July 16, 2021

Colorado Becomes the Third State to Enact a Comprehensive Data Privacy Law

On July 7, 2021, Colorado Governor Jared Polis signed the Colorado Privacy Act ("CPA") into law, making Colorado the third state to enact a comprehensive privacy statute following California's enactment of the Consumer Privacy Act ("CCPA") in 2018 and the Privacy Rights Act ("CPRA") in 2020, and Virginia's enactment of the Virginia Consumer Data Protection Act ("VCDPA") in March of this year.

The CPA grants consumers certain rights over their personal data—including the right to opt out of the collection, use and sale of their data—and imposes affirmative obligations on businesses to safeguard such data. The CPA is similar in many ways to the California and Virginia statutes, and organizations that have already taken steps to comply with the CCPA and VCDPA (as well as the EU's GDPR) may therefore have a leg up in becoming compliant with the Colorado's new law. But the CPA is also unique in several keys respects. In a departure from the Virginia and California laws, the CPA applies to nonprofits as well as businesses. The CPA also notably directs the Colorado Attorney General to create specifications for a universal opt-out mechanism for data sales and processing of personal data for targeted advertising, which businesses will need to adopt and display. In his signing statement Governor Polis indicated that the law seeks to balance consumer protections with the need to foster technical innovation and a welcoming business environment.[1]

Organizations will need to assess whether their business practices are covered by the CPA and, if they are, take measures to ensure they are compliant before the statute comes into effect on July 1, 2023.

Key Provisions of the CPA

Applicability: Entities and Activities That Fall Under the Scope of the CPA

The CPA applies to a broad swath of businesses and nonprofit organizations, with certain significant exemptions noted below. In general, the CPA applies to any "controller" that "conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado" and that either:

- Controls or processes the personal data of at least 100,000 Colorado consumers or more during a calendar year; or
- Derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 Colorado consumers or more.[2]

[1] Signing Statement of Colorado Governor Jared Polis, July 7, 2021, *available at* https://iapp.org/media/pdf/publications/SB21-190_Signing_Statement_CO.pdf

[2] Colorado Revised Statutes § 6-1-1304(1)

Key Definitions

The CPA's definitions of controller, consumer, personal data and sale further clarify its scope.

- The CPA defines a "controller" as an entity that "alone or jointly with others, determines the purposes for and means of processing personal data.[3] This definition mirrors the definition in the GDPR.
- The CPA defines a "consumer" as "an individual who is a Colorado resident acting only in an individual or household context." This notably excludes individuals "acting in a commercial or employment context, [or] as a job applicant."[4]
- The CPA defines "personal data" as "information that is linked or reasonably linkable to an identified or identifiable individual" and excludes "de-identified data or publicly available information."[5]
- The CPA broadly defines a "sale" of personal data as "the exchange of personal data for monetary or other valuable consideration by a controller to a third party." This is similar to the CCPA's definition, whereas the VDCPA defines "sale" more narrowly (limited to monetary consideration).[6]
- The CPA defines "sensitive data" as "personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or personal information of a known child."[7]

Exemptions

The CPA exempts certain types of entities as well as specific categories of data from its requirements.

Under the CPA, entities whose data is regulated by certain federal statutes, including financial institutions subject to the Gramm-Leach-Bliley Act, registered national securities associations and air carriers are exempted from coverage.

The CPA similarly does not cover certain categories of data that are already regulated by other state or federal privacy laws. These categories include educational data covered by the Family Educational Rights and Privacy Act,[8] children's data covered by the Children's Online Privacy Protection Act,[9] Personal Health Information created for purposes of complying with the Health Insurance Portability and Accountability Act,[10] data regulated by the Fair Credit Reporting Act[11] and employment data.[12]

[3] Colorado Revised Statutes § 6-1-1303(7)

[4] Colorado Revised Statutes § 6-1-1303(6)

[5] Colorado Revised Statutes § 6-1-1303(17)

[6] Colorado Revised Statutes § 6-1-1303(23)

[7] Colorado Revised Statutes § 6-1-1303(24)

