BAKER DONELSON

EV AND INFRASTRUCTURE SECTOR

NAVIGATING PRIVACY AND CYBERSECURITY CHALLENGES

TABLE OF CONTENTS

INTRODUCTION TO OUR SERIES

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 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.

ABOUT OUR AUTHORS

Ms. Ji-Otto and Mr. Kostas are members of the multidisciplinary EV and Infrastructure team that Baker Donelson has assembled to focus on this fast-growing sector.

L. Hannah Ji-Otto
CIPP/US, CIPP/E, CIPP/C, CIPP/A, CIPM, FIP
Of Counsel | Nashville | 615.726.5758
hjiotto@bakerdonelson.com

Stefan R. Kostas
Associate | Nashville | 615.726.5697
skostas@bakerdonelson.com

PRIVACY AND CYBERSECURITY ISSUES IN ELECTRIC VEHICLES

Cybersecurity incidents in the automotive industry rose **225 percent** from 2018 to 2021.

Cybersecurity incidents in the automotive industry rose 225 percent from 2018 to 2021[1], 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.

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 remember 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 cybersecurity concerns.

[1] "The Continuing Evolution of Automotive Cyber Security," *IEEE Innovation at Work*, https://innovationatwork.ieee.org/the-continuing-evolution-of-automotive-cyber-security.

RECENT CYBERSECURITY INCIDENTS AND PRIVACY CASES

In recent years, ethical hackers[2] have exposed the vulnerabilities of modern vehicles through remote attacks. A notable[3] 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[4] vehicles, a group of ethical hackers recently uncovered security vulnerabilities[5] in the Application Programming Interfaces (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.

A group of ethical hackers recently uncovered security vulnerabilities in the APIs of car models from **16 manufacturers.**

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 AND 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), National Institute of Standards and Technology (NIST), industry associations, and other recognized standards-setting bodies, as appropriate.

[2] 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.
[3] Steve Tengler, "Cybersecurity Risks: Protecting The Electric And Software-Defined Car," *Forbes*, https://www.forbes.com/sites/stevetengler/2022/06/28/cybersecurity-risks-protecting-the-electric-and-software-defined-car/?sh=7b7be0632475.
[4] Emma Roth, "SiriusXM flaw could've let hackers remotely unlock and start cars," *The Verge*, 2022, https://www.theverge.com/2022/12/3/23491259/sirius-xm-hack-remotely-unlock-start-cars.

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[6] 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:

Risk-based prioritization of protection for safety-critical vehicle control systems and sensitive information

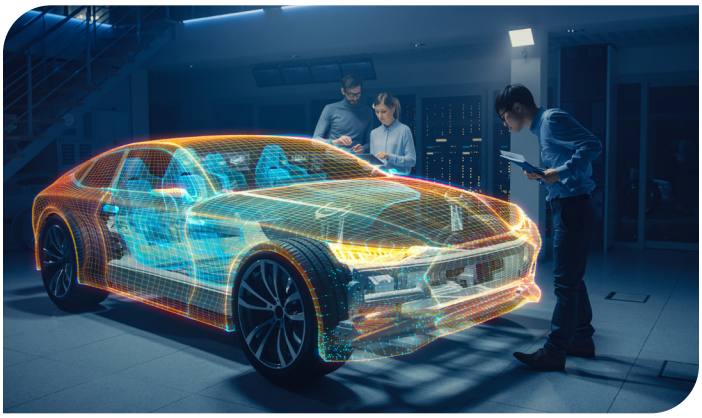
Timely detection and rapid response to potential threats and incidents

Rapid recovery when attacks do occur

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[7] (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.



