January 17, 2023

The Honorable Philip J. Weiser
Attorney General
Colorado Department of Law
Ralph L. Carr Judicial Building
1300 Broadway, 10th Floor
Denver, CO 80203
(720) 508-6000

RE: Comments on the 2nd Draft of Colorado Privacy Act Rules 4 CCR-904-3

Dear General Weiser:

On behalf of the Software and Information Industry Association (SIIA), we write in response to your offices' request for input with regard to the second draft of rules[1] supporting the Colorado Privacy Act (CPA).

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies and associations reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide and companies specializing in data analytics and information services.

SIIA supports privacy as a fundamental value, one essential to individual autonomy and a functioning democracy. We believe that a state data privacy standard that harmonizes meaningful consumer safeguards with appropriate business compliance will ensure smooth implementation of uniform data privacy practices.

We write to propose several modifications that would make the second draft of the regulations stronger. Our revisions are in **green, bolded text**, to distinguish our revisions from that of the Colorado AG's office, whose revisions are noted in red. In sum, our comments address the following issues.

1. The regulations should treat Publicly Available Information (PAI) that has been "inextricably combined" with personal data as PAI (2.02).

[1] Colorado AG's Office. 2nd Draft of Rules on Colorado Privacy Act. Posted to CPA website. Dec 21, 2022.

2. The regulations should revise or remove the term "Sensitive Data Inferences" to align with the CPA and avoid contradictory guidance (2.02).

3. The regulations should refine the duty regarding sensitive data to ensure consent requirements are in line with the CPA (6.10).

4. The regulations should further sharpen the definition of biometric data, focusing on data used to identify a specific individual (2.02).

5. The regulations should streamline individual rights obligations (4.04, 4.05, 4.07) to ensure workable standards for compliance and align the requirements with other state laws.

6. The regulations should remove conflicting requirements for what constitutes a Universal Opt-Out Mechanism signal (5.04) and clarify that controllers can request additional consumer information to inform the Opt-Out Mechanism signal (5.05B).

7. The regulations should limit opting out of profiling "in furtherance of decisions that have legal or similarly significant effects" to Solely Automated Processing (9.04).

8. The regulations should clarify the exemptions for controllers and processors to use data for internal research and related operations and services (6.06 and 6.07).

Detailed Explanation of Proposed Modifications:

1. **The regulations should treat Publicly Available Information (PAI) that has been "inextricably combined" with personal data as PAI (2.02).**

As noted in our previous submission, we were pleased to see the definition of personal data exclude publicly available information (PAI).[2] That definition encompasses both information that is lawfully obtained from government records as well as "any other information that the controller has a reasonable basis to believe the consumer made available to the public." *Id.*

We also welcome the revisions in the second draft of the regulations that delete "inferences made exclusively from multiple independent sources of PAI", so that it is no longer considered personal data (thus, it is considered PAI). Rather than categorize these inferences as an exclusion to PAI, we agree with the AG's office that this data is subject to the First Amendment and is fundamentally PAI. Yet, further refinements are needed in Section 2.02 of the regulations (addressed next) to ensure the regulations comport with the First Amendment and do not undermine socially productive uses of PAI.[3]

[2] Section 6-1-1303(17)(b) of the CPA excludes PAI from the definition of personal data.

[3] The Colorado Department of Law asks the following in the Draft Regulations about Publicly Available Information: *"The Department has provided clarity regarding information that is not included in the*

The draft regulations still diverge from statute by excluding "PAI that has been inextricably combined with non-publicly available Personal Data". This overly broad approach would create additional compliance obligations for companies, undermine the interstate interoperability of consumer privacy laws, and violate the First Amendment. The phrase is not referenced in the statute, and thus diverges from the CPA's intent to exclude all forms of PAI from the sweep of the CPA. We recommend striking this phrase.

The second draft of the proposed regulations seeks to exclude "PAI that has been inextricably combined with non-publicly available Personal Data," from the definition of PAI. The fact that PAI has been commingled – whether inextricably or not with other data – does not negate its status as PAI.

