SBD Explores: Data Privacy

Data privacy, regulation, and driver consent

10-minute Insight

Data from vehicles is used for positive outcomes. Data can help insurers understand the circumstances of an impact. It can be used by fleet operators to check a vehicle is being used appropriately, or by OEMs to help inform future product improvements.

The storage and use of vehicle data is regulated, and these regulations vary around the world. In the EU, there are GDPR requirements. The USA does not regulate automotive data at a national level, but some states have introduced specific requirements. Data is regulated in China, but the requirements are different to those in USA and Europe.

In this edition of SBD Explores, we discuss the variation in data privacy regulation and highlight how some OEMs are making data consent more accessible.

Target audience

Product planning Strategy Engineering

Focus market(s)

Global

What is happening?

1 Companies are keen to make use of vehicle data

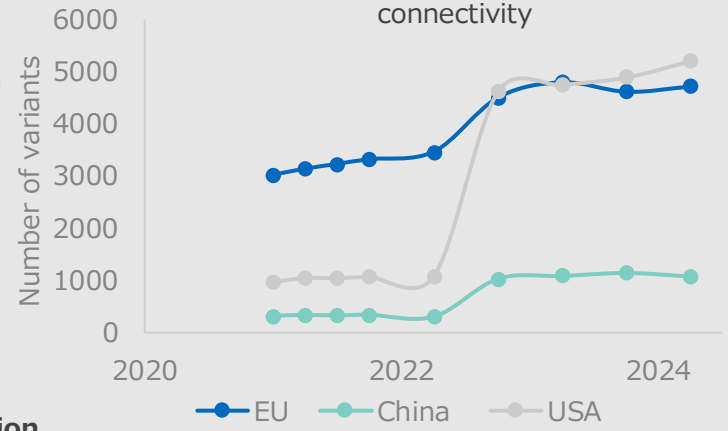
The availability of embedded connectivity in vehicles has been increasing for the past 3 years, as shown in Graph 1. Embedded connectivity is fitted because it allows data to be made available to off-car stakeholders. For example to insurers to determine premiums, or to fleet managers to check driver behavior. In some cases, only data insights are shared off vehicle with no need to transmit raw data. Examples of the uses of data are:

Usage Based Insurance

Product improvement

Crash Reconstruction

Graph 1: Number of variants with embedded connectivity



2 Some vehicle data is in scope of privacy requirements

There is currently no comprehensive data protection framework at a federal level. There are sector-specific regulations that do apply to data protection or sharing. Most do not apply to the automotive industry. Some states have introduced their own data privacy laws, but these are not harmonized at a federal level.

China has three data laws in effect. The Personal Information Protection Act is modeled on the GDPR and applies with the same extraterritoriality rules. The Data Security Law classifies data collected and stored within China. The Cyber Security Law establishes a uniform regime for cybersecurity and "important data".

The General Data Protection Regulation (GDPR) is the most stringent privacy and security law in the world, effective since May 2018. Though effective in the E.U., it imposes obligations onto organizations anywhere if they collect data from, or target products and services towards, E.U. citizens.

Key takeaways

- Data protection requirements for vehicles are not harmonized. Furthermore, general data protection requirements (not automotive specific) are not harmonized.
- Harmonization of vehicle regulations is preferred by OEMs. Harmonization allows a vehicle or component to be developed for multiple markets which saves costs and reduces complexity. Like with any other regulations, differences in requirements create a homologation and compliance challenge. Differences add cost and can result in features not being made available in some regions.
- In Europe, OEMs must observe GDPR when collecting and processing data. Some markets outside of Europe are revising their data protection policies to more closely align with GDPR. OEMs not in Europe may choose to align with GDPR to help compliance with those markets
- A customer's informed consent to the use of their data should always be obtained upon purchase. This is slowing down the process of onboarding vehicles into fleets. SBD report 643 contains more information on how an OEM can develop a smoother consent process for fleet operators.

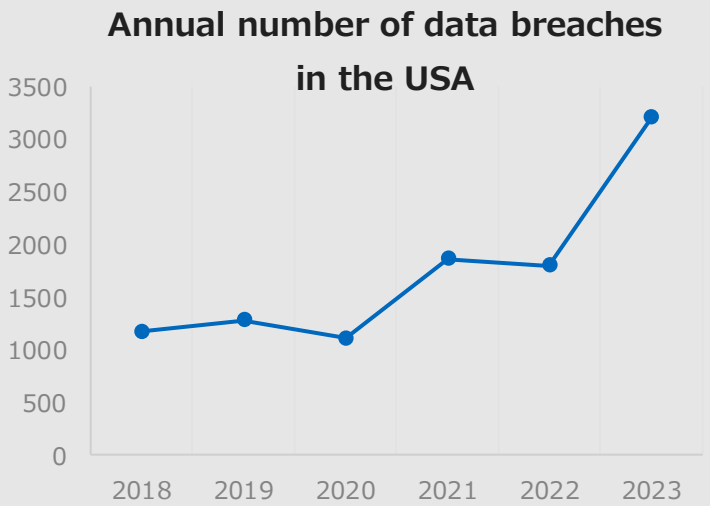
Why does it matter?

