December 9, 2022

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 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 draft rules supporting the Colorado Privacy Act (CPA).

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 600 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 CPA draft regulations stronger. In sum, our comments address the following issues.

1. The regulations should not extend to any form or extension of Publicly Available Information (2.02).

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

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

4. The regulations should sharpen the definition of biometric data (2.02).

5. The regulations should streamline individual rights obligations (4.04, 4.05, 4.09) to ensure workable standards for compliance and align the requirements with other state laws. The regulations should also delete the requirement to document consumer requests responses (4.09).

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

7. The regulations should not equate the delivery of ads to automatically result in profiling that is in furtherance of legal or similarly significant effects (9.03).

8. The regulations significantly exceed the scope of the statute with respect to dark patterns and should be revised accordingly (7.09).

9. Limit opting out of profiling "in furtherance of decisions that have legal or similarly significant effects" to Solely Automated Processing (9.04).

10. 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 not extend to any form or extension of Publicly Available Information (2.02).**

Ensuring a healthy regulatory environment to make productive use of publicly available information (PAI) is an important issue for SIIA members. Many of our members rely on PAI to generate productive and socially beneficial information, products, and services, including, but not limited to: finding missing children, performing corporate due diligence, preventing money laundering and fraud, and facilitating investigative journalism. The policy benefits that result from a robust public domain are more than happy accidents: they are guaranteed by the First Amendment of the U.S. Constitution.

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

The draft regulations diverge from statute by including new elements that are considered exclusions from PAI. This overly broad approach would create additional compliance obligations for companies, undermine the interstate interoperability of consumer privacy laws, and violate the First Amendment. These exclusions are not in line with the CPA's intent, as they are not present in the statute. We recommend striking at least two of the exclusions to PAI.

a. Inferences made exclusively from multiple independent sources of PAI are subject to the First Amendment and should be considered PAI.

First, an inference made exclusively from PAI should not be subject to regulation as if it was not PAI. Just as with any other kind of prior restraint on speech, regulating inferences generated by speech risks conflicting with the rights afforded by the First Amendment.

For example, suppose that a company makes an inference based on a real estate deed, a white pages phone listing, and a newspaper article that a particular "John Smith" is who he claims to be, before delivering a home theater system to him. That person has no privacy interest in the fact that he is identified by these sources as "John Smith." Likewise, an inference that this individual is "John Smith" does not violate his expectation when a transaction (that, presumably, he requested) is cleared. The transfer–and use–of such information remains protected speech.[2] This section of the regulation should therefore be deleted.

Just as businesses are not required to request consent to use publicly available data, the same can be said of inferences that do not require a consumer's consent[3] to process these inferences - neither practice comports with the First Amendment.

At its core, the premise of regulating inferences drawn from multiple independent sources of PAI is in conflict with regulating one independent source (whether credible or not). This would further complicate the ecosystem by choosing winners and losers between companies that draw inferences from strictly one source of PAI (and thus would not fall into the sweep of the CPA) and companies that use multiple sources of PAI.

---

[1] 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 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?"*

[2] *See* Bartnicki v. Vopper, 534 U.S. 514 (2001); IMS Health v. Sorrell, 564 U.S. 552 (2011).

[3] Colorado Privacy Act Draft Regulations. 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."

Regulating inferences drawn solely from independent sources of PAI will lead to an over-regulation of data by treating the PAI-based inference as "potentially" personal data, endangering businesses and consumers alike.

The implications of this are significant. Without the presence of a diverse range of high-quality data and the respective inferences it generates, businesses, consumers and other stakeholders will lose out on the powerful insights generated from evidence-based research and respective outcomes. These outcomes benefit society by mitigating bias, furthering research, and more.[4] A privacy law seeking to regulate inferences could weaken the entire information ecosystem upon which the digital marketplace rests.

In addition, sweeping inferences into the scope of a data privacy law could also empower bad actors (e.g., criminals) to delete data and thus further diminish the quality of the data being processed and the inferences generated. This could hamper the positive impacts felt by a broad swath of industries using mathematical data processing approaches, such as statistical analyses and inferences. Examples include finance, healthcare, retail, and other spaces with real-time markets where businesses and end users depend on predictive and inferential statistics.