We appreciate that the AG's office decided to remove the reference to "inferences derived from multiple independent sources of publicly available data" from the exclusions to PAI. But, because one of the other exceptions to PAI still captures personal data (in instances when the personal data is inextricably combined with PAI), there is a possibility that these inferences from multiple sources of PAI, as well as other forms of PAI, would be covered – even though, consistent with the CPA, they should be considered PAI.

The treatment of "inextricably" combined data as personal data could result in unintended consequences. Today, virtually all government agencies use combined data sets and third party vendors to offer mobile apps and platforms to run their services, assist with data analytics, conduct security audits, and much more.

Government agencies and their vendors inevitably work with a combination of personal and publicly available data that may be considered "inextricably combined." In this case, the term "inextricably combined" does not provide clarity for how government agencies – and, importantly, the vendors whom they depend on to provide everyday services to consumers – should treat this data. If the PAI exclusion remains, consumers (including bad actors) may very well be able to potentially change, modify, or correct any publicly available data held by a state agency which, in turn, could impact an untold number of government services including fraud prevention, eligibility reviews, and other everyday constituent services. This is especially true because there is no quantifiable method to assess whether the data is "inextricably combined" or the circumstances that qualify as not "inextricably combined."

Subjecting the "inextricably" combined data to the CPA could also undermine the use of high-quality decision and analytics tools and weaken a business's ability to equip consumers with high-quality results. Public-private data collaborations and partnerships have created an

---

proposed definition of "Publicly Available Information." Of note, Personal Data obtained or processed in violation of C.R.S. §§ 18-7-107 and 18-7-801 have been excluded from the definition of "Publicly Available Information." Are there any other laws that should be included? Are there additional exclusions beyond these laws the Department should include?"

estimated $3 trillion in economic value as of 2020, and this is only likely to increase over time.[4] Open data and government participation has a critical role to play. These principles are being reinforced by the OECD[5], in its Declaration on Government Access to Personal Data Held by Private Sector Entities, which "seeks to improve trust in cross-border data flows,... by clarifying how national security and law enforcement agencies can access personal data under existing legal frameworks." This milestone initiative has been further reinforced by the White House, which recently published its fifth U.S. Open Government National Action Plan[6]. The plan will focus on increasing government transparency and protection of data, improving outcomes, and combating bias and inequality, while simultaneously improving access to government data by the public sector.

Therefore, we recommend revising proposed Rule 2.02 in the following way:

4 CCR-904-3
PART 2 DEFINITIONS
Rule 2.02 DEFINED TERMS

''Publicly Available Information'' as referred to in C.R.S. § 6-1-1303(17) does not include:
1. Any Personal Data obtained or processed in violation of C.R.S. §§ 18-7-107 or 18-7-801.
~~2. Inferences made exclusively from multiple independent sources of publicly available information~~;
2.~~3.~~ Biometric Data;
3.~~4.~~ Genetic Information;
~~**4. Publicly Available Information that has been inextricably combined with non-publicly available Personal Data; or**~~
4. ~~**5.**~~**6.** Nonconsensual Intimate Images known to the Controller

2. **The draft regulations should revise or remove the term "Sensitive Data Inferences" to align with the CPA (2.02).**

As noted in our previous comments, the second draft of the proposed regulations still includes a standalone term and definition for "Sensitive Data Inferences." This term is not present in the CPA and the proposed use of this term goes beyond the text and intent of the

[4] https://www.mckinsey.com/capabilities/quantumblack/our-insights/collaborating-for-the-common-good; https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information
[5]
[6] Open Government Action Plan. https://open.usa.gov/Fifth%20U.S.%20Open%20Govern

CPA[7]. No other state consumer privacy law uses this term and there is no current precedent for how such a term would be interpreted and applied.

First, the regulations describe "Sensitive Data Inferences" as an extension of information "revealing" sensitive data, which is not referenced in the statute. It is problematic because the term presumes that "inferences" derived from personal data should be regulated the same as the underlying data, sweeping in a host of indirectly correlated data and social determinants that in itself may not be sensitive, or otherwise subject to the scope of the CPA. When read against the definition of PAI, this term will lead to contradictions that will render the regulations unworkable for consumers and businesses.

