May 20, 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 re: Colorado Privacy Act - Public Input for Pre-Rulemaking Session

Dear General Weiser:

On behalf of the Software and Information Industry Association (SIIA), we write in response to your office's request for input in advance of the rulemaking for 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 highlight the following points that we believe would make the CPA stronger in its implementation:

- Publicly available information. Many of our members depend on information in the public domain. The current version of the CPA does not appropriately address free speech concerns in its attempt to exempt publicly available information from the definition of personal data. We recommend a definition that adds widely available media - a defined phrase that clearly exempts the republication of information in databases of newspapers, and in unrestricted social media feeds - in addition to information released by the government, which is part of the existing statutory definition.

- Amend the language to strengthen consumer rights and freedoms. Without this language, covered entities will lack the necessary flexibility to consider when the fulfillment of an individual request may infringe on the privacy of others, especially in circumstances when devices are shared by more than one individual. Other states like Virginia and California take an approach to remedy this problem.

- Add accommodation for infeasible consumer requests. We recommend Colorado include additional guidelines in statute to denote action taken by data controllers, in the event of technically infeasible or unfounded consumer requests, in an effort to harmonize consumer requests with business compliance.

- Clarify provisions categorized as "sensitive data". We recommend clarifying the definition of sensitive data to ensure that consumers and businesses are aligned on the expectations for how sensitive data is treated.

    ○ First, the Colorado bill should include a clear and concise definition of biometric data. We recommend aligning with the definition of biometric data in Virginia's privacy law to avoid confusion in practical application of the definition and help in the implementation of the Colorado bill, while avoiding costly implementation challenges.

    ○ Second, we recommend that the Colorado bill clarify that sensitive data includes data *collected from* a child, rather than more generally *about* a child. This change would help the bill to focus on the issue of concern without leading to implementation challenges ancillary to children's data.

1. Strengthen the definition of Publicly Available Information (PAI) in the Colorado Privacy Act

The CPA's treatment of publicly available information materially differs from - and is much narrower - than that in the California Privacy Rights Act (CPRA), Virginia's Consumer Data Protection Act [1] (VCDPA), and Utah Consumer Privacy Act (UCPA)[2]. In order to pass constitutional muster, the bill must exempt two classes of information from its sweep. The first involves information released by the government, which the statute appropriately carves out. The second type is that which is widely available in private hands and appears on publicly available web sites, in databases of newspapers, and in unrestricted social media feeds. It is this second category of information where the legislation falls short.

In its current form, the CPA defines publicly available information as an exception to personal data.[3] The CPA defines "personal data" as information "reasonably linkable" to a consumer. It then states that such information does not include publicly available information, defined as:

> "information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public."

Section 6-1304(2)(d) also provides that the act does not apply to information made available by a third party that the controller has a "reasonable basis to believe" is protected speech pursuant to applicable law.

---

[1] Virginia Consumer Data Protection Act of 2021 ("VCDPA"), Va. Code Ann. § 59.1-571 through 59.1-581

[2] Utah Consumer Privacy Act, Utah Code §13-61-101 through 13-61-404

[3] Colorado Privacy Act, § 6-1-1303. Definitions. (17) Personal Data (b).

We appreciate that this language is intended to address free speech concerns with consumer privacy legislation. Nonetheless, this formulation is constitutionally inadequate: for example, defamation law protects publishers from liability in public figures even if the publisher's belief is negligent. A newspaper may have a reasonable suspicion that a source's information about a particular matter came from a violation of any number of legal obligations. But the newspaper still has the right to publish, and SIIA's members have the right to republish that information. The government cannot pull that information back out of public discussion. E.g., New York Times Co. v. United States, 403 U.S. 713 (1971); Florida Star v. B.J.F., 491 U.S. 524 (1989).