1 Customer consent options are important

In 2024, it was reported that vehicle owners were discontent with General Motors sharing insurance data with LexisNexis and Verisk. This affected users' insurance premiums. The event has led to lawsuits against General Motors.

So far, across all industries, the number of incidents related to data protection or privacy has been increasing in the USA – as shown in graph 2.

To address the rise in incidents, data protection regulations are spreading, and governments are looking to make examples out of bad actors.

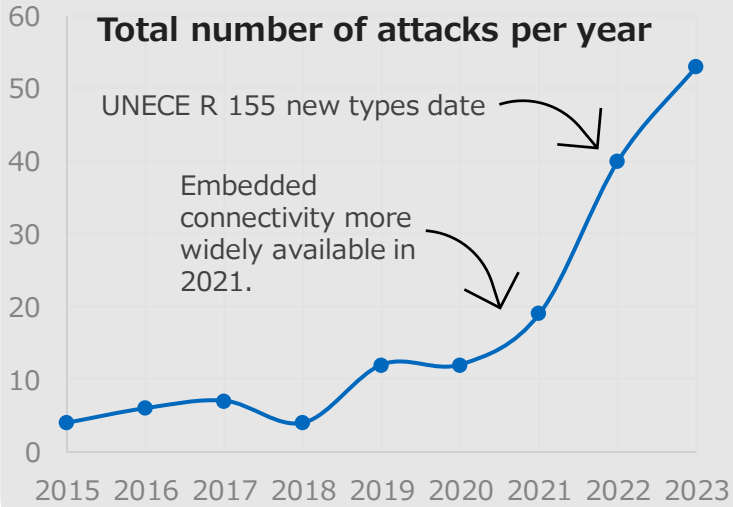


Graph 2: Annual number of data breaches in the USA over the years (not automotive specific) from Statista

2 UN ECE Cybersecurity requirements don't cover data privacy

Cybersecurity attacks have increased as the availability of embedded connectivity has increased. UN ECE Regulation 155 has been introduced and requires manufacturers to conduct an exhaustive risk assessment of potential threats.

Regulation 155 does not provide a definition for data or data privacy, however. It also does not have provisions for the standardization of the process of providing users with the ability to manage data consent within the vehicle.



Graph 3: Shows the number of cyber attacks. Data from SBD Report 905.

Key takeaways

- Globally, the number of incidents involving data protection or data privacy leaks is increasing. The data in graph 2 is not exhaustive, but indicative of a trend. UN ECE R155 was introduced to help OEMs manage cybersecurity risks but does not define data privacy or set requirements on how to provide in vehicle consent.
- Data sharing is not the problem. The issue lies in how the data is being used and by whom.
- Being transparent with customers about how their data is handled is also an important factor OEMs need to consider. For example, customers could have saved money on insurance premiums based on their driving if their driving data is shared with the insurance company by the OEM. The customer's consent must be provided, and importantly, it must be easy to manage consent preferences.
- The outcome is more interest from users in where personal data is used and more of a desire to want control over how data is used. The interest is not necessarily in regulation, but in how best to provide the user with consent options.

Who to watch out for?

The data collection settings in the IVI are not as straightforward as those of some other OEMs. GM does not disclose the length of time for which data will be retained. According to the Mozilla Foundation, data deletion could also be difficult.

BMW collects vehicle data, including personalized news. However, customers can disable data collection via the IVI system. They can also choose the level of data privacy they need from the IVI system.

Toyota allows customers to disable data collection via the IVI system and choose different levels of data sharing when setting up their profile. Customers can also view the terms of use of their data.

Hyundai provides the user with the ability to disable data sharing for voice recognition, GPS and phone information through the IVI. The controls allow the customer to turn on and off certain features, including the service that controls automatic crash notifications.