Second, the definition will cover a range of "inferences," based on data that are also in the public domain, which creates further complications as previously discussed in recommendation 1. For example, the Colorado Division of Insurance (DOI) has undertaken a stakeholder process as part of CO SB 21-169, which seeks to identify and prohibit unintended bias in all lines of insurance.[8] As the DOI evaluates life insurance underwriting practices, the DOI is considering a requirement to use inferences based on race and ethnicity data to determine whether the process leads to unintended bias for applicants. The life insurance carriers themselves do not collect race and ethnicity information. Thus, the DOI has tentatively proposed statistical techniques such as the Bayesian Improved First Name Surname Geocoding to be used to derive race and ethnicity data as a component of the anti-bias testing process.

Third, the new term is without precedent in global privacy regulations or practices, or existing state privacy laws. This will undermine the CPA's objective to establish a framework that is interoperable with other state consumer privacy laws. This misalignment will further complicate business compliance. Well-established privacy regimes like the General Data Protection Regulation (GDPR) are silent on the treatment of sensitive inferences (including exemptions in GDPR Article 9[9]) and do not explicitly sweep in the use of inferences or the respective algorithms, decisions and tools that depend on inferences (as long as it is outside the scope of GDPR Article 22(3)[10]). U.S. law already protects individuals and consumers against discriminatory practices with respect to consumer data and any analysis conducted from that data (such as in guidance supporting best practices of the Equal Employment Opportunity Commission (EEOC)).[11]

---

[7] C.R.S. § 6-1-1308 (Added by 2021 Ch. 483,§1, eff. 7/1/2023.) (7) Duty regarding sensitive data. A controller shall not process a consumer's sensitive data without first obtaining the consumer's consent or, in the case of the processing of personal data concerning a known child, without first obtaining consent from the child's parent or lawful guardian.

[8] https://doi.colorado.gov/for-consumers/sb21-169-protecting-consumers-from-unfair-discrimination-in-insurance-practices

[9] GDPR. https://gdpr-info.eu/art-9-gdpr/

[10] GDPR. https://gdpr-info.eu/art-22-gdpr/

[11] FTC. Protections Against Discriminations and Other Prohibited Practices; EEOC. Privacy.

State privacy laws in Connecticut, Utah, and Virginia include a definition for sensitive data,[12] but none of these laws uses the phrase sensitive data inferences. Sensitive data in these laws is assumed to reflect the actual data points (e.g., mental health status) and not data derived from or closely correlated with that data (e.g., access to a health facility that could potentially identify one's health status). These laws do not reference or directly regulate sensitive data inferences, likely due in part, to the constitutional hurdles with doing so.

Finally, the CPA is the only state consumer privacy law to apply to nonprofits. The new definition of sensitive data inferences would impose severe restrictions on accessing data for commercial research and development – some of which is conducted in public-private partnership with nonprofits and think tanks – and the data's use for other socially beneficial purposes, including political campaigns research, efforts to find missing children, anti-money laundering efforts, and more. Once the regulations delete the term "sensitive data inferences," they will better comport with the First Amendment and ensure the free flow of data to support a democratized, digital economy.

To appropriately address the issue, we recommend the following changes:

4 CCR-904-3
PART 2 DEFINITIONS
Rule 2.02 DEFINED TERMS

"Revealing**"** as referred to in C.R.S. § 6-1-1303(24)(a) ~~**includes Sensitive Data Inferences.**~~ For example:

1. While geolocation information at a high level may not be considered Sensitive Data, geolocation data which shows an individual visited a mosque and is used to indicate that individual's religious beliefs is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a). Similarly, geolocation data which shows an individual visited a reproductive health clinic and is used to indicate an individual's health condition or sex life is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

2. While web browsing data at a high level may not be considered Sensitive Data, web browsing data which, alone or in combination with other Personal Data, creates a profile that indicates an individual's sexual orientation and is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

~~**"Sensitive Data Inference" or "Sensitive Data Inferences" means 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.**~~

[12] Consumer Data Protection Act. Virginia Code Ann. §59.1-571.; Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 et seq. (2022); 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) (WEST) (Effective July 1, 2023)

