U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

January 30, 2023

Office of the Attorney General
Colorado Department of Law
Ralph L. Carr Colorado Judicial Center
1300 Broadway, 10th Floor
Denver, Colorado 80203

Re: Colorado Department of Law, Comments on The Proposed CPA Rules[1]

Dear Attorney General Weiser:

The U.S. Chamber of Commerce ("Chamber") appreciates the opportunity to comment on the Revised Draft Regulations implementing the Colorado Privacy Act ("CPA" or "Act"). For years, the Chamber has advocated for a robust national privacy standard that protects all Americans equally. Concurrently, the business community applauds the willingness of the Office of the Attorney General ("OAG") to work with stakeholders to strike the right balance between promoting consumer protection and promoting innovation. Overall, the OAG should harmonize its Proposed Regulations with the CPA and with other existing frameworks when appropriate.

I. Rule 2.02 (Defined Terms).

a. "Biometric Identifiers"

The language added to the newest "biometric identifiers" definition from the previous one[2] helps to clarify that its scope is limited to data processed for identification purposes, and is not intended to capture common data types. Although the new language incorporates an important clarification, the inclusion of this sub-definition within the definition of biometrics is an unnecessarily confusing construction that is out of step with emerging norms in U.S. state comprehensive privacy laws. The Chamber therefore recommends this definition be amended to align with the definition in the VA, CT, and UT frameworks, which promotes interoperability and capabilities for compliance.

[1] https://coag.gov/app/uploads/2023/01/CPA_Version-3-Proposed-Draft-Regulations-1.27.2023.pdf
[2] https://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf.

b. "Revealing"

To provide great uniformity and seamless compliance, the OAG should avoid creating terminology that has not been tested or adopted in other jurisdictions. The term "revealing" is outside the norm of other jurisdictions in other state privacy laws.

c. "Sensitive Data Inference(s)"

Companies already use a taxonomy of data elements which they classify as "Sensitive Personal Information" ("Sensitive P.I."). This is usually efficiently updated where a law provides a closed list of P.I. classified as Sensitive. However, as currently worded, companies would need to consider what P.I. *could* be used to make a sensitive inference about an individual. This would be very broad and open-ended. This is consequential because Colorado requires opt-in consent and DPIA's to process Sensitive PI. Such a novel definition would require companies to continuously second-guess data processing and could have a negative impact on needed research and development. The Chamber requests this definition be removed from the Proposed Regulations.

d. Clarifying the Scope of "Measurement"

The Chamber requests clarity in the Proposed Rules that in exceptions referring to "measurement"[3] implementing CPA that the term "measurement" include independent measurement. This concept of independent measurement is already widely adopted globally as well as clarified in other state jurisdictions. Independent measurement allows content creators and advertisers to know their actual viewership and other internet impressions in relation to the marketplace, thus allowing for accurate programming and marketing decisions.

II. Rule 4.04 (Right of Access)

a. Broadened Access Rights

The Revised Proposed Regulations have broadened what is required of consumer access requests to include "final Profiling decisions, inferences, derivative data, and other Personal Data created by the Controller which is linked or reasonably linkable to an identified or identifiable individual."[4]

This revision to the Proposed Rule risks creating an overly broad expectation that the access right should yield information that is the statutory requirement of the CPA. The CPA does not require Controllers or Processors to comply with an authenticated consumer request

[3] *See e.g.* CRS § 6-1-1303(25)(b)(IV).
[4] Proposed Rule 4.04(A)(1).

to access it meets the standards of CRS § 6-1-1307(b)[5] or (c)[6] or if data is pseudonymous and "the Controller can demonstrate that the information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information."[7] To ensure consistency with the statute and aligned expectations, this provision should be amended to expressly recognize this exclusion.

b. Trade Secrets

The Revised Proposed Regulations state that if consumers exercise portability rights "and the Controller determines the manner of response would reveal the Controller's trade secrets, the Controller must still honor the Consumer's undiminished right of access in a format or manner which would not reveal trade secrets, such as a nonportable format."[8] Although this right refers to portability rights under CRS § 6-1-1306(1)(e), it does not appear to apply to general rights of access under CRS § 6-1-1306(1)(b).

While the Chamber recognizes that this provision aims to address a tension in the statute between portability and access rights, as drafted, the provision will have the unfortunate effect of compromising industry trade secrets altogether–something the statute explicitly seeks to avoid. To provide adequate protection to trade secrets, as the statute contemplates, such exemptions should apply broadly to both access and portability requests. Absent this clarification, this language should be struck.

III. Rule 5.04 (Default Settings for Universal Opt-Out Mechanisms)

The Proposed Regulations clearly contradict the statutory language of the CPA that states that the Rules for universal opt-out must not adopt a mechanism ("UOOM") that is *"a default setting*, but rather clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data…"[9] The Proposed Rules suggest that the consumer's purchase of a UOOM-enabled product would signify such a choice to use a UOOM.

---

[5] Per CRS § 6-1-1307(1)(b), controllers are not required to comply with an access request if "I(A) The Controller is not reasonably capable of associating the request with the personal data; OR (B) It would be unreasonably burdensome for the controller to associate the request with the personal data; (II) the controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; AND (III) The controller does not sell the personal data to any third party, except as otherwise authorized by the consumer…."

[6] Per CRS § 6-1-1307(1)(c), controllers are not required to "maintain data in identifiable form or collect, obtain, retain, or access any data or technology in order to enable the controller to associate an authenticated consumer request with personal data."