For reasons spelled out in the attached memorandum provided to the California legislature during its consideration of the CCPA, a failure to carve out this category of the public domain will result in the law being held unconstitutional. We note that a legislative consensus has emerged in every enacted privacy statute (as well as the Uniform Law Commission's Uniform Data Privacy Act), which has added a definitional exclusion that allows for the distribution of information in widely distributed media on far more expansive terms than that in the current draft of the CPA.[4]

We therefore suggest that Colorado follow the definition used in CPRA:

> (17) "PERSONAL DATA": (a) MEANS INFORMATION THAT IS LINKED OR REASONABLY LINKABLE TO AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL; AND
>
> (b) DOES NOT INCLUDE DE-IDENTIFIED DATA OR PUBLICLY AVAILABLE INFORMATION.
>
> AS USED IN THIS SUBSECTION (17)(b), "PUBLICLY AVAILABLE INFORMATION" MEANS INFORMATION THAT IS LAWFULLY MADE AVAILABLE FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS ~~AND INFORMATION THAT A CONTROLLER HAS A REASONABLE BASIS TO BELIEVE THE CONSUMER HAS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC.~~ OR INFORMATION THAT A CONTROLLER HAS A REASONABLE BASIS TO BELIEVE IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC BY THE CONSUMER OR FROM A WIDELY DISTRIBUTED MEDIA OR BY THE CONSUMER; OR INFORMATION MADE AVAILABLE BY A PERSON TO WHOM THE CONSUMER HAS DISCLOSED THE INFORMATION IF THE CONSUMER HAS NOT RESTRICTED THE INFORMATION TO A SPECIFIC AUDIENCE.

We do understand that unlike California, Colorado law does not have a definition of "widely distributed media." The term originated in regulations implementing the Gramm Leach Bliley Act, see 12 C.F.R. 1016.3 (4)(1)(ii), which California copied when it implemented its own financial privacy statute. See Cal. Financial Code, 4052(k) ("Widely distributed media" means media available to the general public and includes a telephone book, a television or radio program, a newspaper, or a Web site that is available to the general public on an unrestricted basis). By amending the definition of personal data in this fashion, the bill removes the shadow of facial invalidity and allows the legislature to create meaningful privacy protection for Colorado residents.

[4] A First Amendment analysis of the CCPA, which at the time limited its definition of publicly available information in a manner similar (but not identical) to the draft legislation, can be shared at your convenience.

2. The CPA should be amended to strengthen consumer rights and freedoms

CPRA and the Virginia Consumer Data Protection Act (VCDPA) include an exception to consumer rights if exercise of those rights would adversely affect the rights and freedoms of third parties. See Cal. Civil Code 1798.145(k); Virginia Stat. Ann. § 59.1-582(E). The CPA does not. Controllers use this exception when the fulfillment of a user rights request could create a new privacy risk. Without this language, covered entities will lack the necessary flexibility to consider when the fulfillment of a consumer request may infringe on the privacy of others.

For example, controllers should not be required to provide messages concerning threats or harassment to a suspected abuser, as doing so may lead to retaliatory violence. Relatedly, controllers should have protections to be able to withhold information about a report of abuse or harassment on the controller's platform, maintaining the privacy of the reporter and potentially shielding them from increased abuse.

Addition of language similar to that in Virginia and California will remedy this problem and prevent consequences that we do not believe its authors intend, and we urge that such language be added to section 6-1-1304.

3. Denote a carveout for technically infeasible or unfounded consumer requests

The CPA should limit the potential abuse of the consumer request system. While the CPA allows data controllers to charge consumers for additional requests following the first consumer request for information, it places no qualitative limits on the number of such requests. Furthermore, the statute does not allow businesses to automatically align additional requests with any additional fees (beyond a fee that exceeds the cost of providing the record).

We therefore recommend that Colorado add an exception for technically infeasible, unfounded or excessive requests in an effort to incentivize requests made in good faith. Alternatively, data controllers could be permitted to charge fees, as appropriate, for additional, unreasonable requests.