3. **The draft regulations should refine the duty regarding sensitive data - to ensure consent requirements are in line with CPA statute (6.10).**

In addition, the draft regulations' treatment of "sensitive data" is likely to create significant confusion for businesses and consumers alike because of the novel approach to consent required for this type of data. Unlike other state laws that require one-time opt-in consent for the processing of sensitive data, the draft regulations would require "refreshed consent" annually for processing this category of data. They would also require consent to be gathered "at regular intervals" for all other data. It is evident that there will be significant consent fatigue from such strenuous consent requirements, and it will hamper business compliance and opportunities to bring new products to market, which may use inferential data and data analytics for processing.

We recommend making the following changes:

Rule 6.10 DUTY REGARDING SENSITIVE DATA

A. Controllers must obtain Consent to Process Sensitive Data, ~~**including Sensitive Data Inferences,**~~ consistent with C.R.S. § 6-1-1308(7) and 4 CCR 904-3, Rules 7.02-7.05.

~~**B. Controllers may Process Sensitive Data Inferences from Consumers over the age of thirteen (13) without Consent only if:**~~

~~**1. The Processing purpose of such Personal Data would be obvious to a reasonable Consumer based on the context of the collection and use of the Personal Data, and the relationship between the Controller and Consumer.;**~~

~~**2. The Personal Data and any Sensitive Data Inferences are permanently deleted within twelve (12) twenty four (24) hours of collection or of the completion of the Processing activity, whichever comes first;**~~

~~**3. The Personal Data and any 3.Sensitive Data Inferences are not transferred, sold, or shared with any Processors, Affiliates, or Third-Parties; and**~~

~~**4. The Personal Data and any Sensitive Data Inferences are not Processed for any purpose other than the express purpose disclosed to the Consumer.**~~

~~**C. If a Controller will delete Sensitive Data Inferences within twelve (12) twenty four (24) hours, pursuant to this section, they must (1) include description of the Sensitive Data Inferences subject to this provision and the retention and deletion timeline for such Sensitive Data Inferences in its privacy notice, pursuant to 4 CCR 904-3, Rule 6.03, and (2) include the details of the deletion and verification process in the Controller's Data Protection Assessment, pursuant to 4 CCR 904-3, Rule 8.04.**~~

4. **The draft regulations should clarify the definition of biometric data to avoid confusion and duplication in the regulation of this form of sensitive data (2.02).**

We appreciate changes made in the new draft of the regulations to clarify the definition of "Biometric Identifier" as information "for the purpose of uniquely identifying an individual." But, we strongly recommend this scoping principle be applied to the term "Biometric Data". We recommend eliminating the term "Biometric Identifier".

The regulations define "Biometric Data" as an extension of "Biometric Identifiers," which could lead to conflicting interpretations of the statute and unnecessary overbreadth. We believe that there is no reason to include two separate terms to explain biometric information; one term will suffice and reduce confusion for compliance and routine practice – similar to other state laws that follow this practice.

As we noted previously, we recommend the rules more precisely define biometric data to avoid overreach in the implementation of the law. The proposed definition goes beyond the way in which "biometric data" is typically understood to refer to specific, immutable physical characteristics – such as fingerprints, retinas, DNA, and facial features – that are used for identification purposes. Regulating data reflecting behavioral characteristics is problematic both for companies and consumers because such characteristics are not immutable–they are not fixed and can be changed– and have limited value for identification and authentication purposes. Behavioral patterns based on these sorts of characteristics are considered "soft biometrics," which cannot be depended upon, with high accuracy, to identify a person or enable verification of identity.[13] Thus, technologies using biometric information in this manner present a very different risk profile.

One unintended consequence from the overbroad definition of biometric data and inclusion of the term biometric identifier is the additional consent required for each of these use cases, which is likely to result in consent fatigue. Importantly, the impact of obtaining additional consent would flow to the companies' product development and design as well as the usability of the product for consumers, without a meaningful privacy benefit to doing so. Furthermore, the overly broad approach could unintentionally capture data, such as certain photographs or videos, not used for identification purposes.