Finally, the draft regulations' restrictive approach to inferences are not in alignment with other state consumer privacy laws. As Colorado's consumer privacy law is the first of its kind to apply to nonprofits, the approach to regulating inferences would be particularly problematic for the nonprofit sector that uses inferences to build and inform the research and development pipeline.

To address this concern, we propose that the AG amend proposed Rule 2.02 by removing clause 2 in the definition of "Publicly Available Information".

b. PAI should remain PAI, even if is combined with other forms of data.

The proposed regulations go beyond the scope of the CPA in their treatment of "PAI that has been combined with non-publicly available Personal Data," which we refer to as combined data. The fact that PAI has been commingled with other data does not change its status as PAI. For example, "John Smith" may not exercise rights of deletion or "do not sell" over the content of his real estate deed even if, for example, that information was combined with personal data containing a purchase history from his credit card. That data remains in the public domain.

In addition, treating combined data as personal data could result in unintended consequences. In the law enforcement context, a host of entities that partner directly with law enforcement like the Colorado Attorney General, such as the National Insurance Crime Bureau (NICB), have submitted comments requesting an exemption for their work, given its socially

[4] For example, Brookings is one of a growing list of sources identifying insufficient or improperly narrowed training data as a primary cause of bias. Nicole Turner Lee et al., Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms, Brookings, Brookings.edu (May 22, 2019).

beneficial impact to further the state's public interest.[5] SIIA works with members who routinely provide PAI in combination with lawfully acquired personal data. For example, law enforcement might check utility bills and recent purchases of a property owner before serving a warrant. Many of our members are concerned that bad actors, including criminals, will request that transmission of their "personal" data cease, or that the data could be deleted.

The treatment of combined data would unintentionally weaken the ability of controllers (and other covered entities) to make precise decisions with the data. This is due to the data subject access request rights that would newly apply to the combined data under the CPA. Just as with the discussion on regulating inferences derived from multiple sources of PAI, companies' uses of combined data sources can provide more accurate and ethical results and deliver superior analytical results or decisions. Subjecting the combined data to the CPA could undermine companies' opportunities to build high-quality decision and analytics tools and weaken each company's ability to equip consumers with the high-quality results.

For example, combined data may be used to assist data controllers and processors with online deliveries in the digital marketplace. Such companies use a combination of public records and private databases of customer records to confirm customers' addresses and locations. By subjecting the combined data source to the CPA, businesses will need to gather additional consent and fulfill additional obligations to process the data, which will further delay deliveries and could lead to the deliveries being less accurate and secure.

There are numerous examples of how the draft regulations would curtail productive and socially beneficial uses of PAI, enabling problematic activities of bad actors.

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

"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; or
~~5. Publicly Available Information that has been combined with non-publicly available Personal Data; or~~
4.~~6.~~ Nonconsensual Intimate Images known to the Controller

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

[5] Rulemaking Comment of the National Insurance Crime Bureau on the Colorado Privacy Act (Nov. 2, 2022); see also Rulemaking Comment of the National Insurance Crime Bureau on Colorado Law Enforcement/NICB Partnership: Case Examples (Nov. 2, 2022).

The proposed regulations create a new term and definition for "Sensitive Data Inferences." This term is not present in the CPA and goes beyond the text and intent of the CPA statute. When read against the definition of PAI, it leads to contradictions that will render the regulations unworkable for consumers and businesses.

First, the term "Sensitive Data Inference" is problematic because the term presumes that "inferences" derived from data should be regulated the same as the underlying data, sweeping in a host of data, including correlated data and related social determinants. This term sweeps in a broad array of data that in itself may not be sensitive, or otherwise subject to the scope of the CPA.

Second, the term "Sensitive Data Inference" and its associated requirements could lead to duplication in the way that data is treated within the scope of the law. We believe that the purpose and respective treatment of other defined terms – "sensitive data" and "personal data" – are duplicative with the term "sensitive data inferences," creating confusion as to how the data is categorized by businesses, particularly in use cases where the data could be categorized as more than one of these terms. For example, applying the proposed definition of "sensitive data inferences," the CPA draft regulations would consider a business's processing of information revealing that the "Olympic gymnast Simone Biles suffers from mental health issues" to be PAI, a sensitive data inference, and personal data. This example highlights how the proposed definition of "sensitive data inferences," if implemented, will run into First Amendment and public domain concerns involving PAI.

