BakerHostetler

Colorado's Privacy Act

A Curve Ball on Consent and Targeted Ads

By Andreas Kaltsounis, Shea Leitch and Stanton Burke

On July 7, 2021, Gov. Jared Polis signed the Colorado Privacy Act (CoPA) into law, making Colorado the third state to enact a comprehensive privacy law, joining California and Virginia. The Act goes into effect on July 1, 2023, and shares many of the rights and obligations provided in other comprehensive privacy laws such as the GDPR, CCPA and Virginia CDPA. Our prior blog posts regarding the CCPA/CPRA and the CDPA outline the significant requirements of those laws.

The Colorado Privacy Act similarly provides consumers with various rights to access, obtain a copy of, correct and delete their personal data. Consumers may also opt out of certain processing activities, including data sales and targeted advertising. Like the CCPA and CDPA, the CoPA requires entities to enter into agreements with data processors to ensure that data disclosures are not considered to be sales. In addition to these requirements that have been the hallmark of privacy legislation to date, the CoPA adds a strict consent standard for sensitive data processing. Additionally, under CoPA, Colorado will also be the first state to explicitly require controllers to honor universal opt-out signals for targeted advertising. In this alert, we examine the more unique aspects of the CoPA before turning to the CoPA's more familiar provisions.

Who Should Care?

The CoPA applies to any organization that controls or processes personal data regarding 100,000 Colorado consumers or "derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes the personal data of [25,000] consumers or more." Individuals "acting in a commercial or employment context" are excluded from the definition of "consumers."

Additionally, CoPA establishes broad carve outs for customer data maintained by a public utility, protected health information collected by covered entities and business associates (essentially, HIPAA data), certain FCRA-related data, and data that is collected, processed, sold or disclosed according to the GLBA, FERPA, COPPA, and/or the Driver's Privacy Protection Act. However, diverging from the CCPA and the CDPA, the CoPA does not exempt nonprofit entities.

Novel Provisions

Consent to Process Sensitive Information

Like the CDPA, the CoPA requires companies to obtain consent before processing "sensitive data," which includes information "revealing":

- Racial or ethnic origin.
- Religious beliefs.
- A mental or physical health condition or diagnosis.
- Sex life or sexual orientation.
- Citizenship or citizenship status.
- Genetic data.
- Biometric data.
- Personal data regarding a known child.

Note that unlike the CDPA and CPRA, the CoPA's definition of sensitive data does not include precise geolocation or financial data.

When analyzing whether they process sensitive data, controllers should evaluate whether the data they process reveals any sensitive data, even if no sensitive data will be collected directly. For example, information regarding a person's sexuality may be revealed through profile information developed through the use of cookie data for behavioral advertising. Similarly, it is possible to obtain information regarding a person's racial or ethnic origin through facial recognition and voiceprint.

Under CoPA, companies will have to obtain express, affirmative consent to process personal data if that data involves or reveals sensitive data. CoPA defines consent as "a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data." However, diverging from the CDPA, the CoPA further clarifies that consent does not include:

- Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information.
- Hovering over, muting, pausing or closing a given piece of content.
- Agreement obtained through dark patterns.

Under this definition of consent, companies will no longer be able to use general acceptance of terms of use or broad notices with unrelated terms as evidence of consent to process sensitive personal data. Additionally, a stand-alone cookie banner broadly stating that use of the service constitutes consent to the processing of personal data will not be sufficient. Finally, companies that process sensitive data should examine their privacy policies to ensure the provisions regarding sensitive data are sufficiently clear, as consent obtained through "dark patterns" (i.e., "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice") will not satisfy the CoPA standard. As a practical matter, the new CoPA consent requirements likely mean that controllers processing sensitive data may have to develop a separate privacy notice for the processing of sensitive personal data, to which consumers must agree by express, affirmative consent.

It is also important to note that the CoPA's requirement to obtain consent prior to the processing of sensitive personal data, while aligned with the CDPA and the GDPR, is notably more burdensome than the CPRA—which only requires businesses to provide consumers with the ability to request that the business limit the use of their sensitive personal information to select, permitted purposes.

Universal Opt-Out

CoPA will make Colorado the first state to explicitly require companies to honor a universal opt-out signal. Starting July 1, 2024, controllers must allow consumers to opt out of targeted advertisements and/or the sale of personal data through a universal opt-out mechanism that meets the technical specifications established by the state Attorney General (AG). For example, the Global Privacy Control that was recently endorsed by the California AG in the updated FAQs, if programmed to opt users out of targeted ads and the sale of personal data, would likely satisfy this requirement. The Colorado AG has until July 1, 2023, to promulgate CoPA regulations establishing the technical specifications that a universal opt-out signal must meet.

Notably, the right to opt out of targeted advertisements under the CoPA and CDPA are very similar to the right to opt out of the sharing of personal information under the CPRA. For example, each right includes an exception for advertising to users based on their own activity and interactions on the controller's own website or mobile application, as this is not considered cross context behavioral advertising. In addition, each right clarifies that if a controller ingests personal data from a third party and combines it with its own user's personal data, that would constitute targeted advertising under each statute. As such, to the extent that a business wants to maintain a single approach for the opt-out of targeted ads, the business can likely fulfill the requirement through the CPRA's "Do Not Share My Personal Information" link on the homepage, if applicable.