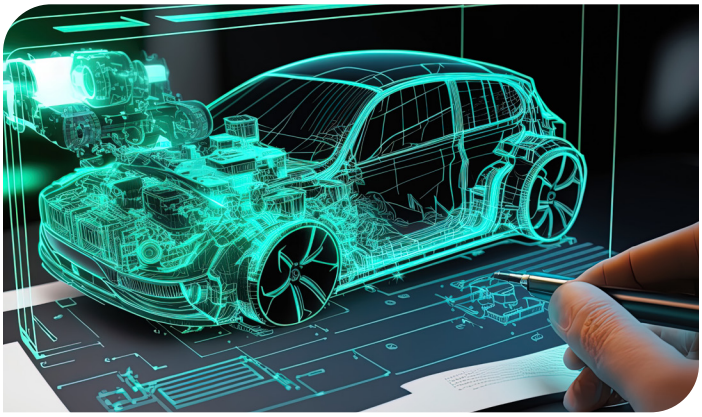
[5] Sam Curry, "Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More," *Sam Curry Blog*, 2023, https://samcurry.net/web-hackers-vs-the-auto-industry.

[6] Steve Tengler, "Cybersecurity Best Practices for the Safety of Modern Vehicles," *National Highway Traffic Safety Administration*, 2022, https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-pre-final-tag_0_0.pdf.

[7] "ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering," *International Organization for Standardization (ISO)*, 2021, https://www.iso.org/standard/70918.html.

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)[8], 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.

[7] "General Data Protection Regulation (GDPR)," *Intersoft Consulting*, https://gdpr-info.eu/.

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.

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.

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.

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.

PRIVACY AND CYBERSECURITY STANDARDS FOR NEVI FUNDED CHARGING STATION PROJECTS

More than **$1.5 billion** in funding to build electric vehicle chargers across the U.S.

The National Electric Vehicle Infrastructure (NEVI) Formula Program, a program established and funded by President Biden's Bipartisan Infrastructure Law[1], has approved more than $1.5 billion in funding for the fiscal years 2022 and 2023 to build electric vehicle (EV) chargers across the U.S. This funding encourages a fast pace of infrastructure implementation and attracts an influx of new players to the electric vehicle charging space. As the adoption of EVs continue to increase and infrastructure is developed, both federal and state regulators are emphasizing the importance of prioritizing consumer privacy and security.

EV charging stations collect sensitive information such as payment data, and are connected to the power grid, meaning that a single attack could have severe consequences for both consumer privacy and the grid itself. Proactively addressing privacy and security issues during the construction of charging stations aligns with the federal government's push for widespread EV adoption and helps to prevent potential breaches in the charging infrastructure. This article offers a high-level discussion of the privacy and security requirements outlined in the Federal Highway Administration's (FHWA) rules and NEVI plans from three states, as well as a list of industry standards for charging stations.

FEDERAL HIGHWAY ADMINISTRATION RULES

The Bipartisan Infrastructure Law requested that the FHWA develop mandatory standards concerning the development and operation of publicly available EV charging infrastructure in U.S. markets. As a result, in 2022, the FHWA proposed mandatory standards to provide a framework for the EV charging sector and the interconnected national grid. On February 28, 2023, the FHWA considered all comments received and published its final standards for projects funded under the NEVI Formula Program and projects for the construction of publicly accessible EV chargers under certain statutory authorities (Final Rule). The Final Rule takes effect on March 30, 2023. Note that the Final Rule is designed to set the *minimum* standards and does not prevent states and other designated recipients from establishing more stringent EV charging infrastructure requirements toward building a convenient, affordable, reliable, and equitable national charging network. To summarize, the Final Rule provides the following minimum requirements on privacy and cybersecurity issues for states and direct recipients of NEVI funds.

Payment processing

Charging stations must offer secure payment methods that are accessible to people with disabilities and do not require a membership to use. Chargers and charging networks must comply with Payment Card Industry Data Security Standards (PCI DSS).

Customer privacy

Charging station operators should collect, process, and retain only personal information necessary to provide charging services to consumers. They must also take reasonable measures to safeguard consumer data.