[8] Colorado Revised Statutes § 6-1-1304(2)(j)(V)

[9] Colorado Revised Statutes § 6-1-1304(2)(j)(IV)

[10] Colorado Revised Statutes § 6-1-1304(2)(e)

[11] Colorado Revised Statutes § 6-1-1304(2)(i)(C)(II)

[12] Colorado Revised Statutes § 6-1-1304(2)(k)

Consumer Rights[13]

The CPA provides various rights to consumers with regards to their personal data, including the right to opt out, the right to access, the right to correction, the right to delete and the right to data portability. Although consumers may only exercise the right to data portability twice per year, the CPA permits consumers to obtain *any* personal data obtained by a controller, which is broader than the similar right enshrined in the VCPDA that permits consumers to obtain only personal data consumers have themselves provided to a controller.

The CPA also differs from other U.S. data privacy laws in that it will require the state AG to adopt rules detailing specifications for a universal opt-out mechanism by which consumers can opt out of data-processing activities for purposes of sales or targeted advertising. Importantly, the law takes the novel step of permitting consumers to exercise their opt-out rights via authorized third parties and through automated means such as a web link, browser setting, browser extension or global device setting.[14]

Additionally, a controller must respond to consumer requests to exercise these rights within 45 days, with the option to extend the period for another 45 days if reasonably necessary.

Duties of Controllers and Processors

Controllers bear the lion's share of responsibility under the CPA.[15] At a high level, the law requires controllers to:

- Provide consumers with an accessible, clear and meaningful privacy notice;
- Disclose in a conspicuous manner any sale of consumer data or processing of personal data for targeted advertising and the manner in which a consumer may opt out;[16]
- Limit the collection of personal information to what is reasonably necessary for the stated purpose and take reasonable measures to secure personal data;
- Refrain from processing sensitive data without first obtaining affirmative consumer consent;[17] and
- Conduct data protection assessments that must be provided to the attorney general upon request.[18]

[13] Colorado Revised Statutes § 6-1-1306

[14] Colorado Revised Statutes § 6-1-1306(1)(a)(II)

[15] Colorado Revised Statutes § 6-1-1308

[16] Colorado Revised Statutes § 6-1-1306(1)(a)(IV)(B) provides that controllers must implement an opt out mechanism by July 1, 2024.

[17] Consumer consent must be affirmative, and such consent cannot be secured through acceptance of general terms of use; hovering over, muting, pausing, or closing content; or use of dark patterns.

[18] Colorado Revised Statutes. § 6-1-1309 requires controllers to conduct data protection assessments of (i) processing of personal data for purposes of targeted advertising or profiling (where certain conditions apply); (ii) any processing of sensitive data; and (iii) sales of personal data.

The CPA also imposes certain obligations on data processors.[19] Processors must adhere to the controller's instructions, assist the controller in meeting its obligations and maintain a duty of confidentiality. The CPA requires that all processing be governed by a contract between the controller and processor that outlines relevant consumer privacy provisions. [20]

Enforcement

The CPA does not authorize a private right of action;[21] the Colorado Attorney General and district attorneys have exclusive enforcement authority.[22] Similar to the California regime and unlike the VDCPA, the CPA grants the Attorney General significant rulemaking authority to specify the details of various provisions of the statute.

Non-compliance with the CPA is considered a deceptive trade practice,[23] which under Colorado law can result in fines up to $20,000 for each violation.[24]

Until January 1, 2025, prior to any enforcement action, the Attorney General or a district attorney must issue a notice of violation to the controller if a cure is possible. An enforcement action may be brought only if the controller fails to cure the violation within 60 days after receipt of the notice of a violation.[25]

Comparison with Other Comprehensive Privacy Regimes

Applicability

The CPA's jurisdictional thresholds are similar to the VCDPA's, which covers entities that (1) control or process the personal data of at least 100,000 Virginia residents annually, or (2) control or process personal data of at least 25,000 Virginia residents and derive over 50% of gross revenue from the sale of personal data.[26]

However, the CPA's lower applicability threshold (25,000 users) kicks in if an entity derives *any* revenue from the sale of personal data, as opposed to a certain percentage of its revenue.