[7] CRS § 6-1-1307(3).

[8] Proposed Rule 4.04(D).

[9] CRS § 6-1-1313(1)(c) (emphasis added).

A consumer's mere use or purchase of a product or service alone does not constitute a clear choice for data processing purposes, and therefore should not constitute a clear choice for a UOOM. Consumers might adopt a particular browser for a variety of reasons not necessarily related to the marketed opt-out settings and thus not representative of an unambiguous choice. This provision should be struck altogether as it directly contradicts the statute's default settings prohibition.

IV. Rule 6.05 Loyalty Program Disclosures

The Revised Prosed Regulations state "a Controller maintaining a Bona Fide Loyalty Program must provide the following disclosures as required by 4 CCR 904-3, Rule 6.05(E), as well as in its privacy notice, *Bona Fide Loyalty Program terms*, and Consent disclosures in requests for Consent to Process Sensitive Data or Personal Data in connection with the Bona Fide Loyalty Program…"[10] Loyalty program disclosure should only be required to be included in the privacy policy and provide a link to the privacy policy in the loyalty terms and conditions.

Loyalty terms and conditions incorporate multi-jurisdictional non-privacy related legal requirements. Adding specific state privacy requirements would only make terms and conditions longer and harder to navigate for consumers. Having one single source of information for loyalty disclosures will be more manageable—updates to a business' privacy policy and loyalty terms and conditions are generally not conducted on the same schedule. Having a single source of truthful information for loyalty disclosures could prevent inadvertent inconsistencies between the privacy policy and terms and conditions as well as prevent notice fatigue.

The Proposed Rules would also require loyalty program disclosure to include "[t]he 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 the Consumer does not opt out of the Sale of Personal Data or Processing for Targeted Advertising…"[2]

It will be very difficult to quantify value to consumers in the way the Proposed Rules would require since so much of it would depend on the individual consumer and how much or how often they leverage a loyalty program. A consumer who patrons a business with greater frequency will likely accrue more benefits from any associated loyalty program and would therefore derive greater value from that program. Additionally, many businesses offer discounted prices to members of their loyalty programs, but the value that is ultimately derived depends on how often a loyalty member makes a purchase and takes advantage of that discounted offer.

[10] Proposed Rule 6.05(E) (emphasis added).
[2] Proposed Rule 6.05(E)(1)(c).

V. Rule 6.09 (Duty of Care)

The CPA establishes a Duty of Care on controllers to "take reasonable measure to secure personal data during both storage and use from unauthorized acquisition."[11] The Revised Proposed Regulations state that among other things "when determining reasonable and appropriate safeguards, Controllers should consider [a]pplicable industry standards and frameworks."[12] To encourage collaborative compliance, the OAG should include a safe harbor for when controllers reasonably conform to such industry standards and frameworks.[13]

VI. Rule 8.04 (Data Protection Assessment Content)

While the revised regulations have made helpful improvements to reduce the prescriptiveness of the requirements in the original Proposed Regulations for conducting data protection impact assessments, the requirements still exceed the standard set out in the statute pertaining to required content.[14] Multi-national companies likely already have a global DPIA as part of their GPA tool, including already making a few relatively minor updates to accommodate US state laws. The proposed DPIA language would likely require them to implement updates to their DPIA's, specifically for profiling in Colorado. Regulated entities should have more flexibility, which could be achieved by making this a guideline for what the DPIA could include depending on the sensitivity and nature of the processing as opposed to a mandate, which is the current language.

VII. Part 9 (Profiling)

a. Transparency

There is new language in Revised Proposed Regulation Section 9.03(A) that removes reference to profiling "used to serve ads," and by extension the implication that serving ads amounts to profiling "in furtherance of decisions that produce legal or similarly significant effects." This revision critically addresses potentially concerning language and provides important clarity regarding controllers' obligations with respect to the profiling opt-out.

---

[11] *Id*. At § 6-1-1308(5).

[12] Proposed Rule 6.09(B)(1).

[13] [13] The 2018 Ohio Data Protection Act (S.B. 220) is a notable model that the Chamber supports. Ohio enacted this innovative data security/cyber law in November 2018. S.B. 220 grants an affirmative defense against data breach tort claims to those businesses whose cybersecurity plans leverage an acceptable industry standard; other states' data protection laws focus on requirements or penalties.

https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220

[14] *See* CRS § 6-1-1309(3).

b. Opt-Out

Under Proposed Rule 9.04(B), companies would likely need to provide a new method for consumers to "opt out" of profiling. Colorado's Proposed Rule for profiling is broader than GDPR, extending to profiling that includes human reviewed automated processing. In contrast, GDPR includes the right not to be subject to solely automated decision-making.[15] It would be preferable for the opt-out right for profiling to be narrowed to only include solely automated processing. CPA does also not specify an opt-out right for human-reviewed decision-making.

c. Data Protection Assessment for Profiling

Data protection assessments for profiling activities should align with requirements in other jurisdictions/ interoperability of privacy frameworks rather than new state-specific requirements different from other assessments.

Thank you for the opportunity to comment. If you have any questions, please contact jcrenshaw@uschamber.com.

Sincerely,

Jordan Crenshaw
Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

[15] General Data Protection Regulation Art. 22 §1 (https://gdpr-info.eu/art-22-gdpr/)