Technical requirements

Chargers, hardware, and software must conform to ISO 15118 standards for charger to electric vehicle communication. Chargers must communicate with a charging network via a secure method and be able to receive and implement secure remote software updates.

Data submission

States and direct recipients must make certain data regarding charging stations and charging sessions available on an aggregated and anonymized basis to the public. Some types of data should be submitted quarterly, some annually, and some only once.

[1] "Bipartisan Infrastructure Law," *U.S. Department of Transportation*, https://www.transportation.gov/bipartisan-infrastructure-law.

Cybersecurity

The Final Rule requires states to implement appropriate physical strategies for the location of the charging station and cybersecurity strategies that protect consumer data and protect against the risk of harm to, or disruption of, charging infrastructure and the grid. FHWA considered public comments on specific cybersecurity standards and decided to leave cybersecurity provisions in this Final Rule as areas of consideration by states to allow for evolution of state NEVI cybersecurity plans outside the regulatory process.

STATE NEVI PLANS

The FHWA has approved the NEVI plans[2] for EV charging infrastructure deployment in all 50 states, Puerto Rico, and D.C. As a result, all states now have access to all fiscal year 2022 and 2023 NEVI formula funding to aid in building EV chargers covering approximately 75,000 miles of highway across the country. Most (if not all) of those approved plans address consumer privacy and cybersecurity issues, which underscores the significance of these issues in the EV charging landscape. What follows is a high-level discussion on the NEVI plans of California, Tennessee, and Florida.[3]

All 50 states, Puerto Rico, and D.C. now have access to all NEVI formula funding to aid in building EV chargers covering approximately **75,000 miles** of highway across the country.

California

The California Electric Vehicle Infrastructure Deployment Plan[4] was approved by the FHWA on September 14, 2022. The plan recognizes the importance of securing EV chargers, because "EV chargers provide direct connections to the vehicle's onboard system and the EV charging service provider's network, and indirectly to the driver's smart phone if the charge is paid for with an app, banking information if a debit or credit card is utilized, telecommunications provider, and the electric grid." The plan cites California's Senate Bill 327 (SB-327), which is a law that requires a manufacturer of a connected device to equip the device with reasonable security features that are appropriate to the nature and function of the device. Although not specifically stated, the plan is signaling that EV chargers can be considered connected devices subject to SB-327. Applying the requirements of SB-327 to charging stations, charging station operators must implement reasonable security features to their EV charging stations to protect any information they collect from unauthorized access, destruction, use, modification, or disclosure.

[2] "State Plans for Electric Vehicle Charging," *Joint Office of Energy and Transportation*, https://driveelectric.gov/state-plans.

[3] We selected California for discussion because it received over $56 million funding in FY 2022, which is fairly large compared to other states. Tennessee and Florida are selected because Baker Donelson has offices in those states.

[4] "California's Deployment Plan for the National Electric Vehicle Infrastructure Program," *U.S. Department of Transportation Federal Highway Administration*, 2022, https://www.fhwa.dot.gov/environment/nevi/ev_deployment_plans/ca_nevi_plan.pdf.

Tennessee

In Tennessee, the Departments of Transportation, and Environment and Conservation collaborated and developed the Tennessee Electric Vehicle Infrastructure (TEVI) Deployment Plan.[5] This plan provides an outline for Tennessee's goals of creating an EV charging infrastructure and joining the interconnected network across the country. One key consideration of the plan is the state's commitment to protecting against cybersecurity risks. Specifically, this plan discusses the attack vectors that arise with the necessary components of EV charging, such as drivers' smartphones, banking information, and the connection between non-state-owned assets and state-owned intelligent transportation system infrastructure. As part of this commitment, "the State will require any subrecipients, prior to issuance of the award or other funding, to provide a cybersecurity plan that 'demonstrates compliance with applicable state and federal cybersecurity requirements.'" The state will then review the plan to ensure the subrecipient has demonstrated compliance with applicable state and federal cybersecurity requirements. Additionally, the plan must provide how the subrecipient will continually maintain and update its cybersecurity protocols throughout the life of the project.

