Updates
October 14, 2022
Western States Continue To Shape US Privacy Landscape: Colorado CPA and California CPRA

The Colorado attorney general's office sent shockwaves throughout the privacy world on September 30, 2022, when it published its proposed Colorado Privacy Act (CPA) draft rules (Draft Rules). The Draft Rules are complex and comprehensive; at 38 pages of single-spaced text, they are longer than the CPA itself. The Draft Rules are accompanied by a proposed timeline for stakeholder meetings and a public hearing.

Coming on the heels of this announcement, on October 10, California announced that it will hold meetings on October 21 and October 22 to discuss "possible adoption or modification of the text [of the draft California Privacy Rights Act (CPRA) regulations]."

Below we outline and analyze some of the key provisions of the Draft Rules and call out certain differences between the Colorado Draft Rules and the CPRA draft regulations released in May.

High-Level Summary and Key Provisions

Overview

The Draft Rules are neatly divided into nine overarching parts: (1) General Applicability, (2) Definitions, (3) Consumer Disclosures, (4) Consumer Personal Data Rights, (5) Universal Opt-Out Mechanism (UOOM), (6) Duties of Controllers, (7) Consent, (8) Data Protection Assessments, and (9) Profiling. Part 10 accompanies these Draft Rules, incorporating by reference the CPA and the World Wide Web Consortium's Web Content Accessibility Guidelines. We focus on some key provisions, ambiguities, and takeaways below.

Definitions

The Draft Rules introduce new concepts of "Biometric Data" and "Biometric Identifiers" but do not clearly define "Biometric Data." "Biometric Identifiers" are defined in the Draft Rules as "data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics," but behavioral characteristics are not defined.

The Draft Rules also introduced a unique concept of "Sensitive Data Inferences." Under the Draft Rules, controllers may process sensitive data inferences without consent if they are deleted within 12 hours of collection or of the completion of the processing. If not deleted in this manner, these inferences would need to be treated as sensitive data requiring consent for processing.

Consumer Personal Data Rights

The Draft Rules offer some flexibility for businesses here, as "Data Rights requests method[s] [do] not have to be specific to Colorado, so long as the request method: (1) clearly indicates which rights are available to Colorado Consumers; (2) provides all Data Rights available to Colorado Consumers; (3) provides Colorado Consumers a clear understanding of how to exercise their rights..." Practically speaking, if adopted, this would likely allow businesses significant leeway to align their data rights processes across different states, including California. Similarly, the Draft Rules would simply require that companies establish "reasonable methods" to authenticate data rights requests without dictating the precise manner in which they must authenticate those requests.

Universal Opt-Out Mechanism

Unlike the draft regulations issued under the CPRA, the Draft Rules provide extensive guidance, including technical guidance, for recognizing and honoring universal opt-out mechanisms (UOOMs). As described in the Draft Rules, UOOMs are a method "to provide Consumers with a simple and easy-to-use method by which Consumers can automatically exercise their opt-out rights with all Controllers they interact with." Specifically, controllers would need to "make clear to the consumer…that the mechanism is meant to have the effect of opting the Consumer out of the Processing of Personal Data for specific purposes or all purposes." Furthermore, the UOOM could "not be the default setting for a tool that comes pre-installed with a device" or "require the collection of additional Personal Data beyond that which is strictly necessary to confirm a Consumer is a resident of Colorado" or to authenticate the opt-out request. Unlike the CPRA draft regulations, which provide that such signals may be any commonly used format, the Draft Rules would provide far more certainty as to which signals must be honored, as the Colorado attorney general's office will be required to maintain a public list of recognized UOOMs.

Duties of Controllers

Similar to other states, the Draft Rules would require businesses to host a comprehensive privacy policy that explains how the company collects, processes, and discloses data. However, the Draft Rules go further than the California draft regulations by requiring controllers to explain the "processing purposes" for each type of information they collect in a level of detail that gives consumers a meaningful understanding of how their personal data is used and why their personal data is reasonably necessary for the processing purpose. While the Draft Rules do not mandate providing these disclosures in a "Colorado-specific privacy notice or section of a privacy notice" so long as the privacy notice contains all of the required portions under the Draft Rules, it is difficult to imagine how companies could provide the required disclosures in a way that is consistent with their disclosure obligations under other laws. Consumers must be notified of "substantive or material change[s]" at least 15 calendar days before the changes go into effect.

