**REGULATORY ALERT**

**TO:** ATP Members

**FROM:** Alan Thiemann, Donna McPartland, and William Snoeyenbos Han Santos, PLLC

**DATE:** January 7, 2023

**RE: Summary of Colorado Privacy Act Proposed Rules**

This Memorandum discusses the key provisions of the Colorado Privacy Act (“CPA”) proposed rules, which were originally published by the Colorado Secretary of State on October 10, 2022 (4 CRR 904-3), although a revised version of the draft rules was recently published on December 21, 2022. We suspect that further changes are probably going to be made between now and final adoption, so testing organizations will need to monitor these changes and try to structure their compliance activities accordingly. The CPA gives the Colorado Attorney General authority to adopt rules governing privacy and requires that the AG specifically adopt rules by July 1, 2023, that detail the technical specifications for one or more universal opt-out mechanisms that clearly communicate a consumer’s affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data.[[1]](#footnote-1)

Public comments may be submitted as part of the formal rulemaking process until February 1, 2023. A public hearing on the proposed draft rules is scheduled for February 1, 2023. Following the hearing, the Attorney General has 180 days to file adopted rules with the Secretary of State for publication in the Colorado Register. Adopted rules go into effect twenty days after publication or on such later date as is stated in the rules. Unfortunately, with this timetable, testing organizations are likely to have almost no lead time to digest the final rules and figure out how to comply before the effective date of the law on July 1, 2023.

Much like California and Virginia, the CPA creates consumer privacy rights for residents of Colorado including the right to opt-out of certain processing of personal data, as well as the right to access, correct, or delete personal data, or to obtain a portable copy of personal data. While the Colorado proposed draft rules share the same general enforcement principles as the California proposed regulations, there are several key differences concerning opt-outs, consent and consent withdrawal, handling consumer request responses, and privacy notices.

1. **OVERVIEW**
2. **Definitions**

The Colorado draft rules clarify many of the terms used in the Colorado Privacy Act that were either undefined or less clearly defined in the CPA’s original text.

1. Biometric Data

Similar to the new California Private Rights Act (CPRA), the CPA includes a separate category of “sensitive data.” Notably, the definition of sensitive data includes **genetic and biometric data** that can be used to uniquely identify an individual.[[2]](#footnote-2) The definition of biometric data is particularly important because the CPA requires controllers to obtain consent for the collection of such data without including a specific definition of genetic and biometric data.[[3]](#footnote-3) Moreover, this consent can be withdrawn at any time by a consumer similar to GDPR requirements for specially protected data.

The Colorado proposed draft rules address this gap by providing an explicit definition. The draft rules define “biometric data” to mean “Biometric Identifiers that are used or intended to be used, singly or in combination with each other or with other Personal Data, for identification purposes. *Unless such data is used for identification purposes*, “Biometric Data” does not include (a) a digital or physical photograph, (b) an audio or voice recording, or (c) any data generated from a digital or physical photograph or an audio or video recording.” Nevertheless, even under this definition, we believe a testing organization would be permitted to have a human match a test taker with a photo ID), or use of a video recording of the test taker and an ID to match a test taker on a remote test.

Further, “Biometric Identifiers” is defined as “data generated by the technological processing, measurement, or analysis of an individual’s biological, physical, or behavioral characteristics, including but not limited to a fingerprint, a voiceprint, eye retinas, irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics.” [[4]](#footnote-4)

The draft definition for biometric data is similar to definitions provided in other state privacy laws but does not directly track any of those definitions.

1. Personal Data

The definition of “personal data” does not include inferences drawn from any information used to create a profile about a consumer but the draft rules refer to inferences in the latest draft. Nevertheless, the law does include a provision to allow consumers to opt out of profiling,[[5]](#footnote-5) which is defined as “any form of *automated* processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual’s economic situation, health, personal preference, interest, reliability, behavior, location, or movements.”[[6]](#footnote-6) These provisions appear to be largely in conflict with one another and will undoubtedly create confusion; the final rules will hopefully clarify this problem. Testing organizations need to be able to assure themselves that each test does not constitute profiling, for which individual test takers may opt out. We believe that this result likely can be met by making sure there is meaningful human involvement in the testing and scoring process.

The CPA draft rules, however, now include restrictions related to “Sensitive Data Inferences”, which are defined as inferences made by a Controller based on Personal Data, alone or in combination with other data, which indicate an individual’s racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status.There is an exception, but it is very narrow. Specifically, controllers may process Sensitive Data Inferences from consumers over the age of thirteen without consent only if the following four-part test is met: the purpose of the processing is obvious to a "reasonable Consumer: both the underlying personal data and the Sensitive Data Inferences are deleted within 12 hours of collection or completion of the processing activity; the data is not sold or even shared with any processors; the data is not processed for any secondary purpose. This may capture some test sponsors’ test security and fraud prevention activities (i.e., citizenship) when looking for cheating rings or other fraudulent activity based on location of individuals. Privacy notices and test taker rules can be updated to inform test takers that the testing organization uses this information for identify verification, test security and fraud prevention. The other parts may be more difficult to meet.

