PUBLICATION

Focus on EV Sector: Navigating Privacy and Cybersecurity Challenges

Authors: Stefan R. Kostas
December 07, 2022

This is the first in a series of alerts that will address 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.

Introduction

The electric vehicle (EV) space is picking up speed as the industry looks to take advantage of recently passed federal legislation. The $7.5 billion infrastructure plan passed by Congress will create an interconnected network of charging stations throughout the United States, with the goal of improving sustainability and equitable access to cost-saving transportation. By 2030, the infrastructure plan calls for EVs to make up half of all new vehicles sold in the United States. In the past four years, the number of charging stations has nearly doubled and is on pace to continue to increase significantly.

While the infrastructure plan promises both growth for the EV sector and committed efforts to reduce fossil fuel usage, it also creates data privacy and security implications that arise throughout the EV ecosystem. The large amount of personal information collected and processed by players in the EV ecosystem triggers compliance obligations under international, federal, and state privacy and data protection laws. Cyberattacks to the charging stations and vehicles, as well as the databases housing drivers' information, has caused, and continues to cause extensive damage to manufacturers on the grid, EV owners, and potentially the national power grid.

Previously, privacy or security has not been the top priority for original equipment manufacturers (OEMs) and other operators on the grid, partially because this industry is less regulated in the United States compared to health care and financial services industries. Recently, however, federal and state governments have shown increasing concern about data privacy in the EV industry. For example, OEMs interested in applying for federal and state grants are now required to implement certain privacy and security measures and satisfy data reporting requirements. As a result, more and more major players in the EV market are putting privacy and cybersecurity issues front and center as they race to obtain those grants and gain consumers' trust.

Based on our experience in advising companies in the EV space, we have observed three main data streams in this ecosystem. In our series, we will discuss privacy and cybersecurity issues affecting the data stream to help EV sector businesses and governmental entities, including OEMs and charging station operators, identify and mitigate compliance and breach risks.

1. **Electric Vehicles**
   EVs, similarly to other gasoline-powered vehicles that have embraced new technology, collect a broad spectrum of a consumer's data every time they get behind the wheel. This data includes precise driving routes through GPS, telematics (e.g., speed and breaking patterns), music preferences, and voice commands. Altogether, this data helps companies learn behavior and patterns to serve consumers better, but collecting it also triggers privacy compliance obligations and opens the door for threat actors to acquire sensitive information. In terms of security issues, an attacker can learn where the driver lives and, with the right technology, steal the EV without a trace.

An attacker can also impair the battery capacity and speed/acceleration faculties of the vehicle, creating dangerous conditions for drivers and others on the road.

2. **Charging Stations**
   Unlike traditional gasoline-powered vehicles, EVs introduce a new place where data can be collected: EV charging stations. Charging stations are essential for EVs to restore their batteries and keep the vehicles in motion. Private and public providers offer these stations and allow the driver to pay to charge their EV. Security and privacy issues arise at these stations because they are connected to the internet and interface directly with EVs. A charging station collects a significant amount of data (including personal and sensitive information) during its attachment to the EV and from all connected devices, which triggers compliance obligations for data collectors and poses significant privacy risks to data subjects in a data breach. Vulnerabilities in charging stations may be used to disrupt the power of a local area, distribute inappropriate content via charging station screens, and gain control of an EV and compromise a vehicle's safety features.

3. **Drivers' Personal Devices**
   Many EVs allow drivers to set up command centers for their vehicles through online accounts. Through these accounts, users can easily access vehicle details such as fuel level, tire pressure, and oil life. From a privacy perspective, operators of those online accounts must understand the laws and best practices for the collection, use, processing, and sharing of drivers' personal information, especially when they intend to use drivers' personal device data for marketing purposes or to set insurance premiums. From a security perspective, an attack on a personal device creates an enormous influx of sensitive data through the admission into social media and any online account of the user.

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 best defend cyberattacks. If you have any questions about this or any other aspect of your privacy and security practices, please contact the authors Stefan Kostas or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity team or our EV and Infrastructure team.