Florida

On September 14, 2022, the FHWA approved the Florida Department of Transportation's (FDOT) Electric Vehicle Infrastructure Deployment Plan,[6] which recognized that Florida "charging stations must provide reasonable assurance against cyberattacks, data breaches, and loss of privacy." The plan also identifies the operational impacts that such cyber incidents may cause, such as power quality issues and phase instability which could result in a cascade of effects throughout the electric power grid.

To address these concerns, the FDOT will develop and implement a cybersecurity plan that will govern such stakeholders as grid operators, vehicle manufacturers, original equipment manufacturers, vendors, and charging network operators. Cybersecurity plan requirements will include full-scope risk assessments to identify the comprehensive threat surfaces presented by the new EV infrastructure, as well as segmentation requirements, compliance with PCI DSS requirements, and documentation of security operations and certification of System and Organization Controls. The cybersecurity plan will also include guidance to inform risk assessments (including schedules for performing the same), as well as processes for selecting and implementing cybersecurity controls. The FDOT will also provide for governance and oversight of this cybersecurity plan and its implementation.

[5] "Tennessee Electric Vehicle Infrastructure (TEVI) Formula Program Deployment Plan," *U.S. Department of Transportation Federal Highway Administration*, 2022, https://www.fhwa.dot.gov/environment/nevi/ev_deployment_plans/tn_nevi_plan.pdf.

[6] "Florida's Electric Vehicle Infrastructure Deployment Plan," *U.S. Department of Transportation Federal Highway Administration*, 2022, https://www.fhwa.dot.gov/environment/nevi/ev_deployment_plans/fl_nevi_plan.pdf.

INDUSTRY STANDARDS

The industry standards listed below are referenced in the FHWA Final Rules, state NEVI plans, or other guidance as best practices for addressing privacy and cybersecurity concerns when constructing EV charging stations.

Open Charge Point Protocol

Open Charge Point Protocol (OCPP) is an application protocol that allows for communication between an EV charging station and the charging station management system. This protocol enables the charging unit and the central management system to communicate across different EV chargers (referred to as Electric Vehicle Supply Equipment, or EVSE). The OCPP's security framework[7] addresses three common security issues: (i) secrecy of communications; (ii) authentication of the server, and (iii) authentication of the client.

ISO 15118

ISO 15118[8] is an international standard for the communications protocol between an EV and the charging station. Through this protocol's plug and charge feature, EV drivers can obtain instant authorization at linked charging stations by plugging the vehicle into the charge point. Charging stations must ensure encryption of messages with the EV and authentication processes to maintain compliance with ISO 15118. These standards have been endorsed by FHWA's Final Rules.

ISO 27001

The ISO/IEC 27001[9] is a comprehensive set of guidelines created by the International Standard Organization (ISO). These standards provide guidance for global businesses to maintain and regulate their information security systems and properly store business data. Specifically, these standards seek to achieve information security through confidentiality, integrity, and availability. Although these ISO standards were not specifically developed for electric vehicles or their charging infrastructure, it has been widely adopted in various industries. As a result, charging station operators may consider using it as a guide when building and configuring the hardware and software of their charging stations.

