Frequently Asked Questions (FAQs) on Automotive Privacy

---

1. **Why did the auto industry develop Privacy Principles for vehicles?**

   Automakers take great pride in providing our customers with safe, reliable products, including data privacy and data security. The Privacy Principles acknowledge that technologies and services in automobiles are increasingly designed to enhance vehicle safety, improve vehicle performance and augment the driving experience, and many of these technologies and services rely upon information generated by vehicle systems. Sometimes, that information includes the precise location of vehicles or how drivers operate their vehicles. The Principles represent a unified commitment to responsible stewardship of the information collected to provide vehicle services.

2. **What are these technologies and services, and why are they useful?**

   As new vehicle technologies and services emerge, the goal of automakers is to continue enhancing benefits to customers while respecting their privacy. Technologies and services available today enable greater road safety through connectivity. Automatic crash notification calls help assist vehicle occupants when needed. Alerts about traffic conditions help reduce congestion. Electronic security or smartphone applications help locate lost or stolen vehicles. These features and more are important to automotive customers, and providing them in a transparent way is important to automakers.

3. **How do the Privacy Principles compare to efforts in other industries and government?**

   Automakers are among the first industries to develop Privacy Principles to address consumer concerns about what data we collect, how we use it, and when/why data is shared. These Privacy Principles have a strong lineage, building on Fair Information Practice Principles, Federal Trade Commission (FTC) guidance, the White House Consumer Privacy Bill of Rights and the guidance of privacy advocates.

4. **What should consumers do to stay informed about their privacy in automobiles?**

   First, check with the automaker: Within a vehicle, internal computers are constantly communicating with each other to operate the vehicle, and automakers work hard to safeguard this in-vehicle computer network to preserve the integrity of safety critical systems. However, not all data needed to operate a vehicle is stored or transmitted. Privacy policies associated with the vehicle system are available to consumers, and automakers encourage their customers to review them. Automakers may provide customer notices through a variety of methods, including online, owner's manuals, paper or electronic registration forms and user agreements, and/or in-vehicle displays. Consumers will also find information on how to delete certain data they stored on their vehicles.

   Second, always ask about privacy policies and practices of relevant providers, including:

- **Wireless carriers:** Many of our customers pair their mobile devices with vehicle-integrated systems, so we urge customers to check the privacy policies of their wireless carriers prior to pairing their device.
- **Mobile app providers:** When customers pair their mobile devices with vehicle systems, they may access mobile apps and websites that have their own policies for customer review.

Third, always ask who wants vehicle data and why: Many data miners, retailers and service providers want access to consumer vehicle data. For example, insurance companies seek access to vehicle data for setting individual premium rates. Some insurance companies only want mileage driven per year, while others may want much more information, such as driving behaviors like hard braking and accelerations, or even GPS locations of travel. The FTC and White House have raised concerns about discriminatory "redlining" services, the practice of denying services or charging more for them for particular groups based on race, sex or where people live and travel. Consumers are rightly concerned about sharing vehicle data with a company that may share that information with business affiliates for any number of reasons, including sales and marketing. This could potentially allow many people to access consumer vehicle data without prior authorization. Several states have passed laws limiting the extent to which insurers can require consumers to allow access to their vehicle data. Under the automotive Privacy Principles, consumers must consent to providing insurers with vehicle data.

5. What types of information are generated, transmitted, retained, or shared in an auto today?

Today, different types of data are generated, transmitted, retained or shared for different purposes:

Data generated in an auto, but not transmitted outside the vehicle, that is necessary for the operation of the vehicle: Within a car, computer systems constantly exchange data to ensure the smooth operation of the vehicle. From steering to braking, crash avoidance, and acceleration, dozens of onboard computers simultaneously share information as consumers travel down the highway. This data is not transmitted outside, or retained in the long-term computer memory, of the vehicle -- unless it is part of a subscription service, in which case owner consent is required under the Principles.

Data transmitted outside of the vehicle: Certain functions can require the transmission of data outside the vehicle. For example, automatic crash notification systems transmit data so that emergency responders can be directed to crash scenes with information on the nature of the crash. Diagnostics systems may transmit data outside the car to identify potential maintenance issues.

Data transmitted into and out of the vehicle: While basic navigation systems are only receivers for directions coming into the car, enhanced navigation systems both transmit and receive data from outside the vehicle so drivers can learn about traffic conditions and get directions. Trip information may be retained for convenient access to previously accessed destinations. For greater convenience, vehicles can also transmit and receive data so consumers can remotely monitor where their car is, remotely start their car, obtain vehicle diagnostics reports and access on-board information services.

Data generation that is required by law: Certain vehicle data is required by law, such as data pertaining to emissions controls, on-board tire pressure sensors, and gauges. The government requires that event data recorders (also known as "EDRs") monitor critical information about the vehicles in which they are installed, but this information is only stored for seconds at a time and constantly overwritten -- unless there is a crash and then the data (immediately prior to and after the crash) is recorded for use in analyzing the performance of the vehicle's safety systems.

Data that is shared: Technical data regarding such matters as warranty or safety is shared with authorized dealers, who also share this information with automakers. Some information may also be shared for marketing purposes, but only with express, affirmative consent by the vehicle owner or registered user.

