PUBLICATION

Privacy and Cybersecurity Issues in Electric Vehicles

Authors: Stefan R. Kostas
February 02, 2023

This is the second article in a series of alerts that addresses what businesses, organizations and governmental entities should be considering as they navigate privacy and cybersecurity challenges encountered in the transition to electric vehicles and the supporting infrastructure. Please find our first, introductory alert here.

Privacy and Cybersecurity Issues in Electric Vehicles

Cybersecurity incidents in the automotive industry rose 225 percent from 2018 to 2021, and insiders expect this growth to continue as more and more consumers engage with the electric vehicle (EV) grid. Due to the incentives provided by the Bipartisan Infrastructure Law, EVs will likely constitute half of all new vehicles sold by 2030 in the United States. While the automotive industry has already increased production of EVs to meet these goals, this is only one part of the equation. The infrastructure supporting EVs and their network of charging stations are in dire need of upgrading to maintain adequate cybersecurity and privacy safeguards, particularly as the use of these systems is poised to expand rapidly.

A Brief Review of Technologies Used by EVs

Similar to conventional gas-powered cars, modern EVs are heavily equipped with technologies that generate large amounts of data. For example:

- **Vehicle telematics systems.** Telematics systems of an EV use sensors and software to produce data on the location, operation, and function of the vehicle and provide information about sudden acceleration or braking, trip histories, and fuel efficiency in real time. This data is communicated back to the original equipment manufacturers (OEMs) or the consumers through applications. OEMs may use the data shared by applications to improve the functionality of the vehicles and spot any issues. Consumers may use applications on their phones to send commands to the vehicle (e.g., remotely start or stop EV charging, control the air conditioning) and track their data using mobile applications.

- **Battery-related software.** Software embedded in an EV helps the vehicle regulate the battery, find charging stations, and control power flows. EVs also receive over-the-air updates through cloud connectivity to automatically improve the operation and performance of the vehicle. Additionally, software may generate data that predicts the remaining range and charge level of the battery.

- **Other in-vehicle technologies**. For example, many EVs are equipped with GPS navigation systems that remembers route histories and info-entertainment systems that understand drivers' voice commands and music choices.

- **Third-party apps.** Apps created and managed by third parties are increasingly entering the EV space. While this accessibility can benefit EV owners, it also creates third-party owned databases that, if hacked, can pose serious privacy issues.

As a result, a functioning EV requires millions of lines of code and relies on technologies that collect a wealth of data, including data about the vehicle and personal identifiable information about the person(s) in the vehicle. The use of those data driven technologies cause privacy and cyber security concerns, which will be discussed below.

Recent Cybersecurity Incidents and Privacy Cases

In recent years, ethical hackers[1] have exposed the vulnerabilities of modern vehicles through remote attacks. A notable example occurred in 2019, when a 19-year-old security researcher gained access to the digital car keys of a number of EVs across the world. By infiltrating a third-party software, the hacker ran commands on a compromised vehicle from a remote location. These commands included unlocking the doors, opening the windows, and disabling the cars' security mode. This attack, although conducted by a programmer with no nefarious motive, highlighted the ability for hackers to retain long-term control of vehicles without any warning to the driver. Shortly thereafter, the third-party app responded by updating the software, and the affected drivers were notified.

After exposing significant vulnerabilities in Sirius XM-connected vehicles, a group of ethical hackers recently uncovered security vulnerabilities in the APIs of car models from 16 manufacturers., The hackers were able to infiltrate employee administrator accounts, thus exposing an ability to control and access records of all customers of an EV OEM. Further, breaching the single sign-on authentication of the other EV OEM created a platform for potential hackers to pose as employees of the company. The hackers demonstrated both the ability to elevate privileges across the infrastructure (by directly communicating with customers) and access to internal controls of the vehicle. A vulnerability was also discovered with device-independent telematics companies,. Hackers obtained the capabilities to perform remote commands on each vehicle (e.g., unlock doors, start engines, honk horns) and even control police cars, ambulances, and other law enforcement vehicles. Although manufacturers subsequently addressed these vulnerabilities, this ethical case study illustrates the importance of implementing and continuously updating safeguards.