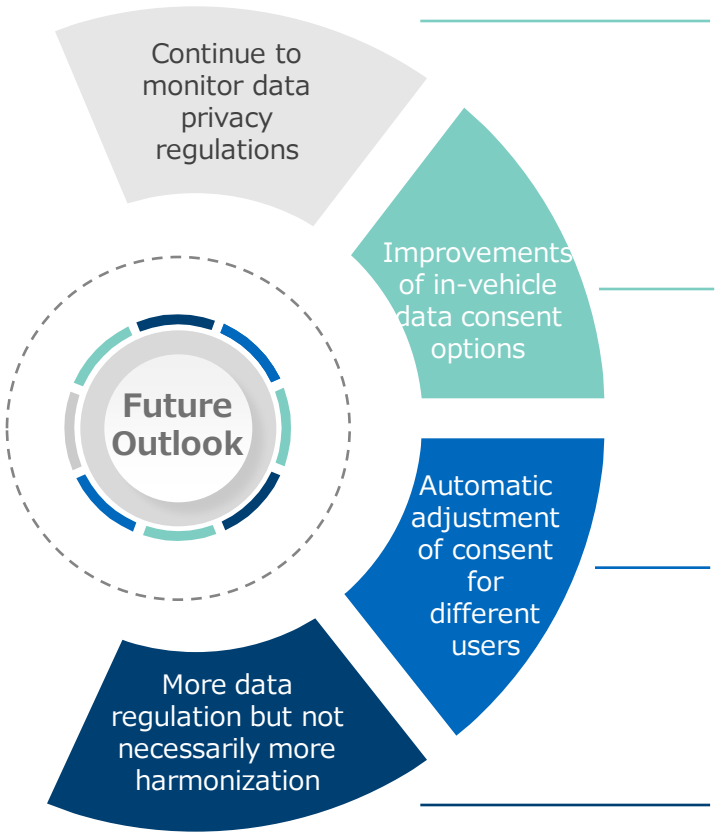
Tesla have made it easy to enable and disable data collection from the IVI. A user may enable or disable the collection of certain vehicle data including Autopilot Analytics & Improvements and Road Segment Data Analytics.

Nissan provides consent prompts whenever a connected feature is opened. Consent prompts are only otherwise available when logging into the portal and app and can be viewed through both channels.

Key takeaways

- SBD expects privacy to become a differentiator for many brands (particularly in the premium sector), who will build into their vehicles new types of privacy experiences.
- The automotive industry can focus on harmonization of the method for a user to provide, or revoke, data consent. The degree of ease with which the consumer can understand and control who has access to their data and how it is being used will be a differentiating factor for OEMs.
- The important thing is to focus on the process of allowing the user to manage data consent options from the vehicle infotainment screen. Requiring the user to visit a website is not following the principal of privacy and accessibility by design.
- Making it easy to manage consent is important. The next step is to determine how to link consent preferences with an individual person, not link with a vehicle. Some vehicles may have consent in place when passed onto second owners for example (without the OEM's knowledge). The second owner may have different preferences.

Where Next?



1. The automotive sector has some data protection regulations, but they vary in each region. Given the fast pace of development, OEMs should monitor development to ensure you are aware of any overlap in requirements or duplication of work.
2. Improving depth and accessibility in the vehicle could be the first step. Systems with more depth could give consent prompts, allow the disabling of consent for third party applications and allow the viewing of documents.
3. The next stage may be the development of a way of verifying the identity of the user so that consent preferences can be adjusted automatically. A system that can tell who the user is. Also, effort may be put into developing an off-board server for data analysis and management, and on-board system serving as a 'lock'.
4. Part of data protection is a political decision, and even if harmonized requirements are put in place, some countries may choose to opt out or put in place their own requirements. In the long term, it may be a reasonable to expect data protection requirements to still be fragmented.

Now | 2-6 yrs. | 6-8 yrs. | 8+ yrs.

Key takeaways

- All trendlines point to consumers caring more about privacy. Expect privacy start-ups to flourish, offering new types of data anonymization and giving consumers greater control.
- Some car makers are already working towards positioning themselves as leaders in data protection and privacy. This could be a leader both data security and accessibility of consent controls.
- In SBDs view, it is unlikely that countries will harmonize their national legislation. This would require political will and dedicated resources. OEMs will have to accept this. What can be harmonized, however, is the process of providing consent and verification of who is providing consent. This may happen.
- In preparation for potential future pressures, it is recommended that OEMs work on a process for ensuring that the correct data consent preferences are selected. For example, if a family have access to a vehicle, the vehicle should be able to know who is driving and adjust consent options depending on the driver.

How should you react?

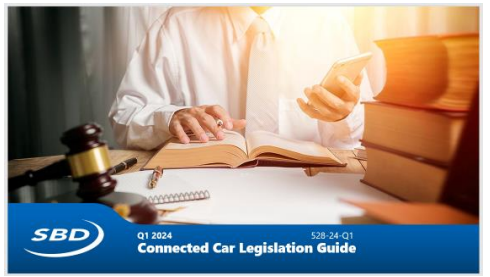
1. **Monitor** the progress of any privacy standards being drafted
2. **Identify** OEMs providing data consent options in the vehicle, and any innovative designs
3. **Improve** the ability of the vehicle to adjust consent automatically depending on the driver

Authors

Kurian Valiyaveettil Kurian
Research Analyst

Michael Levet
Senior Analytical Reports Specialist

Related SBD Reports



528 – Connected Car Legislation Guide

643 – Fleet management solutions

Related SBD Consultancy

- Competitive Assessment
- Market Landscape
- Due Diligence
- Strategic Advisory

Interested in finding out more?

Most of our work is helping clients understand new challenges and opportunities through individual projects. If you would like to discuss recent projects that we've completed, please contact us.