The Draft Rules also dictate a range of required disclosures for controllers that offer "Bona Fide Loyalty Programs," including (1) the categories of personal data collected through the program that will be sold or processed for targeted advertising, if any; (2) the categories of third parties that will receive the consumer's personal data, including whether personal data will be provided to data brokers; (3) the value of the bona fide loyalty program benefits available to the consumer if the consumer opts out of the sale of personal data or processing of personal data for targeted advertising and the value of the bona fide loyalty program benefits available to the consumer if they do not opt out; and (4) a list of program benefits that require the processing of personal data for sale or targeted advertising and the third party receiving the personal data and providing each such program benefit, if applicable. Notably, differing from other state laws, if a customer "refuses to Consent to the Processing of Sensitive Data necessary for a personalized Bona Fide Loyalty Program Benefit, the Controller is no longer obligated to provide that personalized Bona Fide Loyalty Program Benefit. However, the Controller shall provide any available, non-personalized Bona Fide Loyalty Program Benefit for which the Sensitive Data is not necessary."

Data Protection Assessments

The Draft Rules would require that data protection assessments (DPAs) reflect a "genuine, thoughtful analysis" and are performed prior "to initiating a data Processing activity that Presents a Heightened Risk of Harm to a Consumer." Such activities include selling data, processing sensitive data, and engaging in certain types of profiling activities. The Draft Rules specify 18 requirements that must be described "at a minimum" within a DPA.

Highlights of Comparisons Between Colorado and California Draft Provisions

The Draft Rules differ from the CPRA draft regulations in key respects. While businesses will certainly be able to leverage some of the work they do for CPRA compliance to meet the obligations of the Draft Rules, businesses should take note that despite early indications to the contrary from the Colorado attorney general's office, the Draft Rules, if finalized, will impose Colorado-specific obligations.

Below, we highlight brief, high-level comparisons between the two sets of draft regulations:

CONCEPT	COLORADO	CALIFORNIA
Dark Patterns	Comparable language in both states defining and prohibiting dark patterns.	Comparable language in both states defining and prohibiting dark patterns.
Opt-Out Requests	A controller must provide an opt-out method "either directly or through a link, clearly and conspicuously in its privacy notice as well as in a clear, conspicuous, and readily accessible location outside the privacy notice." If a controller uses a link, the link must take a consumer directly to the opt-out method, and the link text must provide a clear understanding of its purpose, for example, "Colorado Opt-Out Rights," "Personal Data Use Opt Out," or "Your Opt-Out Rights."	Businesses are required to provide a "Do Not Sell or Share My Personal Information" that "will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice." Additionally, the CPRA draft regulations provide an alternative opt-out link and corresponding protocols, which encompass both a consumer's right to opt out of sale and right to limit.
UOOM vs. OOPS	Defined as "Universal Opt-Out Mechanisms," the purpose is to "provide Consumers with a simple and easy-to-use method by which Consumers can automatically exercise their opt-out rights with all Controllers they interact with…"	Defined as "Opt-Out Preference Signals," the purpose is to "provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt out of sale/sharing."
Loyalty Programs	If the consumer requests the deletion of their personal data, the controller is not obligated to provide loyalty benefits unless such benefits do not require personal data.	Businesses are required to provide notice of the material terms of the financial incentive program to the consumer before they opt in to the program.
Data Protection Assessments	Minimum of 18 different topics identified in the rule required to be described.	Not addressed in draft CPRA regulations, though the CPRA provides rulemaking authority on this topic.
Profiling/Automated Decision-making	For profiling that produces legal or similarly significant effects, controllers would need to disclose in the privacy policy a "plain language explanation of the logic used in the Profiling process."	Not addressed in draft CPRA regulations, though the CPRA provides rulemaking authority on this topic.

Next Steps

The Colorado attorney general included in its announcement a general schedule of next steps and stated that it will hold three stakeholder meetings in November dedicated to different topics:

- November 10, 2022 – Consumer Rights and Universal Opt-Out Mechanisms
- November 15, 2022 – Controller Obligations and Data Protection Assessments
- November 17, 2022 – Profiling, Consent, and Definitions

Additionally, the Colorado attorney general will hold a proposed rulemaking hearing on February 1, 2023. Those wishing to attend the hearing may register here. After the hearing, the Colorado attorney general will have 180 days to file adopted rules with the Colorado secretary of state for publication in the *Colorado Register*. The CPA is still scheduled to go into effect on July 1, 2023.

Our Privacy & Security Law team will monitor upcoming developments and collaborate with our clients to ensure their concerns are heard as the Colorado attorney general's office and California Privacy Protection Agency move forward with their respective rulemaking processes.

Authors

Explore more in

Technology Transactions & Privacy Law Privacy & Security

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law