February 3, 2023

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

Re: CPA Proposed Draft Regulations

The Computer & Communications Industry Association (CCIA)[1] is pleased to respond to the Colorado Department of Law's (the "Department") Notice of Proposed Rulemaking on the final draft regulations (the "Rules") governing the implementation of the Colorado Privacy Act ("CPA").

We commend the Department for its responsiveness to commenters in making the following changes, which significantly improve the rule text. However, we remain concerned about some language still in the proposed final Rules and further revisions are needed to clarify the scope of the obligation.

DEFINITIONS

A. Rule 2.02 – "Biometric Identifiers"

The revisions to "biometric identifiers" help clarify its scope but concerns remain about the definition's breadth. The Association strongly recommends the Department strike the term "biometric identifiers" and substitute the defined term "biometric data" for all relevant obligations. This revision would avoid creating a needlessly complex separate sub-definition and help align with emerging U.S. state comprehensive privacy laws. Alternatively, the Association would recommend the following amendments in **Attachment A** to the "biometric identifiers" definitions to clarify its scope.

The proposed Rules still contain references to identifiers that might be "intended to be used." Biometric data should be limited to identifiers that are actually used for the identification of specific persons rather than identification generally. It is unclear how the concerns with intended use will not be addressed by any subsequent, actual use.

B. Rule 2.02 – "Human Involved Automated Processing"

Operational challenges are still created by the definition of "Human Involved Automated Processing." CCIA urges this definition be deleted and if needed, modify "Solely Automated Processing" to note that it includes human review with no ability to change the outcome. It is unclear how an organization can prove the level of consideration a human actually gave an output to distinguish between human "involved" and "human reviewed" automated processing. The "Human Involved" term is unnecessary because if the human did not have a

[1] CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. For more information about CCIA please see: https://www.ccianet.org/about.

meaningful opportunity to consider, whether due to policies or other restrictions, then it would simply be "Solely Automated Processing."

CONSUMER PERSONAL DATA RIGHTS

A. Rule 4.04 – Right of Access

Rule 4.04(A) needs to be modified to avoid creating costly compliance challenges for organizations. Controllers must provide a consumer "without limitation" any personal data they obtained and "must include explanations that would allow the average consumer to make an informed decision" on whether to exercise their rights. CCIA proposes eliminating this requirement or limiting it to where the produced data is not reasonably self-explanatory.

The inclusion of "derivatives data" or "inferences" in Rule 4.04(A)(1) could result in businesses being forced to provide content beyond discrete personal data, raising significant confidentiality and intellectual property concerns. The Department should delete this provision to ensure businesses have the necessary flexibility to operationalize these requirements, otherwise, products and services may not be made available to Colorado citizens if it could result in the mandatory disclosure of proprietary information.

CCIA is concerned that the trade secrets language in Rule 4.04(E) still does not extend to access rights. Although the revisions attempt to resolve a tension in the CPA between portability and access rights, the revised provision will have the unfortunate effect of compromising industry trade secrets altogether – something the statute explicitly seeks to avoid. CCIA recommends the Department clarify that exemptions apply broadly to both access and portability requests – absent this clarification, we recommend striking this language.

B. Rule 4.09 – Responding to Consumer Reports

Rule 4.09(C) continues to create confusing compliance obligations for Controllers. It is unclear how Controllers are to respond when the Processor does not provide the "technical and organization" measures described in this provision. CCIA recommends the Department remove this provision to help alleviate the implementation concerns.

Universal Opt-Out Mechanism

A. Rule 5.04 – Default Settings for Universal Opt-Out Mechanisms

Despite the revisions to Rule 5.04(B), it still contradicts the CPA's direct guidance that the opt-out mechanism clearly represents the consumer's "affirmative, freely given, and unambiguous choice to opt-out." Consumers might adopt a particular browser for a variety of reasons, and organizations are unable to verify whether the choice of browser was due to the marketed opt-out settings or an entirely unrelated reason. CCIA recommends the Department remove this provision altogether as it directly conflicts with the CPA and could result in a significant number of erroneous opt-out signals.

DUTIES OF CONTROLLERS

A. Rule 6.05 – Loyalty Programs

Rule 6.05(A) prohibits a business from increasing costs or decreasing the availability of a product or service as a result of a consumer's decision to exercise a data right. CCIA suggests the Rules instead require that the price or service differential be reasonably related to the

value of the consumer's data. For example, ad-supported tiers of services are typical in the video streaming industry. If a consumer opts-out of targeted advertising, the business should be allowed to make up the revenue difference by charging more for the service.

B. Rule 6.09 – Duty of Care

The references to "administrative, technical, organizational, and physical safeguards" in Rule 6.09 should be removed. Although these seem like interchangeable terms, it departs from the statute's express language – "technical and organizational measures" – and other state privacy laws like the California Privacy Rights Act.

C. Rule 6.10 – Duty Regarding Sensitive Data

CCIA recommends the Department clarify the obligations in Rule 6.10(B)(3) to exclude situations where the data is transferred to an affiliate or a processor – and concerning the processor, at least where the processor is acting solely on behalf of a Controller and for no other purpose. Modifying Rule 6.10(B)(3) would avoid imposing overly burdensome requirements that provide no countervailing benefits to consumers.

