November 7, 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, Part 2 Definitions

Dear General Weiser:

On behalf of the Software and Information Industry Association (SIIA), we write in response to the Department of Law's request for input on draft regulations for the Colorado Privacy Act (CPA) to inform the upcoming stakeholder session on *Profiling, Consent, and Definitions*.

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 provide the following preliminary comments on the draft regulations in advance of the stakeholder session on the regulation's treatment of publicly available information, "sensitive data inferences," and the treatment of biometrics.

The Regulations Should Tailor the Definition of Publicly Available Information to Protect Valuable Use Cases and Uphold First Amendment Guarantees.

Ensuring a healthy regulatory environment to make productive use of 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 for finding missing children, performing corporate due diligence, preventing money laundering and fraud, and conducting 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 Colorado Privacy Act excludes publicly available information (PAI) from the definition of personal data. That definition encompasses both information that is lawfully obtained from government records, and "any other information that the controller has a reasonable basis to believe the consumer made available to the public." *Id.* We note, however, that the agency may not enforce regulations that are beyond its constitutional power, or that are beyond the power delegated to them in statute. *See* CRS § 24-4-106 (7)(b).

At the outset, we note that the constitutionally protected public domain is greater than that allowed for in the statute. According to the text of section 6-1-1303(17)(b), in order for the information to be PAI, the information has to be released to the public by the consumer. The First Amendment does not permit the government to withdraw information from the public domain. For example, many of our members make available databases of newspaper articles which will contain information about consumers that the consumer did not release. *Florida Star v. B.J.F.*, 491 U.S. 524 (1989).

The draft regulations take this problem into account by excluding news and third-party observations from the definition of information warranting a "reasonable belief," and SIIA commends the Department for that adjustment. Yet further refinements are needed in section 2.02 of the regulations to ensure the regulations comport with the First Amendment and do not undermine socially productive uses of PAI.[1]

First, an inference made from PAI remains PAI but the draft regulations do not reflect this. 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 "John Smith," nor does such an inference violate his expectation when a transaction is cleared. The transfer–and use–of such information remains protected speech.[2] This section of the regulation should therefore be deleted.

Second, SIIA is concerned that the draft regulation's treatment of "combined data" (i.e., "PAI that has been combined with non-publicly available Personal Data") may lead to unintended consequences. The fact that PAI has been commingled with other data does not change its status as PAI: "John Smith" may not exercise rights of deletion or "do not sell" over

[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).

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, while we understand the concerns that could arise involving mixed data, we nonetheless believe that treating combined data as personal data could result in unintended consequences. In the law enforcement context, SIIA members routinely will 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 more organized criminal elements will request that transmission of their Personal data cease or that it be deleted. We therefore suggest that, rather than interfere with these valuable activities, this provision of the regulations be deleted.

The Regulations Should Avoid Unintended Consequences Involving "Sensitive Data Inferences".

We recommend that the Department of Law remove the term "sensitive data inferences," which goes beyond the text of the CPA and, as proposed, will likely generate confusion for businesses and consumers. The definition encompasses "inferences… 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." We believe the concerns animating this definition are already addressed through other defined terms – "sensitive data" and "personal data" – and the term "sensitive data inferences" will be both duplicative and lead to unintended consequences.

For example, applying the proposed definition for "sensitive data inferences," Colorado would consider information suggesting that the Pope is Catholic to be both 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.

In addition to concerns about the interaction of "sensitive data inferences" with PAI, 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. 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, including sensitive data inferences, 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 expectations and it will hamper business compliance and opportunities to bring new products to market, which may use inferential data and data analytics for processing.

The Regulations Should Sharpen the Definition of Biometric Data.

We recommend narrowing the definition of biometric data to encompass strictly automatic measurements of immutable biological characteristics used for identification purposes. The draft regulations define "biometric data" in an overbroad manner that appears to go beyond the authority granted by the enabling statute. The regulations define biometric data as "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."[3] "Biometric identifiers," in turn, are defined as "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 recommend defining "biometric data" in accordance with emerging US state comprehensive privacy laws, such as those in Virginia: namely focusing on immutable characteristics. The definition of "biometric identifier" should be deleted, as its inclusion risks expanding the consent requirements in the downstream process and the stifled practical applications of the 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.

We intend to provide more fulsome comments on these points and other issues raised in the draft regulations in advance of the rulemaking hearing.

Thank you for considering our views.

Respectfully submitted,

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

[3] 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.