November 7, 2024

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

Re: Colorado Privacy Act 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 would significantly improve the Rule text. However, we remain concerned about certain language still present in the proposed final rules and believe further revisions are needed to clarify the scope of these obligations. CCIA's suggested amendments to the draft Rules are set forth in **Attachment A**.

DEFINITIONS

Rule 2.02 – "Biometric Identifier"

CCIA recommends striking the term "Biometric Identifier" and substituting the defined term "Biometric Data" for all relevant obligations. Defining these terms separately creates needless complexity, and a unified definition would help align with other state comprehensive privacy laws. Alternatively, CCIA would recommend clarifying that neither "Biometric Data" nor "Biometric Identifiers" include digital or physical photographs or an audio or voice recording.

The proposed Rules still refer to identifiers "intended to be used." The definition of "Biometric Data" should be limited to identifiers that are *actually* used to identify specific persons rather than identification generally. It is unclear how the concerns with intended use would not be addressed by any subsequent, actual use.

Rule 2.02 – "Employee"

The proposed Rules define "Employee" to include workers specifically excluded from the definition of an employee under Colorado law, including independent contractors.[2] The Rules therefore risk unintentionally conferring obligations associated with employers and employees upon independent contractors and their clients. CCIA therefore recommends clarifying that an employer's actions taken in accordance with C.R.S. § 6-1-1314 shall not be used as evidence

[1] CCIA is an international, not-for-profit trade association representing small, medium, and large communications and digital services 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.

[2] *See, e.g.*, C.R.S. § 8-40-202(2) (excluding independent contractors from the definition of "employees").

of an employer-employee relationship or to assess any factor used in determining whether a person is an employee.

Rule 2.02 – "Minor"

CCIA recommends defining a "Minor" as an individual who is known to be under the age of 18, or alternatively, to replace all subsequent references to "Minors" with "known Minors." Throughout the Rules, provisions concerning children reference "a known Child," and treating minors similarly would improve the Rules' consistency. Moreover, the Rules' subsequent uses of the term "Minor" occur in contexts where a knowledge standard is most appropriate. Rule 3.02 uses the term in reference to a website's target audience, and therefore applies to situations where controllers have knowledge that minors will use the site. Likewise, Rules 7.02(A)(5)-(6) use the term in reference to a law that applies only to a "consumer whom the controller actually knows or willfully disregards is a minor."[3]

Furthermore, many companies do not collect enough information about individual users to know their age. As written, the Rules would therefore require companies to collect *more* data than they do now, which contradicts data minimization principles. By contrast, a "known Minor" standard allows companies to maintain beneficial data minimization practices.

BIOMETRIC IDENTIFIERS

Rule 6.12(C)(1) – Biometric Identifier Notice

CCIA agrees with the principle outlined in this Rule. However, the phrase "abstract and ambivalent terms" introduces unnecessary ambiguity. The Rules do not define "abstract" or "ambivalent," and any interpretation of this provision's scope will therefore be highly subjective, making the Rule difficult to enforce with any degree of consistency. CCIA therefore suggests changing this Rule to "Concrete, definitive, and specific."

Rule 6.12(C)(2) – Biometric Identifier Notice

CCIA recommends removing this provision, as it risks forcing data controllers to make their privacy policies less comprehensible. Organizations may delineate their data processing procedures based on the data's sensitivity, or any number of other factors, rather than the type of data collected. In such cases, the clearest method of presentation is to explain to consumers what data falls under each procedure. Formatting a privacy policy this way may require interspersing references to biometric data throughout several sections of the policy. Forcing data controllers to group references to biometric data risks creating the misleading impression that the data controller handles all biometric data in the same way, when this may not be the case. The clarity requirement in Rule 6.12(C)(1) sufficiently ensures that controllers adequately notify consumers regarding how their biometric data may be used.

Rule 6.12(D)(2) – Biometric Identifier Notice

CCIA appreciates the need for accessible privacy notices. However, to maximize accessibility, some privacy notices are best presented through forms other than text, such as through images, audio, or a combination thereof. To allow data controllers greater leeway to present

[3] C.R.S. § 6-1-1308.5(2).

privacy policies in the manner most accessible to their consumer base, CCIA recommends removing the final sentence from Rule 6.12(D)(2) ("If the link directs to a privacy notice, it must point the Consumer to the specific section of the privacy notice that includes the Biometric Identifier Notice"), which is not well suited to privacy policies containing audio and/or visual components.