Notably, neither the CPA nor the VCDPA contains a standalone revenue threshold similar to the one included in the CCPA that makes any business that operates in California, collects the personal information of California residents and has annual gross revenues of $25 million subject to the statute.[27] The CPA also does not adopt the inclusive provisions of the California regime that make parent and subsidiary companies that share the same branding subject to the CCPA, even if those individual entities do not alone exceed the applicable thresholds.[28] By comparison, the GDPR extends further than any of its U.S. counterparts,

[19] The statute defines a data processor as an entity "that processes personal data on behalf of a controller." Colorado Revised Statutes § 6-1-1303(19).

[20] Colorado Revised Statutes § 6-1-1305(5)

[21] Colorado Revised Statutes. § 6-1-1310

[22] Colorado Revised Statutes § 6-1-1311

[23] Colorado Revised Statutes § 6-1-1311(1)(C)

[24] Colorado Revised Statutes § 6-1-112(1)(a)

[25] Colorado Revised Statutes § 6-1-1311(d)

[26] Va. Code. Ann. § 59.1-576(A)

[27] Cal. Civil Code § 1798.140(d)

[28] Cal. Civil Code § 1798.140 (C)(1)(C)(2)

including the CPA, by covering any organization that offers goods or services to EU consumers or businesses, *or* collects personal information from EU citizens, regardless of revenue.[29]

Finally, in a departure from both the CCPA and the VCDPA, the CPA also applies to nonprofit organizations. Here, the CPA is more like the GDPR, which includes nonprofit organizations and other associations and applies to any donations these organizations receive from EU data subjects.

Exemptions

Like the VCDPA and CCPA, the CPA exempts certain categories of information based on entity-type and category of data. However, the CPA's exemptions are narrower in some respects than the VCDPA's and CCPA's and broader in others. Most notably, both the CPA[30] and the VCDPA[31] permanently exempt from their coverage employment records and personal information gathered in business-to-business settings. Perhaps the drafters of the Virginia and Colorado statutes looked to avoid the difficulties created by the California regime, which has extended on multiple occasions the exemption for B2B and employee data, initially set to expire on January 1, 2021, and which now expires on January 1, 2023.[32]

Although the VCDPA and CCPA exempt many of the same entities and categories of data as the CPA, the CPA is unique in exempting air carriers and national securities associations.

Consumer Rights

The consumer rights provided under the CPA are also similar to those provided under both the VCDPA and the GDPR. However, the CPA goes further in several key respects. First, and most notably, the CPA requires data controllers to allow consumers to opt out through a "user selected universal opt-out mechanism." The CPA directs the Colorado AG to devise specifications for the opt-out mechanism by July 1, 2023, and the requirement will go into effect on July 1, 2024. Second, unlike the GDPR, the CPA's opt-out right does not contain an exception for profiling that is necessary to perform a contract with a consumer or is authorized by domestic law.

The CPA also parrots the approach taken by the Virginia law by requiring businesses to provide an appeals process for customers whose rights are denied and mandating that consumers be informed of their right to contact the Colorado attorney general.

Duties of Controllers and Processors

For the most part, the CPA's similarities to the Virginia privacy regime carry over to the duties of controllers and processors under the statute. However, the statute departs from both the VCDPA and California data privacy laws by imposing more stringent transparency requirements with regards to the activities of subprocessors, as well as the ability of controllers to limit disclosure of data protection assessments through claims of confidentiality and privilege.

