ALLIANCE FOR AUTOMOTIVE INNOVATION

April 19, 2024

Mr. Matthew G. Olsen
Assistant Attorney General for National Security
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Assistant Attorney General Olsen:

The Alliance for Automotive Innovation ("Auto Innovators") appreciates the opportunity to provide input to the Department of Justice ("Department") on its advance notice of proposed rulemaking ("ANPRM") on *Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern*. We welcome the opportunity to provide the perspective of the auto industry.

Auto Innovators represents the manufacturers that produce most of the cars and light trucks sold in the U.S., original equipment suppliers, battery makers, 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 growth, the automotive industry is the nation's largest manufacturing sector.

Our member companies remain fully committed to U.S. national security. To this end, we share the goals of the ANPRM and appreciate the important role that the Department has in countering the threat to U.S. national security posed by the efforts of certain countries to access and exploit Americans' bulk sensitive personal data.

At the same time, the automotive industry is undergoing a once-in-a-century transformation to cleaner, safer, and smarter vehicles that has the potential to bring many societal, economic, and safety benefits to U.S. consumers and road users. This transformation to automated, electrified, and connected vehicles is largely enabled by and through the collection and use of vehicle data. For example, data from onboard computer systems and sensors may be collected to help a manufacturer identify potential warranty, repair, and related issues, including those that may raise safety issues and require a safety recall. Auto companies may also collect vehicle data as part of their efforts to develop and improve cutting-edge vehicle safety systems. These systems include, but are not limited to, emerging crash avoidance and automated safety features, driver engagement and medical emergency monitoring, and driver impairment detection features. The ability of auto companies to develop and provide these safety systems depends on access to vehicle data.

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* ("Principles").[1] The Principles represent a proactive and unified commitment by automakers to protect identifiable information collected through in-vehicle technologies and distinguish the auto industry from other industries as one dedicated to safeguarding consumer privacy. In particular, the Principles establish a set of baseline privacy protections related to the collection and use of vehicle data. They contain significant commitments from automakers related to transparency, choice, respect for context, data minimization, data security, integrity, and accountability. This includes specific obligations to:

- provide consumers with ready access to clear, meaningful notices about the collection, use, and sharing of identifiable information;
- obtain affirmative consent before using sensitive information for marketing purposes or before sharing sensitive information with unaffiliated third parties;
- use and share identifiable information only in ways that are consistent with the context in which the information was collected;
- collect and retain identifiable information only as needed for legitimate business purposes; and
- implement reasonable measures to protect identifiable information against loss and unauthorized access or use.

The ability of auto companies to continue to support and enhance vehicle safety for U.S. drivers, passengers, and road users must be preserved. For that reason, any proposed restrictions on the collection, use, or sharing of vehicle data should be carefully balanced against the need to collect, use, or share vehicle data for these safety-related purposes. We appreciate the thoughtfulness of the approach outlined by the Department in the ANPRM and the clear attempt to strike this crucial balance. In particular, the proposal's important distinction between prohibited transactions and restricted transactions helps to ensure that the riskiest transactions are eliminated and the risks associated with other transactions are appropriately mitigated and managed.

As the Department continues its work on this consequential rulemaking, Auto Innovators provides the following observations and recommendations:

- **VENDOR AGREEMENTS**: The inclusion of vendor agreement transactions as a restricted transaction may create some challenges for auto companies that may use a component supplier from a country of concern. Auto manufacturers may need to share some vehicle data related to the operation of a component with the supplier of the component for testing, validation, and quality control purposes. In these cases, for safety purposes, vehicle data is often linked with a particular vehicle identification number or device identifier. These numbers are unique to a particular vehicle and may be considered a "listed identifier"

[1] https://www.automotiveprivacy.com

under the ANPRM and therefore subject to the restricted transaction provisions.

To address these situations, the Department should exclude "device-based or hardware-based identifiers" from the list of listed identifiers considered to be "sensitive personal data" under the ANPRM. Device-based or hardware-based identifiers should not be considered sensitive personal data on their own, but only when combined with other categories of sensitive personal data or other listed identifiers included in the ANPRM. If the Department maintains "device-based or hardware-based identifiers" in the list of listed identifiers, it should consider excluding operational or performance data related to a device component from the definition of a vendor agreement for purposes of what is a restricted transaction, so long as no additional sensitive data is shared as part of the transaction.

- **DATA BROKERS:** Auto Innovators is generally supportive of the Department's proposal to prohibit data brokerage transactions involving bulk U.S. sensitive data to countries of concern. However, Auto Innovators is concerned that the proposed definition of "data brokerage" may be too broad and may inadvertently capture a broader collection of transactions than the Department intends. To this end, the Department should consider aligning its definition of data broker with definitions included in a number of relevant state data broker laws (including California) by focusing on whether the U.S. entity has a direct relationship to the individuals to whom the data pertains, rather than on whether the recipient collected or processed the data directly from individuals linked or linkable to that data. Alternatively, the Department should consider exempting from the definition of data brokerage the transfer of data to: (a) a subsidiary or affiliate of a U.S. company; (b) an entity supplying components or parts to the U.S. entity if the data relates to the supplied components or parts; or (c) a third party for purposes of providing a product or service requested by a U.S. person.

- **SECURITY REQUIREMENTS:** While the specific security requirements identified in the ANPRM are widely respected by industry stakeholders, the Department should instead consider providing some flexibility to entities to identify and determine the reasonable and appropriate security frameworks or standards for the entity's industry, the covered data being transferred, and the specific restricted transaction. For example, the National Highway Traffic Safety Administration has issued cybersecurity best practices that may be relevant and appropriate to restricted transactions involving vehicle data. We suggest that the Department provide appropriate flexibility to implement sector-specific standards that are comparable to those specified in the ANPRM.

