PUBLICATION

Cybersecurity and Privacy Concerns in Collecting Data from EV Drivers' Devices

Authors: Linghan H. Ji-Otto, Stefan R. Kostas
July 05, 2023

This is the fourth article in a series 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. Our previous alerts in the series are:

- "Focus on EV Sector: Navigating Privacy and Cybersecurity Challenges" (December 2022)
- "Privacy and Cybersecurity Issues in Electric Vehicles" (February 2023)
- "Privacy and Cybersecurity Standards for NEVI Funded EV Charging Station Projects," (March 2023)

Electric vehicles (EVs) are becoming more popular as the U.S. government is increasing funding and initiatives to welcome more players into the EV space. As EV manufacturers innovate to compete and attract customers, they are increasingly integrating drivers' personal devices into the functionality of the vehicle. Although such technological improvements enhance the driving experience, they also reveal data privacy and cybersecurity challenges crucial to the future of the EV industry.

Many EVs enable drivers to set up command centers for their vehicles through apps on their smartphone or smartwatch. The ability to connect personal devices to an EV is a significant value-add to the consumer and supplies many benefits that are unavailable to owners of traditional vehicles. Connected EVs and devices empower drivers to control various car functions remotely. Meanwhile, EV companies can improve the driving experience by exchanging data with drivers' personal devices. For example, there are mobile apps that allow users to interact remotely with their vehicles using their iPhone or Android device. Users can enable keyless driving, lock or start the vehicle, adjust headlights, use GPS location tracking and roadside assistance, check the vehicle's estimated range and drive mode, and monitor charging information, as well as view details including the odometer, VIN, and current firmware version, all from their personal devices. While these connected features offer unmatched conveniences and advantages to EV drivers, they also raise important cybersecurity and privacy concerns. The following sections of this article will discuss potential issues that arise from collecting data from drivers' personal devices, underscoring the importance of maintaining robust data protection measures in the evolving EV landscape.

Cybersecurity Concerns

The interconnectedness of EVs and personal devices introduces potential threats such as mobile malware, phishing attacks, and data breaches. Mobile malware, specifically designed to target devices like smartphones, aims to access private data. Users can unintentionally download it by clicking on fraudulent ads. Mobile phishing targets services like SMS, WhatsApp, and Facebook, employing techniques to impersonate legitimate businesses and trick users into sharing personal or sensitive data. If an EV company holding users' personal data suffers a data breach, hackers may access users' account credentials and use them to penetrate those connected devices. This intrusion could allow them to control various features offered by EV apps, pinpoint the vehicle's exact location, manipulate its operation, or drain its battery. More alarmingly, hackers could gain access to the users' personal data across multiple apps on the device, potentially exposing sensitive details about their financial accounts, social media profiles, and communication channels, posing a serious security risk.

Additionally, the burgeoning EV industry is fostering a growing market for third-party apps. Such apps offer features that are not always provided by EV manufacturers, enhancing the driver's experience. However, if third-party apps lack adequate privacy safeguards, they could expose connected personal devices to potential cyber breaches. EV companies need to contemplate the implications of these third-party apps and the risks of inadequate cybersecurity and privacy protections. To mitigate such risks, EV companies might consider including disclaimers about third-party apps in their terms and conditions, thus absolving themselves of liability for any breaches or malicious activities associated with these apps.

As the interconnectedness between EVs and personal devices increases, implementing robust cybersecurity measures will be even more essential. Some ways EV companies can enhance security and maintain consumer trust include:

- **Software Updates:** Regularly update software and firmware to address vulnerabilities and protect against threats.
- **Secure Protocols:** Employ secure protocols like Transport Layer Security and systems like Intrusion Detection and Prevention System to safeguard data and preempt cyber incidents.
- **Multifactor Authentication:** Implement this method to provide extra security layers, making unauthorized access more difficult, even with a compromised password.
- **Mock Breach Exercises:** Update data breach response protocols to account for risks associated with collecting data from drivers' personal devices and conduct related tabletop exercises to test these protocols.
- **Data Deletion:** Promptly remove data collected from personal devices when it is no longer needed, further safeguarding privacy.

Privacy Concerns

EV companies holding user profiles need to navigate a myriad of domestic and international privacy laws, potentially elevating compliance costs.

In the U.S., while there is no federal privacy law, several states and industries have implemented specific regulations. State privacy laws are among the most active kinds of legislation this year. While the California Privacy Rights Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Virginia Consumer Data Protection Act have set the stage, newer legislation has passed this year in Tennessee, Iowa, Indiana, and Montana. With the rising tide of state-level privacy laws, companies must confirm that their data practices are in alignment with the specific laws of the consumer's residence state before collecting data from their personal devices.

On an international level, the EU's General Data Protection Regulation (GDPR) enforces stringent regulations on organizations that collect, use, or store personal data, including non-EU companies handling data of EU citizens and residents. GDPR also restricts data transfers to countries – like the U.S. - without an "adequacy decision" from the European Commission, which has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679, whether a non-EU country offers an adequate level of data protection. Consequently, U.S. EV companies need to keep a keen eye on how their technologies process, store, and transfer data collected from personal devices that could be subject to GDPR.

Moreover, compliance with these laws not only demonstrates responsible stewardship, but also mitigates the risk of potential class-action lawsuits, especially in states with defined privacy regulations. For instance, the

California Rental Passenger Vehicle Transactions Law (RPVT) places limits on rental car companies' access to customer data gathered through "electronic surveillance technology." Customers who believe their data has been misused can bring private actions under the RPVTL. Several class-action lawsuits have already been brought under this law in California. These cases stem from customers pairing their smartphones with rental vehicles' infotainment or navigation systems. These lawsuits should put EV and associated companies on notice to maintain robust privacy protocols to comply with state laws and avoid class actions.

Establishing and maintaining a comprehensive privacy compliance program is important for proactively addressing privacy issues. Compared to resolving issues reactively, this approach has the benefit of reducing expenses related to regulatory fines, costly litigation, and more. Here are some steps that electric vehicle companies can begin to take:

- **Data Mapping:** Understanding data flow within the organization should be the first step. This ensures compliance teams comprehend the extent and nature of the issues, such as how many technologies are collecting data from personal devices.

- **Policy Updates:** Existing privacy policy should be assessed and amended to incorporate how data from drivers is collected, processed, stored, and shared through vehicles and their technologies.

- **Vendor Management:** Effectively managing third-party vendors is crucial, given their potential access to data collected by EV apps. Their adherence to privacy standards in handling user data is an important aspect that should not be overlooked, as it helps maintain user trust and solidify data protection.

Conclusion

The ability to control EVs through personal devices offers an enhanced experience for consumers by allowing remote control and charging management at a driver's fingertips. However, this accessibility also creates areas of vulnerability for threat actors to infiltrate personal data and privacy. Gaining access to a personal device can expose personal data, geographical data of the vehicle and its owner, and potentially harmful remote access to the controls of the vehicle. Such access can compromise the driver's financial information, identity, personal safety, and, ultimately, control over the electric vehicle. By staying aware of the risks linked to connected devices and following best practices, EV owners can bolster consumer trust and steer clear of negative consequences including regulatory fines, brand damage, or costly litigation.

If you have any questions or would like more information on this topic, please reach out to L. Hannah Ji-Otto, Stefan R. Kostas, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Group or our EV and Infrastructure Team.