January 18, 2023

Mr. Phil Weiser
Attorney General
Colorado Department of Law
1300 Broadway, 10th Floor
Denver, CO 80203

RE: Notice of Proposed Rulemaking – Draft Rules Governing Implementation of the Colorado Privacy Act (Version 2 of Proposed Draft Rules)

Dear Attorney General Weiser:

The Alliance for Automotive Innovation ("Auto Innovators") appreciates the opportunity to provide feedback to the Colorado Department of Law ("Department") on the proposed draft rules implementing the *Colorado Privacy Act*. We appreciate the Department's continued focus on public involvement and transparency and its commitment to developing thoughtful, well-considered rules.

Auto Innovators is the singular, authoritative, and respected voice of the automotive industry. Focused on creating a safe and transformative path for personal mobility, Auto Innovators represents manufacturers of cars and light trucks sold in the United States, original equipment suppliers, technology companies, and others within the automotive ecosystem. The auto industry is the nation's largest manufacturing sector, contributing $1.1 trillion to the United States economy. As a significant engine for our nation's economy, the auto sector is responsible for 10.3 million jobs and $650 billion paychecks annually.

Our comments below largely reiterate our comments to the Department in response to its request for pre-rulemaking feedback. They are intended to highlight some of the unique impacts that the Colorado Privacy Act and its implementing regulations may have on the auto industry and its ability to deliver a cleaner, safer, and smarter transportation future. As the Department continues its work to develop regulations, we continue to urge it to appropriately account for the purpose of data collection and use in different sectors (e.g., where automotive use cases may differ from social media or web-based use cases).

Requirements for Disclosure, Notifications, and Other Communications to Consumers

The proposed rules require in 3.02(A)(3) and 4.04(B)(2) that disclosures and communications sent directly to consumers be sent in the language in which the consumer ordinarily interacts with the controller. While we share the goal of ensuring that privacy-related disclosures and communications are made available in the same languages as other disclosures and communications, the proposed rule appears to be focused on the language that the consumer uses when attempting to interact with the controller rather than the language that the controller uses when interacting with the consumer. For this reason, we suggest

that "in the language in which the Consumer ordinarily interacts with the Controller" be changed to "in the language in which the Controller ordinarily interacts with the Consumer."

The proposed rules also require in 3.02(A)(5) that the disclosures to consumers be readable on all devices through which consumers interact with the controller, including on smaller screens and through mobile applications, if applicable. This language could be interpreted to require that disclosures be made available to consumers through each of the screens present in the vehicle. Many of these screens have not been designed to relay this type of information and, in some cases, may not be able to support such disclosures. For this reason, we suggest that "[r]eadable on all devices through which Consumers interact with the Controller, including on smaller screens and through mobile applications, if applicable" be modified to "[r]eadable on smaller screens and through mobile applications, if applicable."

Right to Opt Out

Section 4.03(A)(1) of the proposed rules would require that a controller cease processing a consumer's personal data as soon as feasibly possible, but no later than *fifteen days* from the date the controller receives an opt-out request. While we are aligned with the Department in wanting to ensure that opt-out requests are processed quickly, we urge the Department to provide at least thirty days to controllers to respond to these requests.

Right of Access

In our prior comments, we noted that much of the data that is generated and collected from vehicles is from onboard computer systems or sensors and relates to the operation and function of the vehicle and its systems. We noted that, because this information frequently contains detailed data elements related to each vehicle system and component over the life of the vehicle, the volume of data that may be responsive to an access request would be vast and likely overwhelming for the consumer. We requested that, if the Department did not allow for controllers to provide a requestor with an accurate description or summary of operational data for a device owned or used by the requestor, a controller be allowed to limit disclosure of such operational data to data generated within the 12 months prior to the access request. We reiterate this request.