In addition to increased security risks, the use of personal data collected by EVs is subject to legal scrutiny. Notably, class action lawsuits are emerging against automobile companies over their collection and use of personal data. For example, Illinois' Biometric Information Privacy Act (BIPA) prohibits private entities from collecting personal data without prior written consent of the individual. Under BIPA, a private company's failure to meet certain requirements and properly inform the individual evokes a private right of action to the aggrieved individual. Recent lawsuits have arisen that seek damages from automotive and related companies for allegedly failing to obtain written consent for data collection and having inadequate data sharing policies. The complaints further contend that a breach of biometric data is irreversible because it includes highly sensitive and unique identifiers of the individual. These plaintiffs argue they did not agree to their biometric data being collected and shared with third parties, thus violating BIPA. Therefore, the evolving legal scene in Illinois, due to such cases, could serve as a precedent for EV companies, illustrating the potential consequences of not adhering to state privacy laws.

Cybersecurity Best Practices & Guidelines

In light of these risks and recent attacks, more guidance is becoming available to OEMs and the automotive industry. Members of the automotive industry should stay abreast of the available cybersecurity guidance, best practices, design principles, and standards based on or published by the Society of Automotive Engineers International (SAE), International Standard of Organization (ISO), Auto-ISAC, National Highway Traffic Safety Administration (NHTSA), Cybersecurity Infrastructure Security Agency (CISA), NIST, industry associations, and other recognized standards-setting bodies, as appropriate.

There are two frameworks for implementing cybersecurity best practices in EV manufacturing and operation: the NHTSA framework and the ISO/SAE 21434. Although non-binding, the guidelines provide uniform standards to follow and issues areas to consider when building security protocols. OEMs should consider other cybersecurity guidance, best practices, and design principles along with these two frameworks. For example, ISO and NIST have cybersecurity guidance for companies in all industries. Although not specifically applicable to the EV industry, EV OEMs can still use those general frameworks as guidelines to build their cybersecurity programs.

NHTSA recently published Cybersecurity Best Practices for the Safety of Modern Vehicles a set of guidelines to provide automakers with best practices to strengthen cybersecurity and protect consumers moving forward. These guidelines are waiting to be finalized, and they apply to both gasoline-powered vehicles and EVs. NHTSA promotes a multi-layered approach focused on safeguarding the wireless and wired entry points of an EV, all vulnerable to a cyberattack. Specifically, NHTSA suggests that such approach should include*:*

i. risk-based prioritization of protection for safety-critical vehicle control systems and sensitive information

ii. timely detection and rapid response to potential threats and incidents

iii. rapid recovery when attacks do occur

iv. methods for accelerating the adoption of lessons learned across the industry, including effective information sharing

Within the guidelines, NHTSA outlined different vulnerabilities and the automotive industry's obligation to address each vulnerability. NHTSA encouraged OEMs to establish systems that can detect an incident and respond by transitioning the EV into a minimal risk condition. The NHTSA also highlighted the dangers of vehicle sensor data manipulation, including GPS spoofing, camera blinding, and road sign modification. Altogether, NHTSA flagged risk areas within EV development and encouraged communication, through event logs and the Automotive Information Sharing and Analysis Center, to foster collaboration between participants and continuous improvement of security.

Also, the ISO and SAE recently published ISO/SAE 21434 (ISO 21434) – a standard to aid automotive product developers and OEMs in implementing cybersecurity methods for connected vehicles. Generally, ISO 21434 covers cybersecurity governance and structure, secure engineering throughout the lifecycle of the vehicle, and post-production security processes. The standard addresses the production cycle of EVs from initial design to its end-of-life decommissioning. Further, the standard holds that strengthening the approaches that manufacturers use to test their products leads to better safety for EV owners. OEMs are encouraged to apply cybersecurity checks throughout the supply chain and to ensure that software programming examines risks at every step. Overall, the ISO 21434 prompts OEMs to apply rigorous testing with the goal of maintaining safety for hyperconnected vehicles, their passengers, and other vehicles on the road.