1. Noncommercial Purpose

The revised draft regulations added a definition for “noncommercial purpose.” “Noncommercial Purpose” includes, but is not limited to, the following activities when conducted by a state institution of higher education, the state itself, or a city, county, or municipality within the state: (1) processing activities related to the delivery of services and benefits; (2) research purposes; budgeting; (3) improving operations or the delivery services or benefits; (4) auditing operations or service or benefit delivery; or (5) sharing Personal Data between these categories of entities for any of these purposes. While it is not completely clear, given this definition, it would appear that testing organizations whose customers are in state/district local education offices or in state higher education, would not be covered by the CPA.

1. **Opt-Outs**
2. Opt-Out Method Location

The CPA requires controllers to opt out consumers in the following situations: a) processing from targeted advertising; b) the “sale” of their personal data; and c) for profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer. The CPA draft rules set out further requirements for an opt-out method location to qualify as “clear, conspicuous, and readily accessible.” The opt-out method must be positioned in an obvious location of a website or application, such as the header or footer of a controller's internet homepage, or an application's app store page or download page; and available to the consumer at or before the time the personal data is processed for the opt-out purposes. If a link is used, the link must take a consumer directly to the opt-out method and the link text must provide a clear understanding of its purpose. Examples of appropriate wording which may be used include: (a) “Colorado Opt-Out Rights”; (b) “Personal Data Use Opt-Out”, or “Your Opt-Out Rights.”

Regardless of the opt-out used by a test taker, upon receiving an opt-out request, controllers must cease processing the personal data for the opt-out purpose(s) within fifteen (15) days. Accordingly, if tests/test results are considered profiling, then test sponsors/programs will have to deal with the required opt-out mechanisms.

1. Universal Opt-Out Mechanisms

Only if a controller is subject to the opt out requirements noted above, the draft rules set forth the technical specifications and other requirements for user-selected universal opt-out mechanisms (UOOMs) for any targeted advertising (e.g., Google Ads). The draft rules explain the purpose of UOOMs is to provide consumers with a simple and easy-to-use method by which they can automatically exercise their opt-out rights with all controllers they interact with without having to make individualized requests with each controller. The CPA requires controllers to recognize UOOMs effective July 1, 2024.

The draft rules explain the notice and choice provisions that UOOM developers must provide, how default settings must be addressed, and the technical specifications for UOOMs. The UOOM may operate through a means other than by sending an opt-out signal, for example by maintaining a “do not sell” list, so long as controllers are able to query such a list in an automated manner. A controller is permitted, but not required, to display that it has recognized the opt-out signal such as by displaying on its website “Opt-Out Preference Signal Honored.”

As discussed above, if a test sponsor/program is required to deal with UOOMs, this will add a significant compliance burden.

1. **Consent and Consent Withdrawal**

The CPA draft rules requires consent to be:

1. Obtained through the consumer’s clear, affirmative action;
2. Freely given;
3. Specific;
4. Informed; and
5. Reflect the consumer’s unambiguous agreement.

The draft rules provide guidance on each of these elements, which guidance is reminiscent of the European Data Protection Board’s Guidelines on consent. Additionally, the draft rules also clarify that consent can be withdrawn, which is not specifically stated in the CPA.

The proposed rules for consent withdrawal are likely to create new operational hurdles for compliance. The rules follow the California model and require a consumer to be able to revoke consent “as easily and within the same number of steps as consent is affirmatively provided.”[[7]](#footnote-7) But the current draft CPA rules now only suggests that, when an electronic interface is used and when it is feasible, a controller “may” allow consumers to track what processing activities they have consented to or opted out of. Any requirement for “tracking” of opt-outs would likely present technical difficulties for testing organizations, as acknowledged by the “when feasible” language, so this recent change in the draft rules is welcome.

1. Refreshing Consent

The draft rules required controllers to obtain refreshed test taker consent for processing sensitive data on an annual basis. Recently revised draft rules now state that refreshing consent is limited to instances in which a test taker has not interacted with the testing organization in the prior 12 months. It is equally important to note that a testing organization/controller is not required to refresh consent where a test taker has access and the ability to update opt-out preferences at any time through a user-controlled interface.

The revised draft rules also remove the provision that would have required a testing organization to obtain consent to process biometric identifiers or any personal data generated from a digital or physical photograph or an audio or video recording each year after the first year it is stored. Instead, a testing organization still must review such information at least annually to determine if its storage is necessary, adequate, or relevant to the express processing purpose for which it was collected.

1. Retroactive Consent

The revised draft rules also clarify how a testing organization is required to obtain consent for sensitive data. After the CPA goes into effect on July 1, 2023, a controller will be required to obtain consumer consent to collect sensitive data. The revised draft rules require the testing organization/controller to obtain consent prior to January 1, 2024. The revised draft rules also clarify that this requirement applies to the other instances in which the CPA requires consent (such as processing personal data for secondary purposes and circumventing an opt-out choice).