Second, the term presumes that inferences are derived from non-PAI although the definition is not crafted with this limitation. As a result, it will cover a range of "inferences" based on data that are also in the public domain, which would then require covered entities to offer all consumers specific rights with regard to accessing that data. This will lead to enormous implementation hurdles and also undermine socially beneficial uses of PAI that are critical to law enforcement and other public interest purposes.

Third, the new term's inclusion does not align with global privacy regulations or practices, or existing state privacy laws, which is at odds with the intent of the CPA being interoperable with other state consumer privacy laws. This misalignment will further complicate business compliance. To this end, 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[6]) 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)[7]). Existing U.S. federal code 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)).[8]

[6] GDPR. https://gdpr-info.eu/art-9-gdpr/
[7] GDPR. https://gdpr-info.eu/art-22-gdpr/
[8] FTC. Protections Against Discriminations and Other Prohibited Practices; EEOC. Privacy.

The definition of sensitive data is present verbatim in Utah's and Virginia's state laws,[9] but does not include the same reference to 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, and as noted previously, 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 research and development – primarily conducted by 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.~~

[9] Consumer Data Protection Act. Virginia Code Ann. §59.1-571.; Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 et seq. (2022).

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 to concerns about the interaction of "sensitive data inferences" noted under our last recommendation, the term is likely to create significant confusion for businesses and consumers alike that is not likely to be resolved by further amending the term. Through Section 6.10 as written, businesses are unlikely to know the extent to which they must obtain relevant consents. 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.

In particular, the section should be revised so that consent to process inferences derived from sensitive data (except for specific use-cases) is not met with Constitutional challenges, as the regulation of inferential data would be in conflict with the First Amendment.

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) hours of collection or of the completion of the Processing activity, whichever comes first;~~
~~3. The Personal Data and any 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) 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).

The regulations define "Biometric Data" as an extension of "Biometric Identifiers," which could lead to conflicting interpretations of the statute, and unnecessary overbreadth and unintended consequences, if the concurrent use of the terms is not revised. As written, SIIA has concerns with the vaguely constructed definition of biometric data, which will require additional clarification in its practical application to inform business compliance. We recommend the statute 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.[10] Thus, technologies using biometric information in this manner present a very different risk profile.

To address this, we recommend that the regulations use a more precise definition that incorporates a scoping principle to determine the unique privacy interest for regulating biometrics. The inclusion of the term "biometric identifier" as written would capture other uses of the data, beyond those that have a unique privacy interest, which is using the biometric data to identify the individual. As written, the term "biometric identifier" sweeps in a number of common practices that may not involve specifically processing biometric data to identify an individual. For example, when consumers use facial or fingerprint detection for authentication, this would be considered biometrics. Every time a consumer moves the mouse around in virtual reality, this is also considered biometrics. Using virtual reality aids for staging a room with furniture, even if the data is not stored on the local device, would also be considered biometrics. Using connected vehicles that use facial detection or recognition software to spot individuals in the rear of the car but do not store the data on the device would also be swept in. These are examples of fairly routine and socially beneficial use cases that would be considered biometrics, even if they do not have a unique privacy interest or a scoping principle that focuses on identifying an individual.

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

[10] 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).

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[11,12] as a distinct term that includes specific, immutable characteristics used to 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."[13] NIST offers several definitions, each referring to physical and/or behavioral characteristics, rather than derivations from these characteristics.[14] The Code of Federal Regulations and the U.S. Code use definitions that are generally aligned with these.[15]

The definition of "biometric identifier" should be deleted, as its inclusion risks expanding the consent requirements in the downstream process to uses that extend beyond the realm of identification alone, lead to consent fatigue, and it would stifle the practical applications of the

[11] 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.

[12] 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 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).

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

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

[15] *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.").

tools that result. 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.

Thus, we 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 that is used to identify a specific 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 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, 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 streamline individual rights obligations (4.04, 4.05, 4.09) to ensure workable standards for business compliance and align the requirements with other state laws. The regulations should also delete the requirement to document consumer requests responses (4.09).**

The right of access (4.04), right to correction (4.05) and right to respond (4.09) to consumer requests sections (4.04, 4.05, and 4.09, respectively) need to be more streamlined to reflect the responsible and practical best practices by business.

The requirement in the right of access section (4.04) 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 backup/archival/downstream data that adds little value to an end user or a consumer.