The CPA follows the example of the GDPR, as well as U.S. state data privacy laws by setting out data minimization and proportionality requirements whereby controllers must limit the collection of data based on adequacy, relevance and proportionality to the purpose for collection or processing.[33] Also similar to existing privacy regimes, the CPA requires that

[29] Territorial scope of the GDPR from a U.S. Perspective, June 26, 2018 *available at* https://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/

[30] Colorado Revised Statutes § 6-1-1304(2)(k)

[31] Va. Code. Ann. § 59.1-576(C)(14)

[32] Cal. Civil Code § 1798.145

[33] Colorado Revised Statutes § 6-1-1308(3)

controllers establish and maintain reasonable administrative, technical and physical data security practices that are appropriate to both the nature and volume of personal data collected and stored by the controller.[34]

The CPA also continues the course taken by the CPRA and VCDPA by carving out a separate category for "sensitive data." But the Colorado statute diverges from the California regime (and joins the VCDPA) in requiring that controllers first obtain affirmative consent from consumers before processing sensitive data.[35]

Also similar to the VCDPA, the CPA requires controllers to conduct data protection assessments for certain high risk data activities.[36] However, while both the VCDPA and CPA require controllers to produce these assessments at the request of the state AG, only the CPA considers data protection assessments to be confidential and subject to privilege, thereby potentially limiting public disclosure through state freedom of information laws.[37]

The transparency requirements set out by the CPA are not modeled after either U.S. privacy regime, and more closely resemble recent guidance from the European Commission pertaining to the new standard contractual clauses for international data transfers. The CPA, like the EU guidance, requires processors to give controllers notice of all subcontractors, as well as an opportunity to object. As a result, the CPA's requirements of visibility into the activities of subprocessors sets a higher standard than that of the transparency measures in either the Virginia or California statutes.[38]

Enforcement

Similar to the approach taken in the VCDPA, the CPA vests enforcement authority with the state AG. However, the CPA also permits local Districts Attorney to enforce the statute. Both differ from the California laws, which will be enforced by a new administrative authority, the California Privacy Protection Agency. The CPA also diverges from the California regime by explicitly stating that there the statute does not create a private right of action, thus further aligning with the provisions of the Virginia law.

The remedies available under the CPA are less certain than the standardized cost per violation outlined in the VCDPA. Unlike the VCDPA, the Colorado law defines a violation of the statute as a deceptive trade practice and incorporates the penalties available for violations of the Colorado Consumer Protection Act (fines up to $20,000 for each violation).[39] And the CPA provides for a 60-day period during which controllers and processors may cure an alleged violation of the statute, as opposed to the 30 days provided by the VCDPA and CCPA/CPRA.[40]

Implications

- Following closely on the heels of the VCDPA, Colorado's privacy law suggests growing popular support for consumer privacy protections. This momentum, combined with the fact that businesses are subject to an increasingly complex patchwork of state laws, may generate pressure for comprehensive federal legislation.

[34] Colorado Revised Statutes § 6-1-1305(2)(a)

[35] Colorado Revised Statutes § 6-1-1308(7)

[36] Colorado Revised Statutes § 6-1-1309(1)

[37] Colorado Revised Statutes § 6-1-1309(4)

[38] Colorado Revised Statutes § 6-1-1308(1)

[39] Colorado Revised Statutes § 6-1-1311(1)(c); Colorado Revised Statutes § 6-1-105

[40] Colorado Revised Statutes § 6-1-1311(1)(d)

- The similarities between Colorado's new law and the VCDPA may allow companies subject to both statutes to find efficiencies when taking measures to comply with the requirements of both statutes. Further, the similarities suggest that states may be converging around a relatively standard set of consumer rights and core requirements governing businesses.

- The debate surrounding the enactment of the CPA was evident in Colorado Governor Jared Polis's signing statement, which acknowledged the difficult balance between fostering technical innovation and a welcoming business environment while also ensuring consumer protection. Governor Polis called for continued negotiations to pass clean-up legislation, which could lead to further modifications similar to those made to the CCPA by the CPRA.[41]

- The CPA will impose new burdens on U.S. nonprofit organizations falling within its scope, many of which have not previously been subject to a comprehensive data privacy law.

* * *

[41] Signing Statement of Colorado Governor Jared Polis, July 7, 2021, *available at* https://iapp.org/media/pdf/publications/SB21-190_Signing_Statement_CO.pdf

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Chris Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jeannie Rhee
+1-212-373-7466
jrhee@paulweiss.com

Roberto Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Steve Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associates Emily Glavin and Cole Rabinowitz, and Staff Attorney Bertie Cheng contributed to this client memorandum