Statement for the Record
Damon Shelby Porter
Director, State Government Affairs
Association of Global Automakers, Inc.

Before the California Senate Committees on Judiciary and Transportation and Housing in a Joint Hearing to Receive Remarks for Informational Purposes on Automobile Data Collection and Privacy Protection

March 15, 2016

Senators Jackson and Beall and members of both the Senate Committee on Judiciary and Senate Committee on Transportation and Housing, thank you for holding a hearing to receive remarks for informational purposes on automobile data collection. For the record, my name is Damon Porter; I am the Director of State Government Affairs for the Association of Global Automakers. I am joined today by the Honorable David Strickland, former Administrator of the National Highway Traffic Safety Administration (NHTSA), who is present to answer any technical or substantive questions members may have at the conclusion of my statement.

The Association of Global Automakers, Inc. (Global Automakers) represents international automobile manufacturers that design, build, and sell cars and light trucks in the United States. These companies have invested $4.3 billion in California based facilities, directly employ more than 11,000 Californians and sell 57% of the new motor

vehicles and 79% of the green vehicles sold in the Golden State. Combined, our member companies operate more than 95 production, design, research and development, sales, finance and other facilities, as well as North American headquarters, in California.

Global Automakers and our member companies are committed to creating the safest, cleanest and most technologically advanced vehicles on the road. Vehicles in the marketplace today offer an increasing amount of innovative technologies that make the driving experience safer, more environmentally responsible and certainly, more enjoyable. We look to a time, in the very near future, where these active technologies will save more lives, increase mobility and move us toward sustainable transportation systems.

The level and complexity of technology in automobiles continues to grow. As automakers manufacture vehicles incorporating more advanced technologies and these vehicles become more connected, privacy and cybersecurity concerns emerge. Global Automakers and its member companies recognize these concerns and have been taking proactive measures to address them.

GlobalAutomakers

We are pleased that California has presented us with an opportunity to discuss the important subject of vehicle data collection and privacy protection. Global Automakers works with industry leaders, legislators, regulators and other stakeholders in the United States on these issues. Our goal in California, and elsewhere, is to create public policy that improves motor vehicle safety, encourages technological innovation, and protects our planet. It is important for members of the California State Legislature to understand how and why automobiles collect, use, and in some instances, share data generated by the vehicle.

What data is collected by today's automobiles?

Today's new vehicles contain innovative technologies that deliver substantial benefits for consumers by greatly enhancing the safety, performance, and environmental impact of the vehicle, while providing navigation and other valuable information services, theft protection, and diagnostic capabilities.

These technologies rely on various types of data generated by the vehicle. Most of this data is **not** personally identifiable, that is, the information is not linked or linkable either to the vehicle from which the information was retrieved or the vehicle owner.

GlobalAutomakers

Personally identifiable information includes **geolocation, biometric, and driver behavior information.**

I would like to give a few real world examples of what information is being collected in vehicles, where such services are available, and what are the benefits:

1. Geolocation data is necessary for navigation. It also can save lives in the event of a crash by transmitting location data to emergency responders or roadside assistance providers to quickly aid victims in need. As we all know, the "golden hour" is critical for survivability in the event of a crash. The sooner we can get first responders to the scene, the more quickly they will be able to triage the situation.
2. Biometric data can be used to monitor a driver's eyes to gauge fatigue and sound an alarm if he or she falls asleep.
3. Driver behavior data measures speed, braking, and other performance data points critical to enabling advanced traction and cruise control, anti-lock brakes, advanced airbags, and other onboard diagnostics.

GlobalAutomakers

One of the most exciting developments is connected vehicles—vehicles that talk to each other, the infrastructure, and even your mobile device. This life saving capability requires data. Connected vehicles are expected to revolutionize highway safety and potentially save thousands of lives per year by avoiding crashes. Vehicle to vehicle technology, or V2V, allows connected vehicles to wirelessly communicate with each other to warn drivers of possible dangers. The National Highway Traffic Safety Administration (NHTSA) has initiated rulemaking that would **require** new vehicles to be equipped with this safety technology, and the industry is working collaboratively to plan for the successful deployment of connected cars.

We recognize that this connectivity and technology can create potential risk. It is impossible to talk about the need to protect the privacy of vehicle data without addressing cybersecurity. To that end, automakers have established an Automotive Information Sharing and Analysis Center (Auto ISAC) to proactively share information on vulnerabilities and cyber threats across the industry. This is an unprecedented step by any industry, proactively organizing ourselves well before any incident or regulatory pressure. We also are in the process of developing cybersecurity best practices to ensure that as vehicles become more connected, the security of vehicle data and vehicle owners

is protected. The industry took these steps because we realize how important it is to get cybersecurity right, especially with new technologies.

One of the most significant auto cybersecurity vulnerabilities results from unfettered access to vehicle computer systems. Global Automakers and its members strongly support a consumers' right to have their vehicles repaired at the repairer of their choice. In this spirit, all of the major automakers selling vehicles in the United States have entered into a Memorandum of Understanding agreeing to provide access in all 50 states to service, diagnostic, and repair information and tools necessary to service a vehicle, the same as any franchised auto dealers. This includes the ability to electronically diagnose vehicles by accessing onboard diagnostic data stored on the vehicle. At the same time, the industry approach to providing service information to the aftermarket must also recognize the need to protect consumers from third parties that would use vehicle data to hack into the computer systems on their vehicles. Automakers already provide as much information as possible for repair purposes while still maintaining and protecting the integrity of the in-vehicle software. That said, we are aware that some aftermarket parts suppliers and insurance companies have been lobbying policymakers to require automakers to disclose more and more information about proprietary systems behind the

firewall. This issue clearly highlights the importance of balancing access to information such as software used to repair a vehicle, with the need to maintain the security of critical vehicle systems.

Finally, there are certain misconceptions about the ways in which vehicles are collecting and using data that I would like to dispel—most notably, event data recorders or EDRs. EDRs are sometimes likened to "black boxes" in airplanes but this is not accurate. EDRs are programmed generally to record in a continuous loop, writing over information again and again until a vehicle is in a front-end collision or other crash. When a crash with a strong enough impact occurs, the device automatically saves up to 5 seconds of data from immediately before, during, and after an incident.

Based on federal regulations, if a vehicle does have an EDR, it must track 15 specific data points, including speed, steering, braking, acceleration, seatbelt use, and, in the event of a crash, force of impact and whether airbags deployed. In most states, including California, and now under federal law, EDR data is explicitly deemed the property of the vehicle owners and cannot be accessed except: (1) with the owner's consent; (2) a court

order; (3) for vehicle safety research; or (4) when diagnosing, servicing, or repairing the vehicle.

Let me close by saying that the automotive industry continues to develop innovative technologies and services that promise to deliver substantial benefits to the environment and enhance the driving experience. Many of these technologies and services are based upon data generated and collected from a variety of vehicle systems. **Consumer trust is essential.**

Mr. Tobin, representing the Alliance of Automobile Manufacturers, will now explain how the industry has created and is implementing "Privacy Principles" which we believe will give consumers the peace of mind to know that their personal data is not being used for marketing or other monetization without their consent. Thank you, again, for the opportunity to speak and Global Automakers looks forward to working with you on this issue.

- END -