In a similar vein, the right to correction section (4.05) requires that controllers notify *all* processors across "all data flows and repositories" of the consumer request, which is a highly cumbersome process, and in some cases, impractical because of the various downstream providers, as well as archival and backup systems, which a business may work with. 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.

Further to this point, the section on responding to consumer requests necessitates that the controller include the Personal Data "in a form that is concise, transparent and easily intelligible", and "avoids incomprehensible or unexplained internal codes and identifiers" (4.04). Second, the controller is required to share with all processors the consumer request as well as the consumer's response, which is an unusual expectation (not aligned with other privacy regimes), and it does not add direct value to consumer, proportional to the costs and burden it would add to the controller to collect it.

If it is determined that the provision will remain, it is our recommendation that the rules add a new term to note the "disproportionate effort"[16] that these requests may place on a business and thus if the request and its respective effort is not in line with the expected outcome, it may not need to be complied with. Industry made the same request regarding California's consumer privacy regulations, and it was deemed that the term "disproportionate effort" apply to all data controllers, to support compliance and create a safe harbor against unwieldy consumer requests.

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~~, including without limitation, any Personal Data that the Controller's Processors obtained in providing services to the Controller~~.

[16] Modified draft regulations of the CPRA. "Disproportionate effort" within the context of a business, service provider, contractor, or third party responding to a consumer request means the time and/or resources expended by the business, service provider, contractor, or third party to respond to the individualized request significantly outweighs the reasonably foreseeable impact to the consumer by not responding, taking into account applicable circumstances such as, the size of the business, service provider, contractor, or third party, the nature of the request, and the technical limitations impacting their ability to respond benefit provided to the consumer by responding to the request.

B. Personal Data provided in response to an access request ~~must~~ should, to the extent feasible, be:

1. Understandable to the Controller's target audiences, considering vulnerabilities or unique characteristics of the audience and paying particular attention to vulnerabilities of Children.

2. Provided in the language in which the Consumer interacts with the Controller.

3. Provided in a form that would allow the average Consumer to make an informed decision of whether to exercise deletion, correction, or opt-out rights.

a. For instance, the Personal Data must be provided in a form that is concise, transparent, and easily intelligible~~, and avoids incomprehensible or unexplained internal codes and identifiers~~.

b. Nothing herein shall prevent a Controller from complying fully with a Consumer's data portability request pursuant to C.R.S. § 6-1-1306(1)(e).

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 and implementing measures to ensure that the Personal Data remains corrected~~. The Controller shall also instruct all 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 4.09 RESPONDING TO CONSUMER REQUESTS

C. When a Controller complies with a Consumer's Personal Data Right request, the Controller shall also notify all Processors that Process the Consumer's Personal Data of the Consumer's request ~~and the Controller's response~~.

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).**

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 if it is necessary to facilitate and inform the Universal Opt-Out Mechanism signal.

As such, we propose the following revisions:

Rule 5.04 DEFAULT SETTINGS

[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 exercise a user's rights to opt out of the Processing of Personal Data shall be considered the Consumer's affirmative, freely given, and unambiguous choice to use a Universal Opt-Out Mechanism.~~

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 confirm 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. The draft regulations should not equate the delivery of ads to automatically result in profiling that is in furtherance of legal or similarly significant effects (9.03).

The draft regulations equate ads "related to housing, employment, or financial or lending services" to profiling that is in furtherance of "legal or similarly significant effects". On the other hand, the statute states that a decision that produces legal or similarly significant effects means "a decision that results in the provision or denial" of certain services (rather than a decision to advertise such services), and accordingly, the conflict across these paradigms leads to confusion.

Therefore, we suggest the following change, to bring the text of the CPA in line with other US state consumer privacy laws:

Rule 9.03 PROFILING OPT-OUT TRANSPARENCY

A. To ensure that Consumers understand how their Personal Data may be used for Profiling in furtherance of Decisions that Produce Legal or Other Similarly Significant Effects Concerning a Consumer, Controllers that Process Personal Data for Profiling covered by C.R.S. §§ 6-1-1303(10) and 6-1-1306(1)(a)(I) shall provide clear, understandable, and transparent information to Consumers in the required privacy notice, including at a minimum:

(1) What decision is subject to Profiling;

(2) The categories of Personal Data that were or will be Processed as part of the Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects;

(3) A plain language explanation of the logic used in the Profiling process;

(4) Why Profiling is relevant to the ultimate decision;

~~**(5)** If the Profiling is used to serve ads related to housing, employment, or financial or lending services;~~

(6) If the system has been evaluated for accuracy, fairness, or bias, including the impact of the use of Sensitive Data, and the outcome of any such evaluation;

(7) The benefits and potential consequences of the decision concerning the Consumer; and

(8) Information about how a Consumer may exercise the right to opt out of the Processing of Personal Data concerning the Consumer for Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects.