CONSENT

A. Rule 7.03 – Requirements for Valid Consent

The overbreadth of the obligations in Rule 7.03 (E) imposes a significant burden on companies and confusion for consumers to the extent it would require detailed disclosures whenever a consumer chooses to opt-in. Consumers may toggle back and forth between opt-in/opt-out settings on a control page and additional disclosures that must appear whenever the consumer opts-in adds unnecessary friction not required under other state privacy laws. This burden is further compounded by Rule 7.04(C), to the extent that the consent disclosure cannot point back to the privacy notice. CCIA recommends the Department strike this requirement in its entirety or limit it to certain high-risk situations. However, if this provision remains, at a minimum, the Department should include a carve out for where a consumer opts-in after opting-out, such as for targeted advertising or profiling. A similar edit to Rule 7.05 would be required.

B. Rule 7.04 – Requests for Consent

Rules 7.03 and 7.04, when read together, risk imposing substantial friction and clutter for consumers looking to manage their data preference settings. Companies should retain discretion in designing a landing page where consumers may control the settings. To the extent a company must include the full range of disclosures for consent under Rule 7.03, CCIA recommends that it should be sufficient for an organization to rely on the disclosure in the privacy notice. Since the requirements under Rule 7.03 are so varied, the company cannot point to a single section of the privacy notice.

C. Rule 7.09 – User Interface Design, Choice Architecture, and Dark Patterns

The revised language in Rule 7.09(A)(4) is still incompatible with the text of the CPA. The CPA provides consumers with the right to opt-out, creating a default state – consumers are opted-out. CCIA recommends this requirement be deleted.

DATA PROTECTION ASSESSMENTS

A. Rule 8.02 – Scope

The reference to "heightened risk of harm" should refer to the CPA definition at § 6-1-1309.

PROFILING

A. Rule 9.03 – Profiling Opt-Out Transparency

The revised language continues to include overly strict obligations upon a business when assessing and addressing risks in connection with DPAs. CCIA urges the Department to modify the language in Rule 9.03 to replace the term "shall" and revert to "should" in describing this obligation. Other revisions to the Rules have reflected an understanding that the size and complexity of a business must be taken into account as part of operationalizing a requirement.

Despite the revisions to provisions concerning profiling, concerns remain over the scope of protections afforded in Rule 9.03(B). The Department should extend these protections beyond only trade secrets to include "proprietary information" and afford the same to DPAs as described in Rule 9.06(F).

B. Rule 9.06 – Data Protection Assessments for Profiling

The language in Rule 9.06(F) still warrants further revision. CCIA suggests removing the requirement for DPA elements to require third-party software provider reports. DPA elements should be tailored to risk, balancing consumer protection against hindering/impeding business activities, which can also pose harm to consumers. Lastly, CCIA suggests adding "where relevant to the risks" to the profiling DPA elements in Rule 9.06(G). This will require a company to provide information only to the extent that it is related to the specific risks that trigger the DPA.

* * * * *

CCIA and its members thank the Colorado Department of Law for the several opportunities to provide suggestions on how to balance the final regulations. The suggested alternative language discussed herein, which is also provided in **Attachment A** in redline form for ease of review, is offered as a means for achieving the best result for consumers, regulators, and the online ecosystem.

Respectfully submitted,

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association

ATTACHMENT A

Suggested Amendments to Revised Draft Rules

Rule 2.02 "Biometric Identifiers" means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics that are ~~can be~~ Processed for the purpose of uniquely identifying an individual, including but not limited to a fingerprint, a voiceprint, eye retinas, irises, facial mapping, facial geometry

Rule 6.05(A) ~~While a Controller may not increase the cost of or decrease the availability of a product or service based solely on a Consumer's exercise of a Data Right, a~~ A Controller is not prohibited from offering Bona Fide Loyalty Program Benefits to a Consumer based on the Consumer's voluntary participation in that Bona Fide Loyalty Program. However, the Bona Fide Loyalty Program Benefit must be reasonably related to the value provided to the Controller by the Consumer's Personal Data.

Rule 7.04(C) Any interface used by a Controller to request a Consumer's consent must contain the disclosures required by 4 CCR 904-3, Rule 7.03(E)(1). The request interface itself must contain the disclosures required by Rule 7.03(E)(1)(a)-(d) ~~and~~ or the Controller may provide the Consumer with a link to a webpage containing the Consent disclosures required by 4 CCR 904-3, Rule 7.03(e)-(g)~~, provided the request clearly states the title and heading of the webpage section containing the relevant disclosures~~. If technically feasible, the request method must also link the Consumer directly to the relevant section of the disclosure.

Rule 9.06(A)(3) If the Profiling is conducted by Third Party software purchased by the Controller, name of the software and sufficient information to inform evaluation of accuracy where relevant to the risks described in CPA Section 6-1-1309(2)(a)(I-IV) (for example, copies of any internal or external evaluations of the accuracy and reliability of the software).