Other state consumer privacy laws, including VCDPA and Connecticut, have defined Biometric Data[14,15] as a distinct term that includes specific, immutable characteristics used to

---

[13] See, e.g., Abdelgader Abdelwhab and Serestina Viriri, A Survey on Soft Biometrics for Human Identification, in Machine Learning and Biometrics, Jucheng Yang et al., eds. (London: IntechOpen, 2018); U. Park and A. K. Jain, Face Matching and Retrieval Using Soft Biometrics, IEEE Transactions on Information Forensics and Security, v.5, issue 3, at 406-15 (Sept. 2010); A. Dantcheva, What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics, 11 IEEE Transactions on Information Forensics and Security, v.11, issue 3, at 441-67 (Mar. 2016).

[14] VCDPA defines biometric data as: "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." VCDPA further states that biometric data does not include: "physical or digital photographs, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

[15] Connecticut's Act Concerning Personal Data Privacy and Online Monitoring defines biometric data as "data generated by automatic measurements of an individual's biological characteristics, such as a

identify the unique traits of an individual – without including the term "biometric identifier" as a part of the definition. This approach also accords with definitions that are used by the Department of Homeland Security (DHS) and NIST. DHS, for example, describes biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition."[16] NIST offers several definitions, each referring to physical and/or behavioral characteristics, rather than derivations from these characteristics.[17] Federal law and regulation use definitions that are generally aligned with these.[18]

We recommend deletion of the definition of "biometric identifier". By refocusing the definition of biometric data, the Colorado Privacy Act will better align compliance with other state laws while protecting consumers from real risks of privacy harm. We also recommend narrowing the definition of biometric data to encompass strictly automatic measurements of immutable biological characteristics used for identification purposes.

Our suggested definition for "Biometric Data" reads as follows:

> **"Biometric Data"** as referred to in C.R.S. § 6-1-1303(24)(b) means **data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics for the purpose of uniquely identifying an individual** ~~**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

fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual." Conn. Public Act No. 22-15, Section 1. (3) (2022).

[16] *See* Dept. of Homeland Security, Biometrics.

[17] *See* NIST Computer Security Resource Center, Biometrics.

[18] *See* 5 CFR 850.103 ("Biometrics means the technology that converts a unique characteristic of an individual into a digital form, which is then interpreted by a computer and compared with a digital exemplar copy of the characteristic stored in the computer. Among the unique characteristics of an individual that can be converted into a digital form are voice patterns, fingerprints, and the blood vessel patterns present on the retina of one or both eyes."); 21 CFR 1300.03 ("Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both distinctive to the individual and measurable."); 27 CFR 73.3 ("Biometrics. A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable."); 34 CFR 99.3 ("Biometric record as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting."); *see also* 46 USC 70123 ("For the purposes of this section, the term 'biometric identification' means use of fingerprint and digital photography images and facial and iris scan technology and any other technology considered applicable by the Department of Homeland Security.").

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.

~~**"Biometric Identifiers" means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics that 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, facial templates, or other unique biological, physical, or behavioral patterns or characteristics.**~~

We believe that addressing these concerns will create harmony for businesses and consumers and improve the regulation's effectiveness.

5. **The draft regulation should clarify individual rights obligations (4.04, 4.05, 4.07) to ensure workable standards for business compliance and align the requirements with other state laws.**

The sections on the right of access (4.04), right to correction (4.05), and right to data portability (4.07) require clarification to reflect the responsible and practical best practices by business.

The requirement in the right of access section (4.04 A) obligates controllers to provide *all* processor data that a controller has access to when completing an access request. This expectation is at odds with what would be reasonable for a controller to do in relation to an access request, and is also not in all circumstances impactful to a consumer, because it may involve subcontractor, third party, or other type of downstream data that adds little value to an end user or a consumer.