8. **The draft regulations significantly exceed the scope of the statute with respect to dark patterns and should be revised accordingly (7.09).**

The draft regulations (at 7.09 C) state that all dark patterns are prohibited. This mandate conflicts with the intent of the statute, which is to ensure dark patterns are not used to obtain consent. The requirements in 7.03 F, state, in alignment with the statute, that “any agreement obtained through Dark Patterns is not valid Consent,” which is a reasonable measure that businesses are already making good faith efforts to meet. The outright prohibition on the use of dark patterns would be a significant shift from the text and original intent of the statute that is focused on the use of dark patterns for the purpose of obtaining consent. Section 7.09 C would impose additional obligations on businesses that would not be in furtherance of interoperable standards across the states.

Of note, the rule at 7.09 C is also in direct conflict with the rule at 7.09 F, which states: "in addition to the principles included in this part 4 CCR 904-3, Rule 7.09, Controllers may consider statutes, administrative rules, and administrative guidance concerning Dark Patterns from other jurisdictions when evaluating the appropriateness of their proposed choice architecture or system design." It is difficult for businesses to both rely on an explicit prohibition (7.09 C) *and* for them to consider other laws and guidance on the subject as noted in 7.09 F.

To improve clarity and streamline the operational compliance with regard to dark patterns, we recommend striking 7.09 C, which would allow businesses to focus on compliance with the principles under 7.09 B, and in certain circumstances, consideration of guidance regarding dark patterns in other jurisdictions as set forth in 7.09F.

As such, we propose the following change:

Rule 7.09 USER INTERFACE DESIGN, CHOICE ARCHITECTURE, AND DARK PATTERNS
[..]
~~**C. The use of Dark Patterns, as defined in C.R.S. § 6-1-1303(9), is prohibited.**~~

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

The CPA draft regulations distinguish between "Human Reviewed Automated Processing" and "Human Involved Automated Processing," which is based on whether there is "meaningful consideration of available data used in the Processing, as well as the authority to change or influence the outcome of the Processing"[17]. We would encourage the Attorney General's office to clarify the definition of "meaningful consideration." This 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[18] and in written comments[19], 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

[17] See Rule 2.02, Defined Terms:
"Human Involved Automated Processing" means the Automated Processing of Personal Data where human involvement in the Processing includes meaningful consideration of available data used in the Processing as well as the authority to change or influence the outcome of the Processing.
"Human Reviewed Automated Processing" means the Automated Processing of Personal Data where a human reviews the Processing but the level of human review does not rise to the level required for Human Involved Automated Processing. Reviewing the output of the Automated Processing with no meaningful consideration does not rise to the level of Human Involved Automated Processing.
[18] 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.
[19] Comments by Independent Higher Education Committee

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[20]. Similarly, Virginia's consumer privacy law[21] 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.

One such unintended consequence is the processing of data for the purposes of determining college/university eligibility, enrollment, housing, and financial aid. In the higher education context, automated processing where humans are in the loop is used to assess eligibility for financial aid and college application processes. The draft rules allow applicants to opt out of requests when the profiling involves some human review, even if it is not considered "meaningful" in nature. This would be problematic for nonprofit colleges and universities that participate in such activities, but do not have the resources to administer a more robust "Human Involved Automated Processing."

Because of the lack of clarity in what is considered to be "meaningful consideration" and the likelihood that many universities have Human Reviewed Automated Processing as part of their application processes, there would be serious repercussions for college applications and related decisions. If opting out of profiling would result in harm to a consumer - such as ineligibility to receive financial aid to attend school - the rules should not allow consumers to opt out and should not require the institution (the controller) process such a request.

Our recommended edits are as follows:

Rule 9.04 Opting out of profiling in furtherance of decision 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).

C. A Controller may not 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

[20] Article 22 GDPR
[21] Virginia Consumer Data Protection Act

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:

[...]

10. **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.**

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[22] 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
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.
[..]

[22] 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."

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