- **COVERED PERSONS:** The Department should reconsider the ANPRM's proposal to include within the definition of "covered person" any "foreign person who is primarily resident in the territorial jurisdiction of a country of concern." We support the Department's proposal that it develop a public list of covered persons and understand that the public list would serve as a supplement to the defined categories in the definition of covered person. However, we propose that a "foreign person who is primarily resident in the territorial

jurisdiction of country of concern" be considered a "covered person" only if that person is: (a) identified on the public list; or (b) an employee or contractor of a country of concern or of an entity otherwise covered by the definition of covered person.

- **PROPOSED EXEMPTIONS:** The ANPRM's proposal to exempt certain classes of data transactions from coverage is appropriate. In particular, the exemption for intra-entity transactions is important and should be preserved. The Department should consider expanding the exemption to cover all regular intra-entity business transactions, rather than only those transactions that are "incident to business operations." Auto companies operate and sell their products globally, including in countries of concern, and need to be able to share relevant data with subsidiaries and operational units throughout the world.

- **LICENSES:** Auto Innovators strongly supports the proposal in the ANPRM to provide the Department with the ability to issue licenses to entities authorizing covered data transactions that would otherwise be prohibited or restricted. An unprecedented rulemaking such as this has the potential for unintended consequences not anticipated at this stage of the rulemaking. Providing an avenue for the Department to issue licenses in these and other situations is appropriate to accommodate these unintended and unanticipated consequences.

- **INTEPRETITIVE GUIDANCE:** Auto Innovators fully anticipates that, as the Department and entities implement these regulations, areas of ambiguity and challenge will surface. To help entities successfully navigate these ambiguities and challenges, Auto Innovators strongly supports the creation of a program to provide guidance in the form of written advisory opinions so that entities can request an interpretation of any part of the regulations from the Attorney General. As anticipated by the ANPRM, we believe that entities will find such interpretive guidance to be helpful when considering whether a particular transaction is a covered transaction, whether the Attorney General would be likely to issue a license governing a particular data transaction, and whether a person satisfies the definitions of the regulations.

- **DATA CONTROLLER:** The Department should make clear that the rule's requirements only apply to U.S. persons that have or maintain control over the bulk U.S. sensitive data involved in a prohibited or restricted transaction. For example, an automaker should not have compliance obligations with respect to U.S. bulk sensitive data transferred via an aftermarket device from a country of concern that is installed in a large fleet of vehicles by the owner of that fleet. In this type of instance, the compliance obligations should rest entirely with the fleet owner or the manufacturer of the aftermarket device as the controller of the data.

- **COMPLIANCE:** As anticipated by the ANPRM, there is the potential for significant compliance obligations and burdens - including due diligence, record-keeping, and reporting requirements - on entities that engage in a restricted transaction or as a condition of a general or specific license. We appreciate that the Department has attempted to target

record-keeping or reporting requirements to certain situations. However, in identifying "certain narrow circumstances to identify attempts to engage in prohibited covered data transactions," the Department notes that it is considering reporting requirements to identify covered data transactions that are "the highest priority for ongoing compliance and enforcement efforts" and suggests that this could include "[a]ny U.S. person that has received and affirmatively rejected an offer from another person to engage in a prohibited covered data transaction involving data brokerage." While we appreciate the Department's interest in tracking these sorts of offers, we are concerned that the requirement places reporting requirements and compliance burdens on entities that are not engaged in – and, in fact, have affirmatively rejected – a covered data transaction.

In addition, the "know your vendor" and "know your customer" due diligence and record-keeping requirements suggested in the ANPRM are likely to place new – and potentially significant – compliance burdens on entities. The Department should be thoughtful and deliberate about these requirements and carefully consider opportunities to minimize such burdens.

- **EFFECTIVE DATE:** Auto Innovators appreciates the Department's clarification that the program would not apply retroactively before the effective date of the regulations. Since entities will need to develop new processes and mechanisms to ensure compliance with the final regulations, Auto Innovators proposes that the Department also provide sufficient lead time to entities between the publication of the final rule and the effective date of the final rule to effectuate those new processes and mechanisms.

- **ECONOMIC IMPACT:** Finally, the ANPRM correctly identifies the primary economic impacts of the rulemaking in terms of direct and indirect costs. With respect to direct costs, the ANPRM correctly acknowledges that – faced with higher cost associated with executing a vendor agreement with a vendor based in a country of concern – a U.S. company may opt to drop its contract with that vendor and instead rely on a vendor based outside of a country of concern. As the ANPRM points out, this could represent a financial loss to the U.S. company which could now face a higher cost for the good or service.

  However, the Department should consider potential additional costs associated with the possibility of a U.S. company having to contract with a vendor for a lower quality or lower performing component than what may be available through a vendor in a country of concern. For example, if an auto manufacturer is unable to share component-related operational data with the supplier of a particular component located in a country of concern, the auto manufacturer may be forced to contract with another supplier outside a country of concern for that component. If the component from the country of concern is of higher quality or higher performance than the component for which the auto manufacturer is forced to contract, there may be potential impacts on the sale price of the vehicle with the lower quality or lower performing component. In this situation, there may be an additional financial impact to the auto manufacturer resulting from the vehicle's lower sales price.

We very much appreciate the opportunity to provide the automotive industry's perspective on the ANPRM. We look forward to further engagement with the Department on this important topic.

Sincerely,

Hilary M. Cain
Senior Vice President, Policy