In a similar vein to section 4.04 (A), the right to correction section 4.05 (A) requires that controllers notify *all* processors across "all data flows and repositories" of the consumer request, which is a highly cumbersome process. As we noted in previous comments, there are serious complexities to requiring a business to contact all of these entities with the information, which may not add further value for the downstream processors of the data. A downstream processor may not need access to the consumer's request, if it is at a later date or no longer relevant to the obligations of the downstream processor. We recommend, instead, revising the requirement to include downstream processors as appropriate, rather than expecting contact with all known and unknown downstream processors and subcontractors.

Furthermore, section 4.04 (A)(1) and 4.04 (D) creates an expectation that the controller will share forms of data, including derived and inferential data, that at all costs would be required to be shared with the consumer. We disagree with this approach for a number of reasons, including the potential opening this creates for bad actors to use the derived or inferential data to create competing products, commit slander or malign the controller using the data, potential right of actions as a result of abuse of the data, or to conduct other processes

that could potentially harm the controller - even if this does not disclose trade secrets. In its place, we have recommended language that is also in other state consumer privacy laws that focuses on ensuring the good faith efforts by the controller to share information, as deemed appropriate.

Working at cross purposes with sections 4.04 (A)(1) and 4.04 (D), section 4.07 (B) more clearly explains that the controller needs to make efforts to share all data with the consumer to fulfill the data portability rights, so far as the controller does not violate trade secrets. Thus, sections 4.04 (A)(1) and 4.04 (D) seem to contradict section 4.07 B, by placing a higher bar - a tedious requirement on controllers for the right of access - while being more practical in the expectations for the right to data portability. Our edits would reduce confusion in how the two requirements work together and would reinforce the importance of companies protecting their trade secrets.

We therefore recommend the following change:

Rule 4.04 RIGHT OF ACCESS

A. A Controller shall comply with an access request by providing the Consumer all the specific pieces of Personal Data it has collected and maintains about the Consumer, **as deemed appropriate and in good faith by the controller.** ~~**including without limitation, any Personal Data that the Controller's Processors obtained in providing services to the Controller.**~~

1. ~~**Specific pieces of Personal Data includes 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.**~~

[...]

~~**D. If a Consumer exercises the right to access their data in a portable format pursuant to C.R.S. § 61-1306(1)(e) 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 in a nonportable format.**~~

Rule 4.05 RIGHT TO CORRECTION

A. A Controller shall comply with a Consumer's correction request by correcting the Consumer's Personal Data across ~~**all**~~ data flows and repositories, except archive or backup systems, and implementing measures, **as appropriate,** to ensure that the Personal Data remains corrected. The Controller shall also ~~instruct all~~ use the technical and organizational measures or process established by its Processors, to the extent feasible, that maintain the Personal Data at issue to make the necessary corrections in their respective systems and to ensure that the Personal Data remains corrected.

Rule 4.07 RIGHT TO DATA PORTABILITY

A. To comply with a data portability request, a Controller must transfer to a Consumer the Personal Data it has collected and maintains about the Consumer through a secure method in a commonly used electronic format that enables the Consumer to have complete access to and full enjoyment of the Personal Data, including, but not limited to, the capacity to save, edit, and transfer the Personal Data to any other person or platform at Consumer's discretion.

B. Pursuant to C.R.S. § 6-1-1306(1)(e), a Controller is not required to provide Personal Data to a Consumer in a manner that would disclose the Controller's trade secrets. ~~**When complying with a request to access Personal Data in a portable format, Controllers must provide as much data as possible in a portable format without disclosing the trade secret.**~~
~~1. Notwithstanding 4 CCR 904-3, Rule 4.07(B), Personal Data or Sensitive Data Inferences created using a trade secret algorithm or other mechanism must be disclosed to comply with a data portability request without disclosing the algorithm or mechanism itself.~~
~~**1. For example, if sharing both raw or unedited Personal Data along with related inferences or derived Personal Data in an Excel file would reveal a trade secret, the Controller may provide either set of Personal Data in an Excel file, so long as it is clear to the Consumer that the Controller maintains both types of Personal Data.**~~

6. **The draft regulations should remove conflicting requirements for what constitutes a Universal Opt-Out Mechanism signal (5.04) and clarify that controllers can request additional consumer information to facilitate the Universal Opt-Out Mechanism signal (5.05B).**

We reaffirm our previous comments regarding these sections. The regulations appear to adopt a standard for the Universal Opt-Out Mechanism signal that suggests the consumer does not need to actively make an opt-out decision. The intent does not align with the practical application of the Universal Opt-Out Mechanism and would lead to compliance challenges for businesses and confusion for consumers.