6. What data does a consumer own or control in an automobile?

Increased Internet use and smartphones have raised many questions about data and ownership. For instance, a consumer owns a smartphone but not the proprietary system and data that make the smartphone work. As autos evolved into complex computer systems that generate, store and analyze data, similar questions arose about data ownership related to vehicles. Here are the answers:

- **EDR data:** Automakers affirm they obtain vehicle owner consent in order to retrieve EDR data.
- **Infotainment data:** Consumers can control the type of information they enter into the infotainment system, such as music and contact lists.
- **Personal subscription information:** Consumers can control identifying information, including name, address, credit card numbers, telephone numbers and email addresses.
- **Technical data:** Automakers reserve the right to use technical data that is stored in, and relates to the functioning of, the vehicle.

7. What data can consumers review?

Data from contract or subscription-based services: Some vehicle systems and third-party providers allow vehicle owners and registered users to access historical data from a variety of subscription-based services, including roadside assistance, navigation, automatic crash notification, entertainment, and concierge services.

Data from in-vehicle diagnostics: Some data may be accessed by consumers via password-protected websites, report emails, and mobile applications, as well as on-board reporting systems or embedded touch screens. This data includes diagnostics and vehicle information on emissions controls, tire pressure, oil life, upcoming service needs and brake life. Driver behavior information can include vehicle speed, safety belt use and information about braking habits.

8. Why can't consumers access all the data generated in an automobile?

Consumer privacy and safety may be threatened or corrupted when unauthorized individuals access certain vehicle information. That is why it is important to safeguard vehicle information. There are also practical considerations. A home computer has an operating system comprised of millions of lines of codes that are not meaningful to most users. Likewise, a vehicle processes

substantial amounts of data necessary for its functioning but not associated with the owner or registered user.

9. Can a consumer decide to turn off the information flow within a vehicle?

On home computers or smartphones, consumers can tell online advertisers and retailers that they want to avoid "tracking cookies" that retain Internet browsing information. By contrast, automobiles rely on the on-board network of computers to function, and these systems cannot be turned off and still allow the vehicle to operate. However, vehicle owners and registered users have access to a variety of subscription-based services offered by manufacturers and third-party providers. Owners and lessees can opt out of subscription-based services or choose not to contract with certain vendors who seek access to various types of data.

10. Can consumers decide which third parties receive their data?

In many instances, consumers have a choice. For instance, owners and registered users can direct vehicle health reports and forward emails to their repairer of choice**.** If data is collected or transmitted by an automaker or third party, owners and registered users are informed of the collection of required data either at the point of sale or at the point of lease via the owner's manual or through various service subscriptions upon registration or contract. Data is not tracked or shared without such disclosure. Examples of the types of data that consumers can share with third parties include:

- Information necessary to diagnose and repair vehicles.
- Vehicle "health data" such as emissions controls, tire pressure, oil life.
- Driver behavior information such as average speed or engine throttle.
- Subscription-based information and service options such as geolocation, navigation, automatic crash notification, and road-side assistance.

11. How do automakers address sensitive personal consumer information?

The most sensitive types of consumer information relate to geolocation (where the vehicle goes), driver behavior (such as vehicle speed or use of safety belts) and biometrics (physical or biological characteristics that identify a person). For each of these categories, the Privacy Principles require clear and prominent notices about the collection of such information, the purposes for which it is collected, and the types of entities with which the information may be shared.

12. Who has agreed to these Principles?

A list of automakers that have signed onto the Consumer Privacy Principles may be found at www.AutomotivePrivacy.com. When participating automakers work with third-party service providers, automakers commit to taking steps to ensure that these providers adhere to the Principles as well. Regarding automobile dealers, they are franchisees and independent businesses not controlled by automakers, and thus the Privacy Principles do not apply directly to dealers. However, automakers and their dealers have been working together to protect customer privacy and will work to implement the Principles, as well as ensure that customer information is protected throughout the vehicle purchase and ownership periods.

13. When do these Principles go into effect?

Participating automakers commit to meet or exceed the commitments contained in the Principles for new vehicles manufactured no later than Model Year 2017 (which may begin as early as January 2, 2016), and for Vehicle Technologies and Services subscriptions initiated or renewed on or after January 2, 2016. While adherence to the Principles does not require engineering changes in vehicles, if automakers make engineering changes they agree to comply no later than Model Year 2018.

14. To whom are automakers accountable?

Participating automakers agree to meet or exceed these Privacy Principles. By publicly committing to this set of Privacy Principles, participating members become accountable not only to their customers, but also to state and federal regulators.

15. What else are automakers doing to enhance privacy and data security?

Privacy is a priority for all automakers. As vehicles become increasingly interconnected, both data protection and data privacy need to be considered from the earliest stages of product development; in other words, "Privacy is by Design." All automakers today have technical and organizational security measures in place to protect customer data against manipulation, loss, destruction and access by unauthorized parties. And, automakers are working to establish a voluntary automobile industry sector information sharing and analysis center or comparable program for collecting and sharing information about existing or potential cyber-related threats and vulnerabilities in motor vehicle electronics or associated in-vehicle networks.