November 8, 2021

SUBMITTED ELECTRONICALLY VIA EMAIL

Debra Castanon
California Privacy Protection Agency
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

Re: Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)

Dear Ms. Castanon:

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 under the *California Privacy Rights Act* ("CPRA"). We certainly share your goals of protecting consumer privacy and look forward to continued engagement and collaboration with you on these important issues.

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 the manufacturers that produce nearly 99 percent of cars and light trucks sold in the United States. In addition to motor vehicle manufacturers, members of Auto Innovators include 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 and representing 5.5 percent of the country's GDP. As a significant engine for our nation's economy, the auto sector is responsible for 10.3 million jobs and $650 billion in paychecks annually.

Our member companies are committed to protecting consumer privacy and have long been responsible stewards of their customers' information. In fact, in 2014, the auto industry came together to develop the *Privacy Principles for Vehicle Technologies and Services*. The Principles are enforceable by the Federal Trade Commission and represent a proactive and unified commitment by automakers to protect identifiable information collected through in-vehicle technologies. They distinguish the auto industry from other industries as one that is dedicated to safeguarding consumer privacy.

While we appreciate the goal of creating a uniform and inclusive privacy law, we also recognize that consumer privacy is not a one-size-fits-all proposition. We continue to believe that comprehensive consumer privacy laws should account for the significant variation that exists among sectors and the implications that such variation has on consumer privacy. Our comments below highlight the unique

impacts that the CPRA and its implementing regulations may have on the auto industry and its ability to deliver a cleaner, safer, and smarter transportation future.[1]

As the Agency embarks on this important and consequential rulemaking, we respectfully request that sufficient lead time be provided 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.

Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses

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 and 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 suggest that the Agency focus on processing that involves "sensitive personal information" as defined in §1798.140(ae).

The Agency should not set out or establish overly prescriptive requirements as to the content of or process for conducting such audits or assessments. Instead, businesses should be provided flexibility in implementing these audit and assessment requirements to appropriately tailor them to their size and complexity, including the nature and scope of processing activities and expectations of customers. In addition, businesses should be expressly permitted to rely on and leverage well-respected and applicable standards and best practices, such as the National Institute of Standards and Technology's Cybersecurity Framework, with respect to any cybersecurity audit requirement.

We also discourage the Agency from specifying a regular cadence for the risk assessments. If the Agency seeks to establish a trigger for the 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.

As you are aware, the CPRA does not require cybersecurity audits to be submitted to the Agency. Since a cybersecurity audit may reveal sensitive information about how a business defends itself against

[1] The auto industry joins other sectors in expressing practical concerns with some other aspects of the CPRA. This includes the expiration of the exemption for applicant, employee, and independent contractor data and the removal of the opportunity for a business to cure an alleged violation before an administrative enforcement action can be brought. These concerns can, and should, be addressed in a way that furthers the purpose and intent of the CPRA and look forward to working with the Agency and other policymakers in California to that end.

a potential cybersecurity attack and such information – if disclosed – could expose the business to an increased risk of attack, this is the appropriate approach.

In the instance that an assessment or audit is provided to or shared with the Agency, the assessment or audit itself and any proprietary information contained within it or reviewed in conjunction with it must be treated as confidential information. This includes ensuring that audits are exempt from disclosure to the public under the Public Records Act.

Automated Decisionmaking

On its own, the term "automated decisionmaking technology" captures a broad range of use cases, including use cases that do not have significant impacts on consumer privacy. For example, the artificial intelligence that underpins automated driving systems and other advanced safety systems continuously make automated decisions about what actions the vehicle will take to safely respond to and navigate the driving environment. Disabling or reducing the effectiveness of these systems by providing opt-out rights could have significant and unintended motor vehicle safety implications. For example, if a consumer opts out of automated decisionmaking that supports a crash avoidance system, that system will no longer be available to help avoid or mitigate the impact of a crash. Moreover, in the case of this type of complex machine-learning system, it is rarely possible to provide meaningful information to consumers about the logic involved in the decisionmaking processes.