**D. Consumer Responses/Requests**

1. Timing

A testing organization/controller is required to inform a test taker within forty-five (45) days of any action taken on a consumer request. The controller may extend the 45-day period by an additional 45 days where reasonably necessary, given the complexity and scope of the request. The controller shall inform the test taker of the extension within forty-five (45) days of the request and provide an explanation for the delay.[[8]](#footnote-8) This is identical to the procedures in California.

1. Rejecting CPA Personal Data Right Requests

The CPA draft rules explain how a testing organization should respond when rejecting an individual test taker’s personal data right request.[[9]](#footnote-9) To comply with the draft rules, the controller’s response must include the basis for the controller’s decision. This basis includes, but is not limited, to:

1. Any conflict with federal or state law;
2. If the controller relied on an exception to the Colorado Privacy Act found at § 6-1-1304(2), a description of the exception;
3. The Controller’s inability to authenticate the consumer’s identity;
4. Any factual basis for a controller’s good-faith claim that compliance is impossible; or
5. Any basis for a good-faith, documented belief that the request is fraudulent or abusive.

If a testing organization denies a test taker’s request based on inability to authenticate the person, the controller must describe in documentation required by Rule 6.11 its reasonable efforts to authenticate and why it was unable to do so.

A testing organization that decides not to act on a test taker’s request must also provide instructions on how to appeal the controller’s decision in accordance with C.R.S. § 6-1-1306(3).

When a testing organization complies with a test taker’s request, the controller shall also use the technical and organizational measures or process established by its to fulfil requests for personal data held by the processors.[[10]](#footnote-10) Finally, a testing organization that is a controller must maintain all documentation as required by Rule 6.11.

**E. Privacy Notices**

The revised draft rules no longer require privacy notices to be structured around processing purposes. Originally, the Colorado Attorney General believed purpose-based privacy notices would be the best way to give meaning to the purpose specification and secondary use provisions of the CPA. After considering comments which argued purpose-based Privacy notices would be overly burdensome and not interoperable with California privacy notice requirements, the purpose-based requirement has been eliminated. Instead, the revised draft rules require that the processing purpose and type of personal data processed be linked in a way that gives consumers a “meaningful understanding of how their personal data will be used.”[[11]](#footnote-11)

The revised draft rules do require that controllers provide notices to test takers when there are substantive or material changes to a privacy notice. Such changes must be communicated to consumers in a manner by which the Controller regularly interacts with Consumers. The draft rules have a wide definition of Substantive or material changes that “may include, but are not limited to,” changes to: (1) categories of Personal Data Processed; (2) Processing purposes; (3) a Controller’s identity; (4) the act of sharing of Personal Data with Third-Parties; (5) the identity of Affiliates, Processors, or Third-Parties Personal Data is shared with; or (6) methods by which test takers can exercise their Data Rights request. Fortunately, the 15-day prior notice requirement was removed but the Controller is required to notify the test taker in a way that they regularly interact. If you normally convey changes to your privacy policy on your website or test registration homepage, this may be acceptable.

**CONCLUSION**

This Memorandum focuses on the draft rules we feel are most relevant to testing organizations, but we would caution that individual organizations may have specific procedures and policies that could be impacted by the CPA/draft rules in unique ways. Accordingly, you should do a comprehensive review and evaluation of the current draft rules to ascertain exactly what steps you and your organization will need to take to achieve compliance.

We will continue to monitor the status of the Colorado draft rules and report on the upcoming hearing outcome after the public comment period ends. As further information on the CPA draft rules becomes available, we will provide updates. When final rules are announced, we will provide a summary and comparison to help guide testing organizations in compliance efforts.

In the meantime, we recommend that testing organizations that do business in Colorado, or have a significant number of test takers located in Colorado, should begin to prepare for the new law/rules, but evaluating their privacy compliance efforts to identify what changes may be required under the Colorado rules as they exist at this time.

1. §6-1-1313(2) [↑](#footnote-ref-1)
2. §6-1-1303(24) [↑](#footnote-ref-2)
3. §6-1-1308(7) [↑](#footnote-ref-3)
4. 4 CCR 904-3 Rule 2.02 [↑](#footnote-ref-4)
5. §6-1-1306(1)(a)(C) [↑](#footnote-ref-5)
6. §6-1-1303(20) [↑](#footnote-ref-6)
7. 4 CCR 904-3 (Rule 7.07(A)) [↑](#footnote-ref-7)
8. § 6-1-1306(2)(a)-(b) [↑](#footnote-ref-8)
9. 4 CCR 904-3 (Rule 4.09) [↑](#footnote-ref-9)
10. 4 CCR 904-3 (Rule 4.09 (C)-(D)) [↑](#footnote-ref-10)
11. 4 CCR 904-3 (Rule 6.02) (A) [↑](#footnote-ref-11)