Navigating the complex world of autonomous vehicles can seem like a daunting task, especially when it comes to data privacy. What types of data do they collect? What are best practices for companies collecting autonomous vehicle data? How should my business implement effective data security? Read on to find answers to these and many other questions in our autonomous vehicle FAQs.

What kinds of data do autonomous and connected vehicles collect?

Autonomous and connected vehicles collect a wide range of data, from image and...
Image & Sensor Data

Image and sensor data is collected by video cameras, radar, thermal imaging and lidar to help the autonomous vehicle “understand” where it is relative to other objects on the road. Data collection points include driver speed, traffic conditions and surrounding objects such as curbs, trees and pedestrians.

Location Data

Location data, provided by GPS, includes point-in-time and route data. Absent additional safeguards, aggregating this data may indicate frequently visited locations. This data provides significant value to consumers and businesses while also implicating privacy concerns.

Why are data collection issues important to autonomous vehicle companies?

Autonomous vehicles require a vast amount of data to operate safely and answer questions such as where is the vehicle right now, and in what direction is it heading? In order to answer these questions, today’s connected and autonomous vehicles are actively collecting 100x more data than a personal smartphone.

California has led the way in providing consumers with transparency and rights surrounding the personal information their vehicle is gathering about them. Virginia, Colorado, Utah and Connecticut followed suit to develop comprehensive consumer privacy laws, which will also address these issues. California will update its existing consumer privacy law with new regulations covered under the California Privacy Rights Act (CPRA), which will take effect January 1, 2023.

What are some examples of data privacy issues?

Combining sensor and image information with location data can produce a data set that creates individually identifiable information, which the driver may want to keep private. The fact that the CPRA includes geolocation in its definition of ‘sensitive personal information’ and gives consumers the right to limit a business’s ability to use and share the sensitive personal information it collects about them could potentially impact this type of data collection. When considered as a full data set, the information collected by autonomous vehicle companies will likely be impacted by the evolving data privacy regulatory environment.

What are some key considerations when creating privacy policies for autonomous and connected vehicles?

Developing a strong privacy policy includes asking and answering the following questions:

- What type of personal data is the company collecting?
• When and how is that personal data being collected?
• How is that data being used?
• How is that data being stored?
• With whom is that data being shared?
• What elements of that data are being sold, if any?
• Who owns that data?

Finding answers to these questions is typically not a straightforward or simple exercise. In-house counsel should be prepared to have conversations with individuals in many different departments to fully understand the business’s practices around collecting and handling personal data. Effective communication with consumers via the privacy policy starts with a comprehensive internal understanding of personal data protection practices.

**What are the key data privacy best practices for autonomous vehicle companies?**

The Alliance for Automotive Innovation (Auto Innovators), a leading automotive industry group, spearheaded the development of consumer privacy protection principles in 2014. The organization reviewed these principles again in 2018 and is committed to periodic review to ensure their relevancy. These principles can be a useful data point.

**Key elements of these principles include:**

• Transparency
• Choice
• Respect for Context
• Data Minimization, De-Identification and Retention
• Data Security
• Integrity and Access
• Accountability

**What are the best practices for ensuring data security?**

Autonomous vehicle companies should remain flexible and be willing to adapt to evolving cybersecurity principles. There are many different approaches and best practices.

As an example, the National Highway Traffic Safety Administration (NHTSA)
recommends a layered approach to cybersecurity. NHTSA’s Cybersecurity Framework is structured around five principles — identify, protect, detect, respond and recover — and can be used as a basis for developing comprehensive data security policies.

**NHTSA describes how this approach “at the vehicle level” includes:**

- **Protective/Preventive Measures and Techniques:** These measures, such as isolation of safety-critical control systems networks or encryption, implement hardware and software solutions that lower the likelihood and diminish the potential impact of a successful hack.

- **Real-time Intrusion (Hacking) Detection Measures:** These measures continually monitor signatures of potential intrusions into the electronic system architecture.

- **Real-time Response Methods:** These measures mitigate the potential adverse effects of a successful hack, preserving the driver’s ability to control the vehicle.

- **Assessment of Solutions:** This involves information sharing and analysis of a hack by affected parties, development of a fix and dissemination of the fix to all relevant stakeholders (such as through an Information Sharing and Analysis Center). This layer ensures that once a potential vulnerability or a hacking technique is identified, information about the issue and potential solutions are quickly shared with stakeholders.

**How should autonomous vehicle companies strike a balance between data privacy and commercial opportunities?**

In this dynamic landscape, autonomous vehicle companies should create data privacy policies that provide transparency, protect consumer privacy and respect consumers’ choices. Effective data protection practices allow customers a reasonable level of control over their data while still enabling business opportunities to monetize downstream value chains.

© 2022 Varnum LLP

---

National Law Review, Volume XII, Number 192