NIST Standards

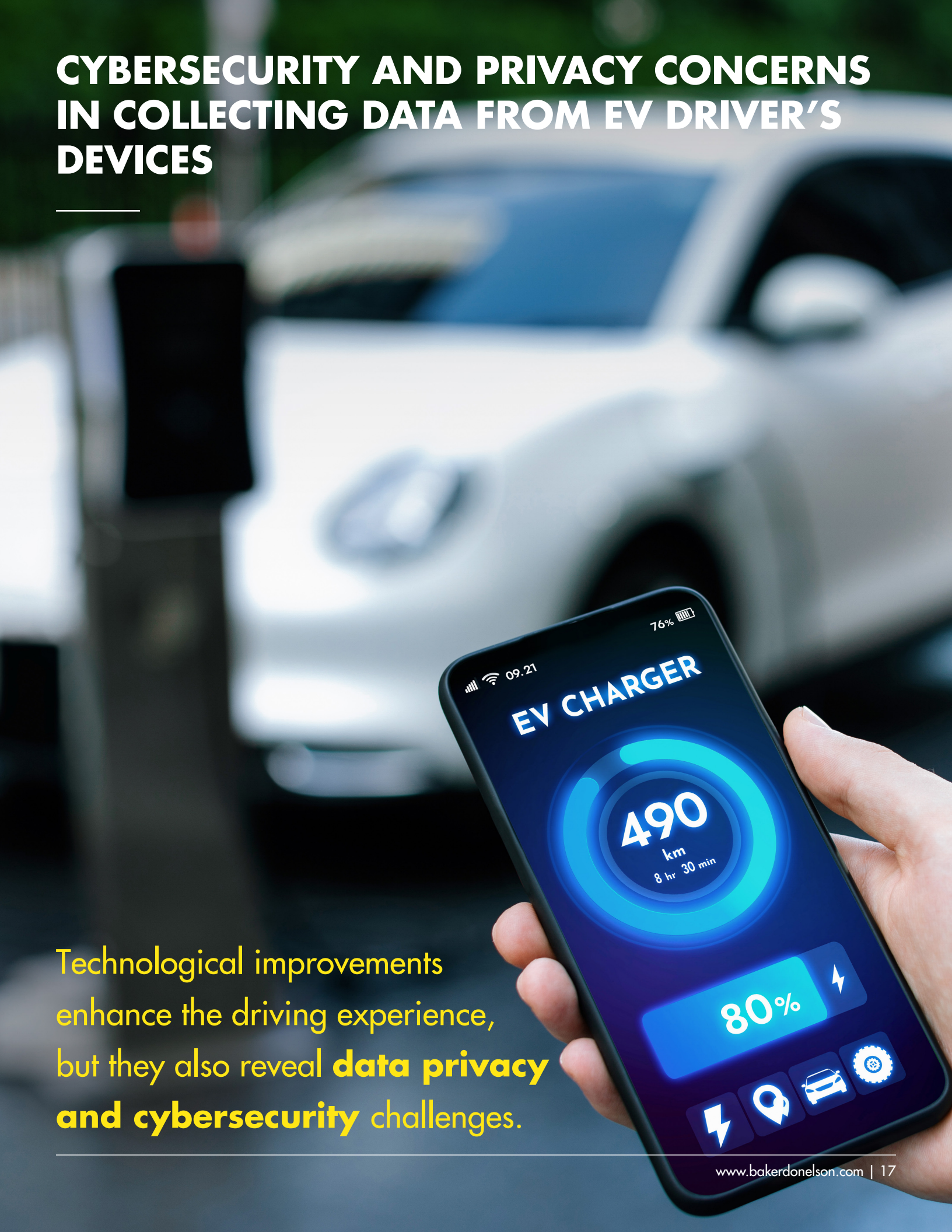
The National Institute of Standards and Technology (NIST) provides non-binding guidelines for technologies and processes. NIST is currently developing a guidance document to provide methods for evaluating EVSEs with commercially available test instrumentation. NIST has previously released a tentative code[10] regarding the operating requirements and transaction capabilities of EVSEs. This tentative code included the recommendation to administer repeated tests for accuracy and consistency. A published guidance document from NIST will have clearer standards for EVSEs and a safe, reliable, and interconnected national network.

BOTTOM LINE

Establishing secure cybersecurity and privacy protocols is paramount to the protection of consumers as EV charging infrastructure is developed across the nation. Different levels of regulators have emphasized this point. To protect sensitive customer data, prevent security breaches, and ensure eligibility for federal and state funds, it is crucial to maintain compliance with federal and state-level regulations and industry standards. Companies constructing EV charging stations should seek guidance from legal counsel on specific requirements and implement the best practices outlined in this article. By doing so, companies can establish safe and secure charging stations that protect their customers' privacy, while contributing to a cleaner and more sustainable transportation system.