Privacy Considerations

OEMs must consider the implications of applicable privacy and data protection laws as early as possible during the vehicle design phase. Using numerous sensors and tracking devices installed in a vehicle, an EV collects a large amount of data from its drivers and passengers, including sensitive personal data. By collecting, processing, storing, and transferring personal information, EV companies may trigger privacy compliance obligations under both domestic and international laws. Multiple privacy laws may apply to a particular data processing activity, depending on what types of data are collected, who the data subjects are, and where the data is stored. Violation of applicable privacy laws may lead to severe negative consequences, including regulatory enforcement actions, class actions, and reputational damages. Domestically, OEMs have the obligation to comply with federal and state privacy laws when deciding how its vehicles collect or process individuals' personal information. On the federal level, among other things, OEMs should disclose their privacy practices to data subjects (including drivers and passengers) without any misrepresentations. Violations might be prosecuted by the FTC under Section 5 of the FTC Act.

If certain categories of information are collected (e.g., health information, information about minors or students), OEMs are obligated to apply heightened standards to such datasets as prescribed by applicable federal statutes. State laws may also impact OEMs and the ways in which their vehicles collect data. Five states have passed comprehensive privacy laws: California, Colorado, Connecticut, Utah, and Virginia. By way of example, in California, an OEM, if considered a "business" under the California Consumer Privacy Act (CCPA), is obligated to make certain privacy disclosures to residents of those states and establish a procedure to promptly respond to consumers' requests regarding their data. A private cause of action is available under the CCPA, meaning that California consumers have statutory basis to assert claims resulting from data breaches and claim statutory damages of between $100–$700 per violation and per consumer. This number can increase quickly if a breach involves thousands of California consumers. Additionally, if a data processing activity involves biometric data, it is prudent to check specific state law requirements (for example, BIPA requirements).

International privacy and data protection laws also come into play if the company has an eye on the European market, or simply because the vehicle uses cloud-based software that stores data in decentralized locations globally. The General Data Protection Regulation (GDPR), which is often considered one of the most stringent data protection laws in the world, applies to EU companies as well as companies that operate from outside the EU if they offer goods or services to EU residents or monitor the behavior of EU residents. Many types of data collected by EVs and its numerous technologies fall under the GDPR's broad definition of "personal data," thus making the manufacturer of the vehicle subject to the law. It is also important to keep in mind that the GDPR restricts data transfers from the EU to a country without an adequacy decision from the EU (including the United States). This restriction poses issues for many U.S.-based OEMs, if they have business needs to transfer EU data to the U.S. for purposes including analytical and marketing. Those OEMs, therefore, need to implement at least one appropriate mechanism to legalize such international data transfers under the GDPR. A single breach of the GDPR may be fined up to the greater of €20 million or 4 percent of the company's annual global turnover.

As a result, OEMs are challenged with designing a comprehensive privacy compliance program under a patchwork of international, federal, and state laws while designing their EVs. While the cost of a global privacy compliance program can in some cases be sizeable, the potential costs of non-compliance can be more significant and come with undesirable consequences, including loss of consumer trust and reputation damages. Businesses should carefully weigh the costs and benefits of their current privacy compliance scheme.

How can OEMs significantly reduce legal and compliance risks associated with large amount of data collected by EVs?

Moving forward, OEMs carry an important responsibility in integrating cybersecurity into the design of EVs. Such responsibility extends from the EVs themselves to the entire grid, including charging stations, software updates, and any other third-party systems that interface with the EV. As EVs collect an abundance of consumers' personal information, it is vital to safeguard each system associated with the vehicle. On balance, OEMs shall look to the NHTSA and ISO 21434 guidelines (among others) for best practices and consider privacy implications in designing its EVs to create the safest driving experience for EV owners.

Baker Donelson has a multi-disciplinary team focused on EV and infrastructure that tracks issues and provides tailored advice to ensure that clients' privacy and security programs follow applicable laws and how to best defend cyberattacks. If you have any questions about this or any other aspect of your privacy and security practices, please contact Stefan Kostas or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity team or our EV and Infrastructure team.

[1] An ethical hacker is a person who hacks into a computer network in order to test or evaluate its security, rather than with malicious or criminal intent.