We recommend the following change to Section 1 [5]:

> 2 (c) UPON REQUEST, A CONTROLLER SHALL PROVIDE TO THE CONSUMER THE INFORMATION SPECIFIED IN THIS SECTION FREE OF CHARGE; EXCEPT ~~THAT, FOR A SECOND OR SUBSEQUENT REQUEST WITHIN A TWELVE-MONTH PERIOD, THE CONTROLLER MAY CHARGE AN AMOUNT CALCULATED IN THE MANNER SPECIFIED IN SECTION 24-72-205 (5)(a).~~ IN CIRCUMSTANCES WHERE THE REQUEST IS EXCESSIVE, REPETITIVE, TECHNICALLY INFEASIBLE, OR UNFOUNDED, IN WHICH CASE THE CONTROLLER CAN DENY THE REQUEST OR CHARGE CONSUMERS AS APPROPRIATE FOR SUCH REQUESTS.

4. Focus the definitions and parameters of "sensitive data" with respect to biometrics and information about children.

[5] Colorado Privacy Act § 6-1-1306. Consumer personal data rights - repeal. 2 (c). Consumer Requests.

The CPA requires a consumer's opt-in consent for processing sensitive data. "Sensitive data" is defined to include many categories of data, some of which require additional clarification for practical implementation purposes.

a. Biometric Data

Biometrics have grown in use and availability because of their high level of accuracy in identifying and authenticating individuals and their potential to further safeguard consumers' security and safety. We agree that consumers should have the right to appropriate notices and consents concerning the collection, retention, destruction, and disclosure of their biometric information in business operations. We recommend the statute expressly define biometric data to avoid overreach in the implementation of the law.

In section 1[6], the CPA defines "sensitive data" to include "biometric data," but the statute does not define what biometric data is. The lack of a definition could lead to overly broad interpretations and unintended consequences.

As written in CPA, as part of the definition of "sensitive data":

> (24) "SENSITIVE DATA" MEANS: … (b) GENETIC OR BIOMETRIC DATA THAT MAY BE PROCESSED FOR THE PURPOSE OF UNIQUELY IDENTIFYING AN INDIVIDUAL;

Other states have avoided these problems by adding definitions. For example, the 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."[7] The 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.[8]

This robust definition serves as a wise and practical limit on the unintended consequences that the CPA's lack of definition will cause. For example, in Illinios [9] (which has made this determination) companies have had to obtain additional consent to process every photograph a consumer decides to voluntarily post to a website and have faced a litany of class action lawsuits based on processing photographs. We believe that addressing these concerns will prevent the unintended complication of the use of photographs in a range of low-risk, routine activities.

b. Information about children

---

[6] Colorado Privacy Act. § 6-1-1303. Definitions. 24 (b).
[7] Virginia Consumer Data Protection Act of 2021 ("VCDPA") Va. Code Ann. § 59.1-571. Definitions. (enacted from Virginia Senate Bill 1392).
[8] Id.
[9] Illinois BIPA. 740 ILCS 14/10.

Section 1[10] also defines sensitive data as “personal data from a known child,” which would lead to ambiguity in its practical application. The definition could encompass information that parents or guardians voluntarily share about their children - including personal data that is not sensitive, such as photos of their child shared with close friends and family via the internet. It could prevent newspapers from highlighting any achievements of local children or critical announcements made to identify missing children. To clarify this, we recommend this provision be amended as follows.

The statute should read:

> "SENSITIVE DATA" MEANS: …OR (c) PERSONAL DATA COLLECTED FROM A KNOWN CHILD.

* * *

Thank you for considering our suggested revisions to the CPA. We would welcome the opportunity to discuss them in further detail.

Respectfully submitted,

Christopher A. Mohr
SVP for Intellectual Property and General Counsel

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

[10] Colorado Privacy Act. § 6-1-1303. Definitions. 24 (c).