[7] "Open Charge Point Protocol (OCPP) Security Explained," *Wevo*, 2022, https://wevo.energy/white-papers/open-charge-point-protocol-ocpp-security-explained.
[8] "ISO 15118-20:2022 Road vehicles – Vehicle to grid communication interface – Part 20: 2nd generation network layer and application layer requirements," *ISO*, https://www.iso.org/standard/77845.html.
[9] "ISO/IEC 27001 Information security management systems," *ISO*, https://www.iso.org/standard/27001.
[10] "3.40. Electric Vehicle Fueling Systems – Tentative Code" *National Institute of Standards and Technology U.S. Department of Commerce*, 2017, https://www.nist.gov/system/files/documents/2016/11/10/3-40-17-hb44-final.pdf.

CYBERSECURITY AND PRIVACY CONCERNS IN COLLECTING DATA FROM EV DRIVER'S DEVICES



Technological improvements enhance the driving experience, but they also reveal **data privacy and cybersecurity** challenges.

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)[1] 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

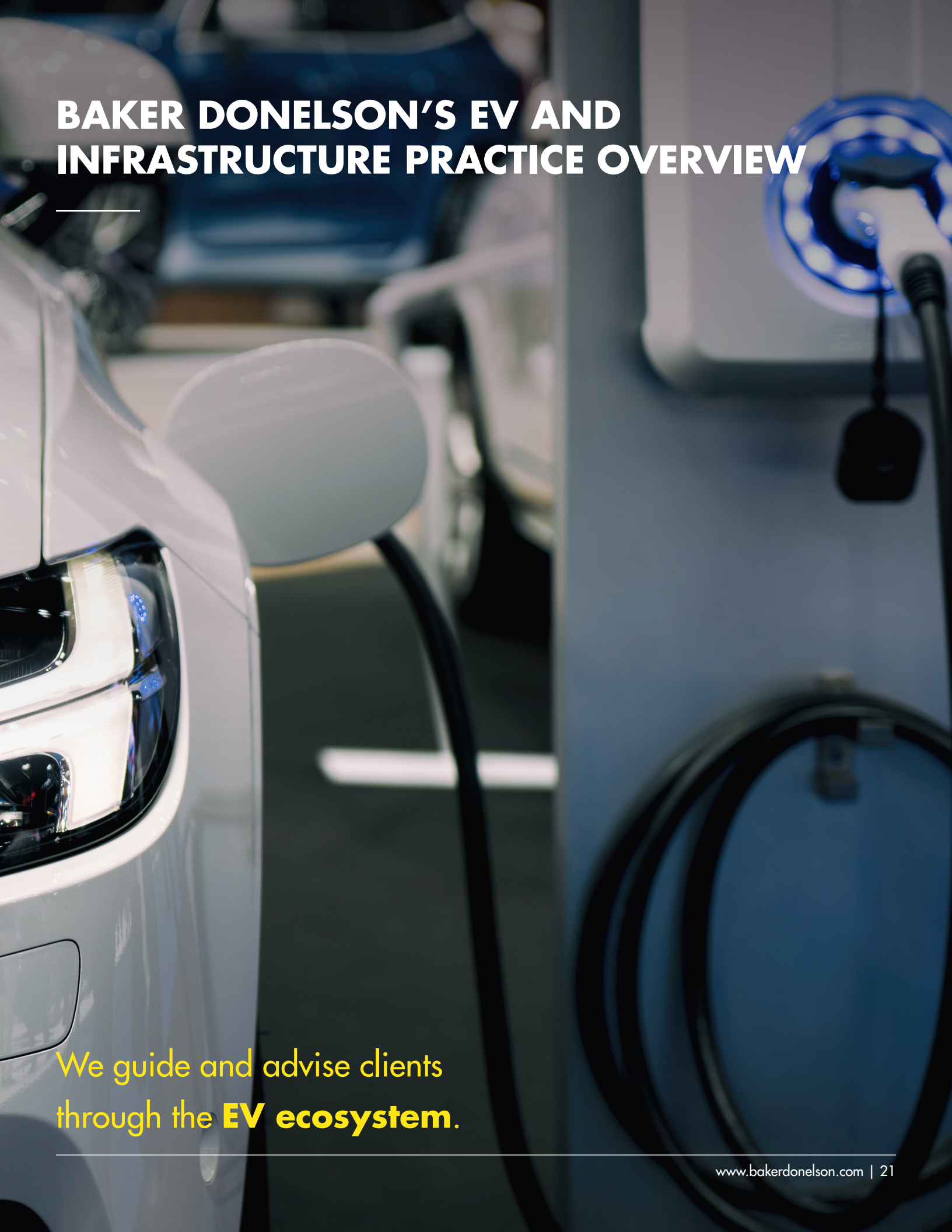
Effectively managing third-party vendors is crucial, given their potential access to data collected by EV apps. Their adherence to privacy standards in handling user data is an important aspect that should not be overlooked, as it helps maintain user trust and solidify data protection.