In addition, a controller may only receive a partial data element, such as an IP address through the Universal Opt-Out Mechanism, but the controller may need additional information to validate the signal. The regulation should clarify that the controller can request additional consumer information, as necessary and proportionate, to facilitate and inform the Universal Opt-Out Mechanism signal.

As such, we propose the following revisions:

Rule 5.04 DEFAULT SETTINGS FOR UNIVERSAL OPT-OUT MECHANISMS

[A..]

~~B. Notwithstanding 4 CCR 904-3, Rule 5.04(A), a Consumer's decision to adopt a tool that does not come pre-installed with a device, such as a browser or operation system, but is marketed prominently as a privacy-protective tool or specifically as a tool designed to that will exercise a user's rights to opt out of the Processing of Personal Data using a Universal Opt-Out Mechanism, shall be considered the Consumer's affirmative, freely given, and unambiguous choice to use a Universal Opt-Out Mechanism. The marketing for such a tool may also describe functionality other than the exercise of opt out rights and it need not refer specifically to opt-out rights in the State of Colorado.~~

1. ~~Example: A browser manufacturer markets its browser as a "privacy friendly" browser, highlighting that the browser sends a Universal Opt-Out Mechanism signal by default. The browser does not come pre-installed with a device or operating system and must be installed by the Consumer. The Consumer's decision to use this browser represents the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt- Out Mechanism. The Consumer need not be given an explicit choice about whether to use the Universal Opt-Out Mechanism in this example.~~

Rule 5.05 PERSONAL DATA USE LIMITATIONS

A. A platform, developer, or provider providing a Universal Opt-Out Mechanism shall not use, disclose, or retain any Personal Data collected from the Consumer in connection with the Consumer's utilization of the mechanism for any purpose other than sending or Processing the opt-out preference.

~~B. When processing a Universal Opt-Out Mechanism, a Controller may not require the collection of additional Personal Data beyond that which is strictly necessary to authenticate a Consumer is a resident of Colorado or determine that the mechanism represents a legitimate request to opt out of the Processing of Personal Data as permitted by C.R.S. § 6-1-1306(1)(a)(IV).~~

7. **Limit opting out of profiling "in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer" to Solely Automated Processing (9.04).**

The second draft of the regulations creates additional clarity regarding the distinction between "Human Reviewed Automated Processing" and "Human Involved Automated Processing"[19]. We would still encourage the Attorney General's office to clarify the definition of

[19] Colorado Privacy Act Draft Regulations V2, Definitions 2.02:
"**Human Involved Automated Processing**" means the ~~Automated~~ Processing of Personal Data where a human ~~involvement in~~ automates the Processing ~~includes~~ through the use of computers, computer programs, software, or other digital technology and (1) engages in a meaningful consideration of available data used in the Processing ~~as well as~~ and any output of the Processing and (2) has the authority to change or influence the outcome of the Processing.

"meaningful consideration" and we also recommend that opting out of profiling should be limited to decision making involving solely automated processing. Further clarity is essential for data controllers to understand their obligations for each category of processing activity and comply with the requirements.

As stakeholders mentioned during the Colorado public sessions[20] and in written comments[21], there are clear, unintended consequences in a number of contexts, including housing, financial services, and higher education, which can arise if consumers opt out of profiling that involves a human in the loop and that leads to decisions that have "legal or similarly significant effects." Of note, CPA compliance is required for nonprofits within every sector, which compounds the problem further.

It is more feasible to limit opting out of profiling "in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer" to Solely Automated Processing. This is the case in other global privacy regimes, including the GDPR, which states that "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" in Article 22[22]. Similarly, Virginia's consumer privacy law[23] does not differentiate between human involved and human reviewed automated processing, and instead, only requires controllers to comply with an authenticated request to allow consumers to exercise the right to "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." The lack of interoperability between Colorado's approach to profiling and other state laws will further exacerbate compliance.