As you are aware, CPRA specifically mentions "profiling" as an area of automated decisionmaking technology to be addressed by regulations. We recommend that the Agency limit the scope of automated decisionmaking technology covered by the regulations to profiling. If the Agency opts to include automated decisionmaking technology beyond profiling in the regulation, the Agency should consider broadening its applicability to only include decisionmaking technology with significant economic or legal impact for a consumer, such as decisions about housing, lending, educational opportunities, or employment.

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

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.

Consumers Right to Delete, Right to Correct, and Right to Know

Auto Innovators acknowledges the interest in providing consumers with a right to correct inaccurate personal information. We continue, however, to have concerns about how this right can be effectively exercised in some contexts, including with respect to vehicle-generated data. Some of the data that is collected from vehicles is data generated by vehicle systems and components, including sensors. An accuracy challenge from a consumer related to this type of vehicle data is likely to create unnecessary and unresolvable challenges for vehicle or component manufacturers.

To that end, we suggest that the Agency limit the right to request correction of personal information that has been provided directly by the consumer to the business in order to receive services. We also recommend that the Agency allow businesses to deny a consumer's request to correct personal information if the consumer fails to provide sufficient information to investigate the accuracy of the challenged personal information or when the business has reason to believe that the personal information is accurate. Moreover, we recommend that the Agency clarify that a business is not required to correct information that it has received from a third party. In these cases, the business should be permitted to refer the consumer to the third party from which it received the personal information for correction.

The Agency should set out reasonable limitations on the frequency with which a consumer can request that personal information be corrected. For example, the Agency should allow businesses 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. At a minimum, a business's obligation to correct inaccurate information should be aligned with a business's disclosure obligations under §798.130(b).

Consumers' Right to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information

Unlike a mobile phone or a social media account, vehicles are often used by individuals other than the vehicle owner (e.g., a spouse, family member, friend or neighbor, rental car customer, etc.). In almost all cases, an auto company does not know which consumer is using a particular vehicle at a particular point in time and would therefore not know when to honor a consumer's opt-out preference. As it is unclear how a global opt-out preference signal would work or translate effectively to the vehicle environment, it is premature for the Agency to require that all businesses accept a global opt-out preference signal. As CPRA provides other mechanisms by which consumers can effectively exercise their opt out rights, the Agency can take additional time to consider the broad implications of requiring all businesses, including those within the auto industry, to accept a global opt-out preference signal.

Information to be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)

Much of the data that is generated and collected from vehicles is from onboard computer systems and sensors and relates to the operation and function of the vehicle and its systems. This data is very technical in nature and is of little use to the average consumer. In addition, this information frequently contains detailed data elements related to each vehicle system and component over the life of the vehicle. Since the average life of a vehicle is nearly 12 years, the volume of the data that may be responsive to a request for specific pieces of information would be vast and likely overwhelming for the consumer. For this reason, the Agency should deem disclosure of operational data for a device owned or used by a consumer beyond the 12-month window as involving a disproportionate effort. In addition, the Agency should consider permitting a business to deny a consumer's request if the consumer requests the same information multiple times.

As noted above, in most cases, an auto company does not know which consumer is driving a particular vehicle at a particular point in time. As a result, an auto company is generally unable to associate specific vehicle data with a person who was driving the vehicle when that vehicle data was generated. This poses significant, practical challenges for auto companies with respect to consumer requests for access to vehicle data and creates the potential for significant harm to consumers. For example, the sharing

of vehicle geolocation data with a consumer who was not using the vehicle at the time the geolocation data was generated may create privacy or even safety risks (e.g., an abusive individual seeking information about where his or her spouse has driven a vehicle.) For this reason, we urge the Agency to specifically confirm that a business is not required to provide access to specific pieces of personal information if it cannot verify that the personal information being requested relates specifically to that consumer or, in the case of data generated by a device, that the consumer was the consumer using the device when the requested personal data was generated.

Consumer privacy remains critically important to our member companies. We appreciate the opportunity to provide this feedback and input and look forward to continuing to work with the Agency on this and other privacy-related matters.

Sincerely,

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