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.

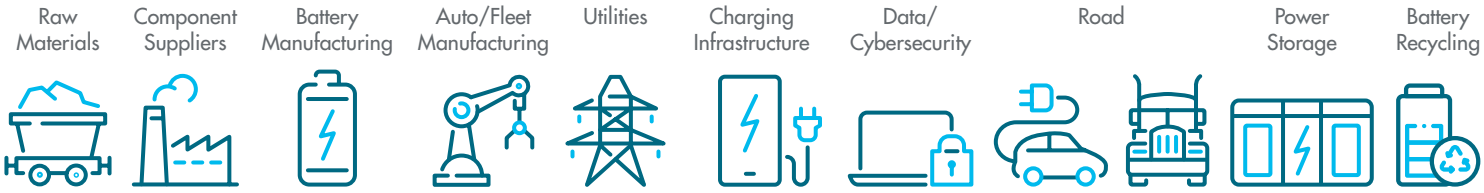
[1] "Chapter 1.5 - Rental Passenger Vehicle Transactions," *Casetext*, https://casetext.com/statute/california-codes/california-civil-code/division-3-obligations/part-4-obligations-arising-from-particular-transactions/title-5-hiring/chapter-15-rental-passenger-vehicle-transactions.

BAKER DONELSON'S EV AND INFRASTRUCTURE PRACTICE OVERVIEW



We guide and advise clients through the **EV ecosystem**.

As a full-service law firm, we support EV manufacturers and suppliers, including software technology and charging system providers, in all legal and business matters such as major transactions, technology, project financing, construction, regulatory, employment, IP, product liability, privacy and data security issues.



Our team stays abreast of issues and developments that arise with the design, manufacturing, production, finance, and distribution of goods in the EV sector, including:

- Experienced energy, corporate, privacy and cybersecurity, technology, intellectual property, construction, environmental, transportation, and real estate attorneys and policy advisors, who assist automotive and other related manufacturing clients in navigating the transition from internal combustion engines to electric vehicles