The requirement to honor universal opt-out requests is likely to present challenges to controllers. To date, different technology companies and industry organizations have offered opt-out methods for certain tracking technologies. However, no consensus has developed as to how a universal opt-out would work in practice with the variety of tracking technologies and industry players existing in the adtech ecosystem. Both Delaware and California require companies to disclose whether they respond to "Do Not Track" signals; however, honoring "Do-Not-Track" signals has remained optional under these laws. After July 1, 2024, honoring a universal opt-out signal satisfying the AG's requirements will no longer be optional under the CoPA.

Familiar Provisions

Consumer Rights

Under the CoPA, consumers are granted rights to access, obtain a portable copy of, correct, and delete their personal data. Consumers also have the right to opt out of: (1) targeted advertising, (2) the sale of personal data and (3) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer. As discussed more thoroughly above, controllers may not process sensitive data without consent.

Right to Appeal

Under the CoPA, if the controller decides it will not act on a request, the controller must inform the affected consumer of the reasons for not taking action and provide the consumer with instructions on how to appeal the decision. The appeal process must be conspicuously available and as easy to use as the process for submitting the original request. Upon receiving an appeal, the controller has 45 days to inform the consumer with a decision and an explanation of the reasons in support of the decision. The controller must also inform the consumer of their ability to contact the state AG if they have concerns with the results of their appeal.

Controllers and Processors

The CoPA requires controllers and processors to enter into Data Protection Agreements and outlines the required provisions, which include:

- Processing instructions to which the processor is bound, including the nature and purpose of the processing.
- The type(s) of personal data subject to the processing, and the duration of the processing.
- That data will be deleted or returned to the controller at the end of the term of the agreement.
- An agreement to make necessary and relevant information available to the controller and its auditors to demonstrate compliance.

In addition, processors must adhere to the controller's instructions and flow down contractual obligations to sub-processors. Regarding audits, processors are obligated to either submit to "audits and inspections" by the controller or, with the controller's consent, engage an independent auditor to evaluate the processor's security controls on an annual basis at least. The auditor's report must be provided to the controller upon request.

Data Protection Assessments

Under the CoPA, controllers are directly obligated to respond to consumer rights requests, whereas processors are obligated to assist controllers with consumer requests. Controllers must

conduct a data protection assessment (DPA) for each of their processing activities involving personal data that presents a heightened risk of harm to consumers, including targeted advertising, selling personal data, processing sensitive data, and certain profiling activities that create a foreseeable risk of unfair treatment of consumers, financial or physical injury, or intrusion upon the solitude or seclusion of the private affairs of consumers. The assessment must identify and weigh the benefits from the processing to the controller, consumer, other stakeholders and the public against the potential risks to consumers' rights. Assessments must be made available to the AG upon request. However, the disclosure of a DPA does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment.

As with the CDPA, controllers will also have a duty to adhere to certain principles when processing personal data, including transparency, purpose specification, data minimization, avoiding processing for secondary purposes that are not compatible with the specified purpose, using reasonable measures to secure personal data, and avoiding discrimination on the basis of protected characteristics or the exercise of a right by a consumer.

Enforcement

The CoPA does not create a private right of action. The Colorado AG and district attorneys have exclusive authority to enforce the provisions of the CoPA. Non-compliance with the law is considered a deceptive trade practice. While the CoPA does not directly identify penalties for noncompliance, deceptive trade practices are subject to a $20,000 civil penalty per violation under the Colorado Consumer Protection Act. Since each violation can be interpreted to mean a separate violation with respect to each consumer or transaction, the penalties may increase considerably. Before initiating an enforcement action for violations of the CoPA, the Colorado AG must provide a 60-day cure period to enable the business to rectify non-compliance. However, the notice and cure provision is automatically repealed on Jan. 1, 2025.

What's Next?

In general, the Colorado AG has the authority to promulgate additional rules and guidance around the CoPA, but is not required to do so. However, as mentioned above, by July 1, 2023, the Colorado AG must adopt rules for the universal opt-out mechanism. In addition, the Colorado AG may adopt rules that govern opinion letters and interpretive guidance by July 1, 2025.

Conclusion

While many of the rights and obligations set forth in the CoPA are familiar to organizations that process personal data, the CoPA establishes novel provisions including new consent requirements regarding sensitive data and a universal opt-out, as well as additional requirements around Data Processing Agreements and Data Protection Assessments. Companies subject to the GDPR or the CCPA will have a head start with respect to preparations for the CoPA's July 1, 2023, effective date. That said, companies that process sensitive personal data regarding consumers should begin to consider how to provide notice and collect appropriate consent under CoPA. Additionally, companies that operate in the digital advertising space should carefully watch for guidance provided by the California AG or Colorado AG as to what universal opt-out signal may be acceptable under the CCPA/CPRA and the CoPA, respectively.

If you have any questions regarding the applicability of these privacy laws and how to prepare for them, including conducting data mapping, updating privacy policies and data processing agreements, and/or building a process for conducting a data protection assessment, feel free to reach out to the authors or others in BakerHostetler's Digital Assets and Data Management (DADM) Practice Group, subscribe to our Data Counsel blog, and visit our Consumer Privacy Resource Center.

02.08.21.16.37_P01