REQUIRED CONSENT AND EMPLOYEE CONSENT

Rules 7.02(A)(5)-(6) – Required Consent

CCIA recommends referring to a "known Minor" rather than a "Minor." As discussed in CCIA's comments on the definition of "Minor" under Rule 2.02 above, these Rules institute consent requirements for activities listed in C.R.S. § 6-1-1308.5(2). However, § 6-1-1308.5(2) applies only to a "consumer whom the controller actually knows or willfully disregards is a minor."[4] It makes little sense for these Rules to impose consent requirements for a class of persons specifically excluded from § 6-1-1308.5(2)'s protections.

Rule 7.09(C) – Employee Consent to Collect and Process Biometric Identifiers

CCIA is concerned that requiring employers to obtain new consent forms from their employees in every circumstance contemplated under Rule 7.08 will be too burdensome, particularly for small businesses. CCIA instead recommends adding a caveat to Rule 7.09(C) (or alternatively to Rule 7.08) allowing employers to rely on consent obtained from a new hire or existing employee, and only required to obtain renewed consent if the controller expects to collect or use data differently than previously identified. This addition would grant employees the same consent rights as the current rule, but would eliminate much of the unnecessary paperwork for employers, thus avoiding a disincentive for businesses to grow their workforces.

DATA PROTECTION ASSESSMENTS

Rule 8.04(A)(2) – Data Protection Assessment Content

Currently, the Rules provide differing knowledge standards for different data subjects, referring to "known Children" while foregoing any knowledge standard in the definition of "Minors." As discussed previously, CCIA recommends replacing "Minors" with "known Minors." Requiring controllers to summarize their processing of data from minors unknown to the controllers is not feasible.

Rule 8.04(A)(6) – Data Protection Assessment Content

Given the Ninth Circuit's recent holding in *NetChoice LLC v. Bonta*,[5] it is likely unconstitutional to require DPIAs to include reporting on any heightened risk of harm that is reasonably foreseeable from the offering of a particular service to minors. Such a requirement, in the court's words, "clearly compels speech by requiring covered businesses to opine on potential

[4] *Id.*
[5] 113 F. 4th 1101 (9th Cir. 2024).

harm to children."[6] Moreover, the DPIA requirement is not likely to withstand First Amendment scrutiny because it is not the least restrictive means of protecting minors from harmful content: the court further held that "a disclosure regime that requires the forced creation and disclosure of highly subjective opinions about content-related harms to children is unnecessary for fostering a proactive environment in which companies, the State, and the general public work to protect children's safety online."[7] CCIA therefore opposes the proposed modification to this Rule.

INTERPRETIVE GUIDANCE AND OPINION LETTERS

Part 10 should outline a process that encourages companies to seek advisory opinions. However, the proposed Rules impose unnecessary hurdles and risks that will likely discourage requests. To make this process more user friendly, the framework should support speedy opinions that minimize the risk to the company of making a request. To achieve these ends, the rules should:

- Limit the requirements for submitted material to what is necessary for an opinion. The Rules should minimize what is mandatory in an initial submission, with an option for the Attorney General to request additional details. See CCIA's comments on Rule 10.03(E).

- Set clear deadlines for when the Attorney General will issue an opinion (e.g. 60 days). This deadline should be the shortest time feasible (note that the Texas Attorney General's settlement with Meta was provided within a 30-day window). Businesses should not need to wait in limbo for an opinion any longer than necessary.

- Allow companies to withdraw requests due to changes in their circumstances.

- Specify protections for any materials submitted as part of a request, such as protection against public disclosure and a safe harbor that prevents the Attorney General from using the submitted materials to bring any action against the requesting company.

- Separately, the rules should include a disclaimer that the Attorney General shall not use a company's failure to seek an advisory opinion against the company in any enforcement action.

Rule 10.02(A) – Scope and Effect of Opinion Letters

This Rule currently refers to requests made pursuant to "Rule 10.04." However, Rule 10.04 specifies guidance on *issuing* opinion letters. The Rule governing *requests* for such letters is Rule 10.03. CCIA recommends correcting this citation.

