March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

RE: Invitation for Preliminary Comments on Proposed Rulemaking

Dear Mr. Sabo:

The Alliance for Automotive Innovation ("Auto Innovators") appreciates the opportunity to provide feedback to the California Privacy Protection Agency ("Agency") in response to its invitation for preliminary comments on proposed rulemaking relating to automated decisionmaking, cybersecurity audits, and risk assessments.

Auto Innovators represents the manufacturers that produce most of the cars and light trucks sold in the U.S., original equipment suppliers, technology companies, and other value chain partners within the automotive ecosystem. Representing approximately 5 percent of the country's GDP, responsible for supporting 10 million jobs, and driving $1 trillion in annual economic activity, the automotive industry is the nation's largest manufacturing sector.

As this rulemaking addresses novel topics, we respectfully request that the Agency provide sufficient lead time between the finalization of the regulations and the effective date of the regulations. Our member companies take their compliance obligations seriously and need adequate time to align their processes and mechanisms with any new regulatory requirements. To that end, we request that the regulations be finalized at least 12 months before any new obligations or responsibilities take effect. In addition, to ensure sufficient input from stakeholders, we also request that any draft regulations be released for a public comment period of at least 90 days.

Automated Decisionmaking

The term "automated decisionmaking" captures a range of use cases that do not have significant consumer privacy impacts. For example, automated driving systems and other advance vehicle safety systems incorporate artificial intelligence that makes automated decisions about what actions a vehicle will take to safely navigate the driving environment. Proving opt-out rights to disable or reduce the effectiveness of such systems could unintentionally and significantly implicate motor vehicle safety. For example, if a consumer opts out of automated decisionmaking that supports a crash avoidance system, the system may no longer help avoid or mitigate a crash's impact on the driver, passengers, or other road users. The complexity of these vehicle systems also means that it is rarely possible to provide meaningful information to consumers about the logic involved in the decisionmaking process.

For this reason, we recommend that the Agency limit the scope of automated decisionmaking technology covered by the forthcoming regulations to "profiling." If the Agency chooses to cover automated decisionmaking beyond profiling, the Agency should only include decisionmaking technology with significant economic or legal impact for a consumer, such as decisions about educational opportunities, employment, housing, or lending. This would be consistent with other legislation and the White House's Blueprint for an AI Bill of Rights, which applies to automated systems that "have the potential to meaningfully impact individuals' or communities' exercise" of "civil rights, civil liberties, and privacy," "equal opportunities," or "access to critical resources or services." At a minimum, such regulations should not apply to decisionmaking technology onboard vehicles that aids or automates driving functions.

To the maximum extent possible, the Agency should avoid requiring separate and distinct disclosures for various aspects of the CPRA. Any requirements to disclose that automated decisionmaking technologies are in use should be incorporated into the existing disclosure requirements in §1798.110.

Finally, we recommend that any right to request access to specific pieces of information related to automated decisionmaking technologies be limited to personal information. In other words, if the information is not stored by the business in a way that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, it should not be subject to an access request. This limitation would be aligned and entirely consistent with the right to access information in §1798.110 of the CPRA, as well as the general exceptions at 1798.145(j)(1) and (j)(3).

Cybersecurity Audits

We appreciate that the CPRA recognizes that not all processing of personal information presents a significant risk to consumers' privacy or security and only requires an annual cybersecurity audit for the subset of processing activities that pose such a risk. The Agency should focus on processing that involves "sensitive personal information," as defined in §1798.140(ae) when determining what processing presents a significant risk to consumers' privacy and security.

The Agency should take a flexible approach with regards to the content of, and the process for conducting, such audits. Instead, businesses should be able to appropriately tailor their implementation of these audits to the size and complexity of their operations, including the nature and scope of processing activities and expectations of their customers. In addition, the Agency should expressly provide organizations the ability to leverage existing standards and best practices, such as the National Institute of Standards and Technology's Cybersecurity Framework.

Finally, since an audit may reveal sensitive information about an organization's cybersecurity posture which could result in increased risk of a cybersecurity attack if disclosed, the Agency should not require agencies to submit their audits to the Agency. If audits are submitted to the Agency, they should be treated as confidential information with sensitive technical information redacted, subject to applicable privileges and exempt from public disclosure under the Public Records Act.

Risk Assessments

Once again, we appreciate that the CPRA recognizes that not all processing of personal information presents a significant risk to consumers' privacy or security and only requires regular risk assessment for the subset of processing activities that pose such a risk. In determining what processing

presents a significant risk to consumers' privacy and security, we reiterate our support for a focus on processing that involves "sensitive personal information" as defined in §1798.140(ae).

The Agency should refrain from setting out or establishing overly prescriptive requirements as to the content of or process for conducting such risk assessments. Instead, businesses should be provided flexibility in implementing these assessment requirements so that they can be appropriately tailored to their size and complexity, including the nature and scope of processing activities and expectations of customers.

We also discourage the Agency from specifying a regular cadence for risk assessments. If the Agency seeks to establish a trigger for risk assessments, the Agency should consider requiring businesses to update their risk assessment when there is a material change in their processing activities that is likely to have an impact on consumer privacy. Moreover, in determining when such risk assessments should be submitted to the Agency, we encourage the Agency to carefully balance the value of such submissions against the burden that such submissions may impose on businesses and the Agency. Rather than requiring every relevant business in California to periodically submit risk assessments to the Agency, the Agency should consider limiting risk assessment submissions to those requested by the Agency in conjunction with a relevant investigation or inquiry.

We appreciate the opportunity to provide input on this rulemaking and look forward to further engagement with the Agency on these important topics.

Sincerely,

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