectation is that he's going to do intelligent enforcement and focus on those who don't show the proper amount of respect for the law rather than those who are working hard to comply with the provisions."

The Legislature also handed the attorney general's office rulemaking power, a feature that's present in the California framework but not in the Virginia law.

"Accordingly, Colorado may be positioned to lead the nation on how to interpret and implement the Virginia/Colorado legislative framework," noted Szewczyk, the Ballard Spahr partner.

As part of this rulemaking authority, the Legislature has directed the Colorado attorney general to develop the technical specifications for a universal opt-out mechanism that companies beginning in July 2024 will be required to use to allow consumers to exercise their rights under the law. While Virginia also allows individuals to opt out of having their personal data processed for sales, targeted advertising or profiling, it doesn't require the use of a specific opt-out mechanism, noted Marian Waldmann Agarwal, of counsel at Morrison & Foerster LLP.

"Colorado goes a step further and would require the AG to issue rules by July 1, 2023, when the [law] would enter effect, for technical specification of one or more universal opt-out mechanisms," she said. "So this would be something new for controllers to consider if within the [Colorado law's] scope."

Andrew Baer, the chair of the technology, privacy and data security practice at Cozen O'Connor, added that it would be interesting to see if the opt-out mechanism proscribed by the Colorado attorney general ends up becoming "a baseline for future privacy laws in other states and the federal government and ultimately becomes universal practice."

When asked for comment on the new law and how his office planned to enforce it, Weiser in an emailed statement specifically pointed to the authority that the legislation gives to his office "to develop rules to protect consumers while enabling companies to use information to keep consumers safe and to provide valued services."

"Right now, companies are collecting data on consumers that consumers don't know about," the attorney general said. "Absent action at the federal level, states like Colorado are advancing effective data privacy policy solutions. The core part of the Colorado data privacy bill that really matters is consumers will have the ability to control and dictate how their data is used."

The new Colorado law is certain to be far from the last word on these issues, with state lawmakers indicating that they intend to amend the law in the near future to refine certain provisions and several other states seriously considering their own privacy proposals.

Washington state, Florida and Oklahoma came close to putting such legislation on the books this year, but fell short due to disagreements mainly over whether consumers should be allowed to sue for alleged violations. A few other states, including Massachusetts, New Jersey and Pennsylvania, are still in session and have privacy proposals on the table, but attorneys expect the real movement to come in 2022, when all the state legislatures are back in session.

"Virginia and Colorado are really solidifying a foundation for other states to copy," said Pimentel, the McDermott partner. "For companies, next year is going to be a busy one, with three laws on the books that will take effect in 2023 and more state laws likely to get through, so they'll need to give some thought to what they need to put in place as far as strategy and budget when it comes to their compliance programs."

The push will also continue for Congress to establish a federal framework before the three new privacy laws go live in 2023, attorneys noted.

"Everyone likes to talk about the differences across these state bills," said Lindsey Tonsager, vice chair of the data privacy and cybersecurity practice at Covington & Burling LLP. "But the hope is that federal privacy legislation will recognize and codify all the common elements these laws share while avoiding the inconsistencies and divergences that are starting to emerge at the state level."

--Editing by Orlando Lorenzo and Alyssa Miller.