Rule 10.02(C) – Scope and Effect of Opinion Letters

The factors listed in this rule would all seem to weigh *against* issuing an opinion letter to avoid interference with any proceeding before the secretary or court in question. CCIA instead

[6] *Id.* at 1117.
[7] *Id.* at 1122.

recommends that the Attorney General consider the following factors instead: (1) Whether the matter involves a substantial or novel question of fact or law with no clear agency or court precedent, and (2) whether the subject matter of the request and consequent publication of advice is of significant public interest.

Rule 10.02(E) – Scope and Effect of Opinion Letters

CCIA recognizes that each opinion letter will apply to a fact-specific set of circumstances, and that the Colorado Privacy Act will apply to each company's proposed action in a unique manner. Nevertheless, while businesses should not rely on fact-specific determinations in opinions issued to other parties, they should be allowed to rely on any broadly applicable principles contained in such letters. Such reliance would help reduce noncompliance among businesses.

Rule 10.02(G) – Scope and Effect of Opinion Letters

As noted in the general comments on Rule 10, the Rules should protect all materials submitted to the Attorney General in a letter request from public disclosure, and from being used by the Attorney General to bring an action against the requesting company. These protections should hold regardless of whether the Attorney General issues a response, or what type of response is issued.

Rule 10.03(A) – Requests for Opinion Letters

Since CPA regulations took effect only in 2023, companies may have well-founded questions about their existing processing activities. This Rule should permit Companies to use the advisory opinion process for questions about their pre-existing activities for 2-3 years following the law's effective date.

Rule 10.03(E)(3) – Requests for Opinion Letters

CCIA understands that the letters in question are intended as guidance on fact-specific applications of the CPA, and that such guidance cannot be given without all the available facts. CCIA therefore supports the requirement that requests for such letters contain complete and specific descriptions of all information relevant to the request. However, the requirements in several subsections of this Rule discourage companies from seeking advisory opinions, as they may have to provide sensitive information when making the request. Moreover, these requirements can be significantly reduced while still providing the Attorney General with all information necessary to make a decision. Rather than require production of the information listed in subsections (a) through (f), the Attorney General should be able to request information from the following categories as necessary to issue an opinion:

- Specific parties that access the relevant data, when such access poses a high risk (such as data brokers). In all other cases, it should be sufficient to request categories of parties who would have access to the data rather than specific parties.

- Descriptions of disclosures that will be provided to consumers or data protection assessments that have been conducted. Companies should not be required to provide

the finished disclosures and assessments, as they may wish to use information in the advisory opinion to help craft them.

- Trade secrets or confidential information, provided that the Rules expressly assure that such information will not be disclosed.

These modifications will better assure requesters that seeking a letter will not compromise their sensitive information.

Rules 10.05(B)-(C) – Scope and Effect of Interpretive Guidance

While CCIA understands the rationale behind not making the Attorney General's advisory opinions binding, companies should be allowed to use these opinions as persuasive authority should an action be brought against them in which CPA compliance is at issue. The advisory opinions' purpose is to incentivize compliance with the CPA. Prohibiting companies from using these opinions as persuasive authority in enforcement actions undoes much of the Rule's purpose: offering companies guidance as to their legal standing under the CPA. Allowing companies to use the opinions as persuasive authority rewards those companies who have been diligent in ensuring their compliance, while still avoiding the infringements upon the powers of courts and agencies that would result from making the advisory opinions mandatory authority.

* * * * *

We appreciate your consideration of these comments. We look forward to continuing to participate in the Department's ongoing regulatory process, including reviewing and providing feedback on the series of proposed rules. We hope the Department will consider CCIA a resource as these discussions progress.

Sincerely,

Jesse Lieberfeld
Policy Counsel– Privacy, Security, and Emerging Technologies
Computer & Communications Industry Association

ATTACHMENT A

Suggested Amendments to Revised Draft Rules

This Attachment contains CCIA's suggestions for specific modifications to the Revised Draft Rules. The text below is the draft Rules text after the Department of Law's revisions. CCIA's proposed deletions are in red and proposed new language is in green.

