# GLOBAL AUTOMAKERS
# FREQUENTLY ASKED QUESTIONS
# CONSUMER PRIVACY PROTECTION PRINCIPLES

## 1. Why is the auto industry making a commitment to protect the privacy of our customers?

Global Automakers and its member companies recently unveiled auto industry consumer privacy protection principles for vehicle technologies and services (Principles). The Principles acknowledge that the connected car, and the associated technologies and services, involves the collection of data to enhance vehicle safety, improve vehicle performance, comply with environmental requirements, and augment the driving experience. However, with increasing connectivity, automakers maintain that customer privacy must still be a priority. The Principles commit automakers to take certain steps to protect the personal data generated by their vehicles, including the precise geolocation of vehicles or how drivers operate their vehicles.

## 2. What type of personal information are the automakers committing to protect?

Personally identifiable information that vehicles collect, generate, record, or store in an electronic form that is retrieved from the vehicles by or on behalf of an automaker. Personally identifiable information includes data that is reasonably linkable to the vehicle, owner or registered user, and personal information provided by individuals subscribing to or registering for vehicle technologies and services.

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 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.

## 3. Do customers have a choice about whether their personal information is shared with third parties, such as insurance companies and third party marketers?

Yes, the automakers are committing to giving their customers a choice when it comes to their personally identifiable data being shared with any third party, including marketers and insurance companies.

In addition to giving their customers a choice when it comes to third parties, the automakers are also committing to give their customers choice before using their personally identifiable

information for marketing purposes.

**4. How do customers exercise choice about the sharing of personal information with third parties?**

Automakers will require the customer's affirmative consent, also referred to as opting in, prior to sharing the customer's personal information with third parties. There is no one-size-fits-all approach to obtaining affirmative consent, so automakers will likely develop a range of methods, appropriate to the circumstances, to obtain such consent. For example, customers might be asked to sign a document if they register for a service when they initially purchase a vehicle, or click "accept" on a touch screen system, or provide a verbal assent to a company representative, or take other clear action.

**5. Are the automakers taking any steps to prevent the government from obtaining their customers' personal information?**

Yes, the automakers will not provide their customer's geolocation data to the government unless they are presented with a warrant or a court order.

**6. What types of information are collected, used or shared by the automobile today?**

Today, different types of data are collected, used, and shared for different purposes:

- **Data collected by the vehicle, but not transmitted outside the vehicle, that is necessary for the operation of the vehicle:** Within a vehicle, 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.

- **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 severity 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 the location of their vehicle,

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 are shared with authorized dealers, who also share this information with automakers. In the case of safety recalls, this is a requirement of federal law. Some information may also be shared for marketing purposes, but only with express, affirmative consent by the vehicle owner or registered user.

**7. Does the customer own or control any data 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 vehicles evolve into complex computer systems that generate, store and analyze data, similar questions arose about data ownership related to vehicles. Set forth below are some examples of where the customers control data generated by the vehicle:

- **EDR Data:** Automakers affirm that consumers own the data that is collected in their EDRs.

- **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 address.

- **Technical Data:** Automakers reserve the right to use technical data that is stored in, and relates to the functioning of, the vehicle.

**8. Do the customers have the ability to review any of the data collected by the vehicle?**

Customers have the ability to review and correct data collected 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 automatic crash notification, roadside assistance, navigation, entertainment, and concierge services.

Customers also have the ability to review 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.

**9. 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.

**10. 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. Automobiles rely on the on-board network of computers to function, and these systems cannot be turned off and still allow the vehicle to safely operate. That is why safety, operations, compliance, and warranty information is collected by necessity. 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.

**11. How long will automakers hold on to the customers' personal information?**

Automakers commit to making a deliberate determination regarding whether and how long to keep personally identifiable information. When this personal information is no longer necessary for legitimate purposes, automakers commit to deleting or de-identifying the information.
Automakers collect information for a variety of legitimate purposes, including, among others, providing customers with services, developing and improving products and services, complying with legal and regulatory obligations, diagnosing or troubleshooting vehicle systems, improving vehicle safety, communicating with owners and registered users, preventing fraud or criminal activity, maintaining warranty and business records, and promoting security.

**12. If I download an app to my car will that data be covered by the Principles?**

No. The ability to download third party mobile apps to an in-vehicle app platform is still in the early stages, but it is likely the number of third party apps that vehicle owners and registered

users can choose to download to their vehicle will increase. For most third party apps, the vehicle owner or registered user who elects to download the app will have a direct relationship with the app provider and the terms of that relationship will govern any data collected or generated by the app.

### 13. How do the Principles compare to efforts in other industries and government?

Automakers are among the first industries to develop Principles to address consumer concerns about what data we collect, how we use it, and when/why data are shared. These 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.

### 14. Who has agreed to these Principles and when do they go into effect?

The following automakers have committed to the Principles:

AMERICAN HONDA MOTOR CO., INC.
ASTON MARTIN LAGONDA OF NORTH AMERICA, INC.
BMW OF NORTH AMERICA, LLC
CHRYSLER GROUP LLC
FERRARI NORTH AMERICA, INC.
FORD MOTOR COMPANY
GENERAL MOTORS LLC
HYUNDAI MOTOR AMERICA
KIA MOTORS AMERICA
MASERATI NORTH AMERICA, INC.
MAZDA NORTH AMERICAN OPERATIONS
MERCEDES–BENZ USA, LLC
MITSUBISHI MOTORS NORTH AMERICA, INC.
NISSAN NORTH AMERICA, INC.
PORSCHE CARS NORTH AMERICA
SUBARU OF AMERICA, INC.
TOYOTA MOTOR SALES, USA
VOLKSWAGEN GROUP OF AMERICA, INC.
VOLVO CAR GROUP

These Principles apply to all 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 that are initiated or renewed for all vehicles on or after January 2, 2016.

**15. Do these Principles apply to vehicles manufactured prior to Model Year 2017?**

These Principles are intended to establish a baseline on privacy for newer vehicles. As is true with any new guideline or requirement, the Principles apply prospectively. It is possible that automakers may compete on the issue of privacy and could find ways to apply the Principles to the current fleet. For example, automakers committed to applying the Principles to any vehicle technologies and services subscriptions renewed after January 2, 2016.

**16. Do these Principles apply to third-party service providers, suppliers of aftermarket devices, independent new car dealers, or other third parties?**

These principles do not, currently, apply to these third parties. When participating automakers work with third-party service provides, automakers commit to taking steps to ensure that these providers adhere to the Principles as well. Automakers are sharing these Principles with new vehicle dealers, who may implement their own privacy policies.