The proposed rules require in 4.04(B)(1) and (3) that the specific pieces of data that are provided to a consumer in response to an access request "avoid incomprehensible internal codes." While we appreciate the Department's goals, we are concerned about the significant burden that such a requirement would place on auto companies for some vehicle-generated data. As noted above, much of the data that is generated and collected from vehicles relates to the operation and function of the vehicle and its systems and components. This data, which is frequently transmitted as manufacturer-specific technical codes, has not been standardized across the industry. Any effort to translate this subset of data into a format that would be understandable to consumers or to standardize this data across the industry would be a massive undertaking and take considerable time with little corresponding benefit to consumers. We urge that this requirement be stricken or, at the very least, data related to the operation and function of a device and its systems or components be exempted.

The proposed regulations further specify in 4.04(C) that, in response to an access request, a controller is not required to disclose a consumer's government-issued identification number, financial account

number, health insurance or medical identification number, an account password, security questions and answers, or biometric data. We appreciate the Department's extra efforts to protect particularly sensitive data from disclosure, even in response to an access request. We suggest that the Department also consider adding geolocation information to this list of data that is not required to be disclosed in response to an access request. Vehicle location information is sensitive data and the disclosure of this information to someone who was not in the vehicle at the time that the location information was generated could pose significant privacy and even, in some cases, personal safety risks.

Similarly, in our previous comments, we requested that the Department clarify that a controller is not required to provide access to specific pieces of information if it cannot determine that, in the case of data generated by a device, the consumer was the consumer using the device when the requested data was generated. We reiterate this request and suggest that the Department include a new provision with 4.04 providing that "[a] Controller shall not be required to disclose data generated by a device owned or used by the Consumer if the Controller cannot confirm that the specific data being requested was generated while the consumer was using the device."

Right to Correction

In our previous comments, we recommended that a controller be permitted to deny a consumer's request to correct personal information if the consumer has requested that the same information be corrected multiple times in an abbreviated period of time. We once again recommend that, at a minimum, a controller's obligation to correct inaccurate information be aligned with a controller's obligations to respond to an access request.

Right to Deletion

The proposed regulations require in 4.07 that controllers transfer data to consumers in a way that allows them to "save, edit, and transfer" the data. The underlying statutory text only requires that controllers provide the data in a way that allows the consumer to "transmit" the data to another entity and does not reference an ability to "save" or "edit." We strongly urge the Department to align the regulations with the underlying statutory text and not include an additional "save" or "edit" capability.

Obligations on Controllers

In our prior comments, we expressed concerns with how a universal opt-out mechanism would work in the in-vehicle context. Rather than addressing our concerns, the proposed rules state in 5.08(B) that "[a] Controller shall be capable of recognizing any Universal Opt-Out Mechanism recognized" by Colorado. We continue to believe that applicability of a universal opt-out mechanism to vehicle-generated data is premature and urge the Department to limit applicability at this time to web browsers and other traditional online environments that support existing global opt-out mechanisms.

Required Consent

The proposed regulations include a provision in 7.02(B)(1) that requires consent to process sensitive data collected prior to July 1, 2023. Auto companies may not be able to effectively integrate vehicle platforms that are already in the market today into new data management tools or processes. For this

reason, we urge that any new regulatory requirements be prospective and only apply to data collected after the effective date of the law.

Data Protection Assessments

We appreciate that the proposed regulations incorporate materiality into the requirement to update a data protection assessment and identify a variety of modifications that "may" be considered material changes requiring a data protection assessment update. However, the use of the term "without limitation" in 805(D)(1) is confusing and may inadvertently imply that any of these changes would automatically be considered a "material change." We suggest that the term "without limitation" be removed from the provision.

Finally, we further reiterate the request we made in our prior comments that data protection assessments be submitted to the Attorney General only when requested in conjunction with a relevant investigation or inquiry.

Consumer privacy remains critically important to Auto Innovators and its member companies. We appreciate the opportunity to provide this feedback on the proposed rules and look forward to continuing to work with the Department on this and other privacy-related matters.

Sincerely,

Hilary M. Cain
Vice President
Technology, Innovation, & Mobility Policy