***2.02* – "Biometric Identifiers": CCIA recommends striking this definition and changing all references to "biometric identifiers" to "biometric data, or alternatively, modifying the rule as follows:**

***2.02* – "Biometric Identifiers"** is defined as set forth in C.R.S. § 6-1-1303(2.4), and means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual. Biometric Identifier includes, including but not limited to a fingerprint; a voiceprint; a scan or records of eye retinas or irises; a facial mapping, facial geometry, or facial templates; or other unique biological, physical, or behavioral patterns or characteristics. "Biometric Identifiers" do not include the following: (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.

***2.02* – "Employee"** as used in C.R.S. § 6-1-1314 is set forth in C.R.S. § 6-1-1314(1)(b) and means an individual who is employed full-time, part-time, or on-call or who is hired as a contractor, subcontractor, intern, or fellow. No action taken by an employer in accordance with C.R.S. § 6-1-1314 shall be used as evidence of an employer-employee relationship or to assess any factor used in determining whether a person is an employee.

***2.02* – "Minor"** is defined as set forth in C.R.S. § 6-1-1303(16.5) and means any consumer who is known to be under eighteen years of age.

6.12(C) – A Biometric Identifier Notice must be clear. Information contained in such notice shall be concrete, definitive, and specific.~~:~~

> ~~**1.** Concrete, and definitive, avoiding abstract or ambivalent terms that may lead to varying interpretations.~~
>
> ~~**2.** If included in a privacy notice, clearly labeled, such that Consumers seeking to understand a Controller's collection and use of Biometric Identifiers can easily access the section of the privacy notice containing relevant information.~~

6.12(D)– A Biometric Identifier Notice must be reasonably accessible. Such notice may be:

> **1.** A separate notice made available in its entirety prior to the collection or Processing of Biometric Identifiers; or

2. Linked to from the homepage of a website or on a mobile application's app store page or download page. If using a link, the link must be conspicuous and must clearly indicate it relates to Biometric Identifiers in the link text. A Controller that maintains an application on a mobile or other device shall also include a link to the Biometric Identifier Notice in the application's settings menu. ~~If the link directs to a privacy notice, it must point the Consumer to the specific section of the privacy notice that includes the Biometric Identifier Notice.~~

7.02(A)– Pursuant to C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7), and 6-1-1308.5, and 6-1-1314(4) a Controller must obtain valid Consumer Consent prior to:

...

5. Processing the Personal Data of a known Minor as contemplated in C.R.S. § 6-1-1308.5(2)

6. Using any system design feature to significantly increase, sustain, or extend a known Minor's use of an online service, product, or feature, as contemplated in C.R.S. § 6-1-1308.5(2);

7.09(C) – Consent required by an Employer to collect or process an Employee's or prospective Employee's Biometric ~~Identifier~~ Data shall be consistent with the requirements for Consent provided in 4 CCR 904-3, Rules 7.03-7.08. Once an Employer has obtained Consent to collect or process an Employee's or prospective Employee's Biometric Data in a manner consistent with the requirements for Consent provided in 4 CCR 904-3, Rules 7.03-7.08, such consent shall satisfy the Employer's requirement to refresh consent provided in 4 CCR 904-3, Rule 7.08(A) until such time as the Employer reasonably expects to use or collect data in a manner not previously identified when the Employee or prospective Employee last gave Consent.

8.04(A) – At a minimum, a data protection assessment must include the following information:

1. A short summary of the Processing activity;

2. The categories of Personal Data to be Processed and whether they include Personal Data from a known Minor as described in C.R.S. § 6-1-1303(16.5); or Sensitive Data, including Personal Data from a known Child as described in C.R.S. § 6-1-1303(24);

...

6. The sources and nature of risks to the rights of Consumers associated with the Processing activity posed by the Processing activity~~, including the sources and nature of any heightened risk of harm to Minors that is a reasonable foreseeable result of offering an online service, product, or feature to Minors~~. The source and nature of the risks may differ based on the processing activity and type of Personal Data processed. Risks to the rights of Consumers that a Controller may consider in a data protection assessment include, for example, risks of:

...

10.02(A) – Opinion Letters are only issued in response to requests made pursuant to 4 CCR 904-3, Rule 10.034.

...