Our recommended edits are as follows:

Rule 9.04 OPTING OUT OF PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER

B. Requests to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer based on Solely Automated Processing ~~**or Human Reviewed Automated Processing**~~ shall be honored pursuant to C.R.S. § 6-1-1306(2).

"**Human Reviewed Automated Processing**" means the ~~Automated Processing~~ automated processing of Personal Data where a human reviews the ~~Processing~~automated processing, but the level of human ~~review~~engagement does not rise to the level required for Human Involved Automated Processing. Reviewing the output of the ~~Automated Processing~~ automated processing with no meaningful consideration does not rise to the level of Human Involved Automated Processing.

[20] Colorado Stakeholder Session on *Profiling, Consent, and Definitions*. November 17. Remarks by Stephanie O'Malley, Representative for Independent Higher Education of Colorado. At 17:00 - 20:00/3:02:06.
[21] Comments by Independent Higher Education Committee
[22] Article 22 GDPR
[23] Virginia Consumer Data Protection Act

C. A Controller may decide not to take action on a request to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer if the Profiling used is based on Human Involved Automated Processing **or Human Reviewed Automated Processing, unless the Decision is likely to Bring Harm to the Consumer**. If a Controller does not take action based on this reason, the Controller shall inform the Consumer pursuant to C.R.S. § 6-11306(2)(b) and include the following information~~:~~, or share a link to such information if it is included in the Controller's privacy notice:

[...]

8. **Clarify the exemptions for controllers and processors to use data for internal research and related operations and services, to support interoperability with the exemptions for controllers and processors in other state laws (6.06 and 6.07).**

We reaffirm our previous comments on the following, which have not been addressed in the second draft of the regulations. The CPA (at C.R.S. § 6-1-1304, Pg. 12-13) states that Controllers and Processors are offered specific exemptions with regard to the processing activities of a Controller or Processor. The exemptions include permitting Controllers or Processors to use Personal data to "conduct internal research to improve, repair, or develop products, services, or technology"; "identify and repair technical errors that impair existing or intended functionality"; and "perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller."

Further clarity in the regulations regarding these exceptions to the data minimization and purpose specification principles is critical. The draft regulations should clarify that processors and controllers can use the data for internal research and other internal activities and operations that may not be specified in the contract. This approach will align to other state consumer privacy laws and regulations and create greater interoperability.

For example, the draft regulations to the CPRA[24] brings additional clarity with regard to the opportunities for data controllers to use the data for internal operations that may not be specified in the contract, which is a routine process for businesses that are at different stages of the product life cycle and may require additional data for new product testing, security/debugging, experimentation, and launch.

Therefore, our recommended clarification to Rule 6.06 and 6.07 is as follows:

Rule 6.06
Purpose Specification

[24] The CPRA Modified Draft Regulations (pgs. 54-55) state that "An SP [Service Provider] shall retain, use, or disclose personal information collected pursuant to its written contract with the controller" for a number of purposes, including "internal use by the service provider or contractor to build or improve the quality of the services it is providing to the business, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person."

A. Controllers shall specify the express purposes for which Personal Data are collected and Processed in both external disclosures to Consumers as well as in any internal documentation required by this Part 6.
[..]
E. A controller may collect Personal Data for internal use by the processor to build or improve the quality of the services it is providing to the controller, even if the Processing purpose is not specified in the contractual agreement.

Rule 6.07 Data Minimization
C. A Controller shall not collect Personal Data other than those disclosed in its required privacy notice, or if it is collected subject to the exceptions listed pursuant to C.R.S. § 6-1-1304. If the Controller intends to collect additional Personal Data the Controller shall revise its privacy notice, and notify Consumers of the change to its privacy notice pursuant to 4 CCR 904-3, Rule 6.04.

* * *

Thank you for considering our suggested revisions to the CPA draft regulations. We are happy to discuss in further detail, as appropriate.

Respectfully submitted,

Divya Sridhar, Ph.D., Senior Director, Data Policy
Software and Information Industry Association