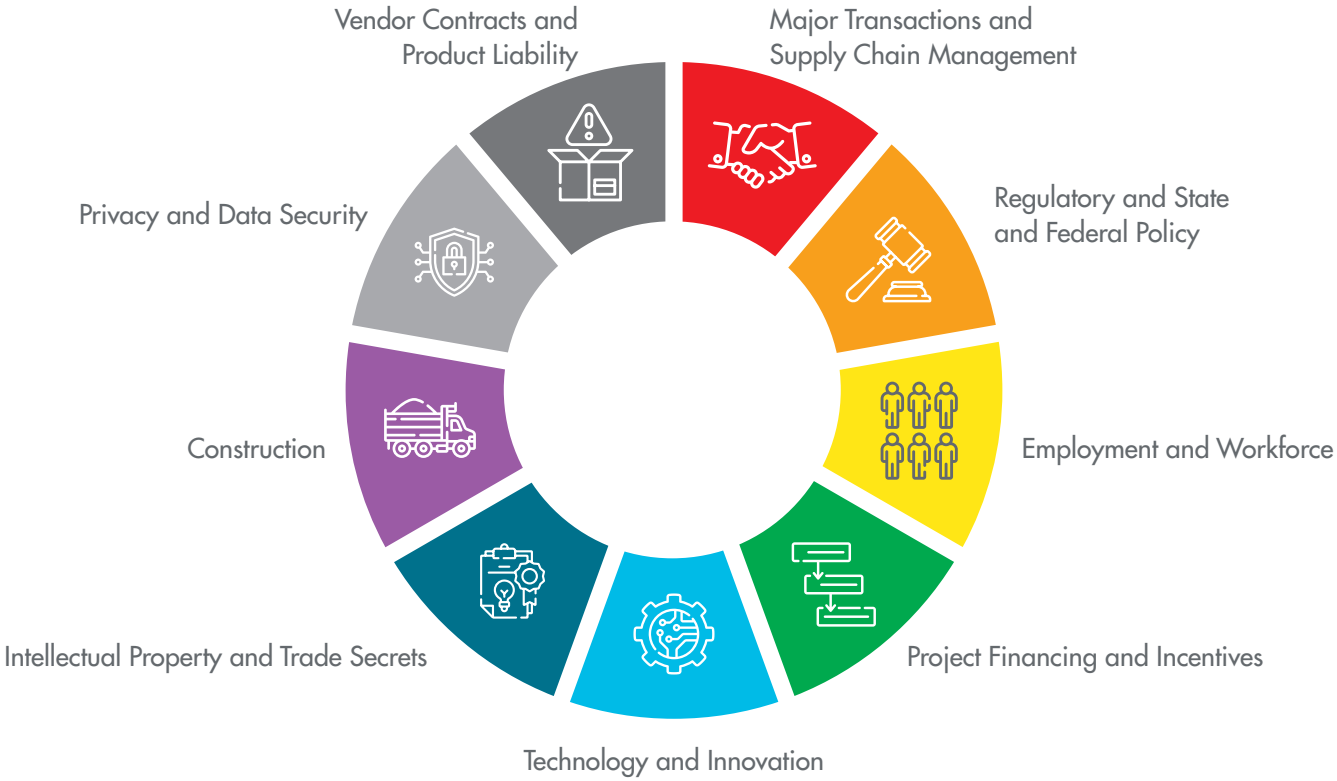
Guide and advise clients through federal and state rules and regulations that may impact:

- EV distribution
- Battery storage
- Vehicle charging and infrastructure
- Sustainable management of the entire EV life cycle to ensure environmental and safety compliance at the state and federal levels

Work with clients on monitoring and gaining access to available tax incentives and grant programs, including:

- Infrastructure Investment and Jobs Act of 2021 (IIJA) that allocates $7.5 billion for EVI nationally
- Inflation Reduction Act of 2022 (IRA) that provides consumers with $14 billion in new tax credits for the purchase of EVs and EV manufacturers with billions in tax and grant incentives
- Significant incentives put in place by state and local governments

Provide strategic guidance to EV manufacturers and suppliers, including software technology and charging system providers, in all legal and business matters.



ALABAMA • FLORIDA • GEORGIA • LOUISIANA • MARYLAND • MISSISSIPPI • NORTH CAROLINA • SOUTH CAROLINA • TENNESSEE • TEXAS • VIRGINIA • WASHINGTON, D.C.

www.bakerdonelson.com