***10.02(C)* –** The Attorney General shall determine, at the Attorney General's discretion, whether to issue an Opinion Letter. In making this determination, the Attorney General may consider factors including, without limitation, whether:

1. ~~The Opinion Letter will terminate a controversy or remove one or more uncertainties as to the application of the law to the requestor's situation;~~ Whether the matter involves a substantial or novel question of fact or law with no clear agency or court precedent; and
2. ~~The request involves a subject, question, or issue that concerns a formal or informal matter or investigation currently pending before the secretary or a court; and~~ Whether the subject matter of the request and consequent publication of advice is of significant public interest.
3. ~~The request seeks a ruling on a moot or hypothetical question.~~

...

Within 60 days of receiving a request for an opinion letter, the Attorney General shall either (1) issue an opinion letter, (2) notify the requesting party that an opinion letter will not be issued, or (3) notify the requesting party of any further information necessary to reach a decision.

***10.02(E)* –** A~~n~~ fact-specific determination in an Opinion Letter may not form the basis of a good faith reliance defense for persons or entities who were not the subject of that Opinion Letter as described in the Opinion Letter request. However, persons or entities who are not the subject of an Opinion Letter may use statements regarding established principles under the Colorado Privacy Act as persuasive authority when making a good faith reliance defense.

***10.02(G)* –** The Attorney General may decline any request to issue an Opinion Letter. The Attorney General may, when it is deemed appropriate, issue Interpretive Guidance calling attention to established principles under the Colorado Privacy Act, even when a request that was submitted was for an Opinion Letter. Regardless of whether the Attorney General issues an Opinion Letter, Interpretive Guidance, or no response, the Attorney General shall not publicly disclose any materials submitted in the course of a request made pursuant to 4 CCR 904-3, Rule 10.04, nor use any such material in bringing any action against the requesting person or entity. A person or entity's failure to seek an Opinion Letter or Interpretive Guidance shall not be held against that person or entity in any enforcement action. A person or entity requesting an Opinion Letter or Interpretive Guidance if the Opinion Letter or Interpretive Guidance has not yet been issued.

***10.03(A)* –** A request for an Opinion Letter must be prospective in nature, pertaining to an activity that the requestor in good faith specifically plans to undertake, or pertain to an existing practice that the requesting party has already undertaken, if the request for an Opinion Letter is submitted within three years after the effective date of 4 CCR 904-3. The plans may be contingent upon receiving a favorable Opinion Letter.

***10.03(E)* –** Each request for an Opinion Letter must be fact-specific and narrowly framed to the specific activity in question, and must set forth the facts underlying the request in as much detail as possible, including without limitation:

...

3. A complete and specific description containing all relevant information bearing on the activity for which an Opinion Letter is requested. ~~, including without limitation~~ Upon reviewing this information, the Attorney General may then request further information as necessary from the following categories:

~~**a.** A complete and specific description of the activity, transaction or agreement that the requestor plans to undertake, or any Personal Data Processing that that will result from the activity, agreement or transaction that the requestor plans to pursue.~~

~~**b.** A description of the personal data involved, including whether the personal data is sensitive personal data, and the category of sensitive data.~~

c. A description ~~of~~ classifying each of the categories of parties that would have access to the Personal Data involved, and/or a description of each of the parties that would have access to any sensitive data involved.

d. A description ~~and draft~~ of any disclosures relating the Personal Data involved that will be provided to consumers, and a description of the location and form in which the disclosure will be provided.

e. A ~~copy~~ description of any data protection assessment conducted in anticipation of the contemplated Processing activity, if required by C.R.S. § 6-1-1309; and

f. If applicable, a designation of trade secrets or confidential commercial or financial information. The Attorney General shall not publicly disclose information received pursuant to this provision.

***10.05(B)* –** Interpretive Guidance issued by the Attorney General is informational only and is not binding on the Attorney General or Colorado Department of Law with respect to any particular factual situation. However, a requesting party may use Interpretive Guidance issued by the Attorney General as persuasive authority in any related action brought against the requesting party by the Attorney General or the Colorado Department of Law under the Colorado Privacy Act.

***10.05(C)* –** Interpretive Guidance issued pursuant to this section is for informational purposes only, and may not serve as ~~the basis for~~ mandatory authority in a good faith reliance defense. However, a requesting party may use Interpretive Guidance issued by the Attorney General as persuasive authority in a good faith reliance defense.