I. INTRODUCTION

Development, testing and commercialization of Autonomous and Connected Vehicles is moving forward at an incredible pace. Indeed, in October of this year, the California Department of Motor Vehicles announced that it will allow autonomous vehicles that lack steering wheels, foot pedals, mirrors, and human drivers to be tested on its roads starting sometime mid-2018.  

While these advances will fundamentally change our relationship with our vehicles, they also raise a host of privacy and data security concerns which, to date, have not been clearly defined. This leaves those in the industry in the dark as to how to ensure they are properly protecting consumers (and themselves) from privacy and cybersecurity pitfalls. These concerns are especially appropriate given legislative activity at the federal and state level, along with the Federal Trade Commission’s (“FTC”) recent announcement that it will use its enforcement power to target entities that fail to have proper privacy and cybersecurity policies and procedures in place.

Although there are currently few binding laws or guidance as to what manufacturers and related entities must do to properly address privacy and cybersecurity concerns, this whitepaper summarizes the current environment facing the Autonomous and Connected Vehicle industry and offers some best practices to be employed while the legal landscape continues to evolve.

II. THE DIFFERING CHALLENGES OF PRIVACY AND DATA SECURITY

Although the terms privacy and data security (or cybersecurity) are often used interchangeably, they represent very distinct concepts and each pose their own unique challenges. To ensure a consistent terminology in this whitepaper, we will differentiate the two

1 Aaron Charfoos is a Member, and Michael Derksen is a Senior Attorney, at Dykema Gossett PLLC. Address questions to the authors at acharfoos@dykema.com and mderksen@dykema.com. The views expressed and positions taken in this paper are solely those of the authors and do not necessarily represent the view and positions of the firm or any of its clients, the University of Michigan or MCity’s participants.


3 This whitepaper relates to best practices and procedures to be utilized in the United States, given that other countries have significantly different regulatory regimes.
early on. On the one hand, privacy refers to an individual’s ability to control the collection and use of their personal information. This is particularly important in the Autonomous and Connected Vehicle context as today’s vehicles can collect and store thousands of gigabytes of data in a single day. Issues such as the actual ownership of the data are beyond the scope of this whitepaper. However, we will explore known restrictions on the use of information and what the proper disclosures may look like. On the other hand, data security or cybersecurity refers to either the protection of the data collected from authorized access and disclosure or, potentially more troubling, the ability of a third party to actually take control of the autonomous and connected vehicle’s systems. 4

III. CURRENT REGULATORY ENVIRONMENT FACING AUTONOMOUS AND CONNECTED VEHICLES

Like many other privacy and data security issues, today’s regulatory environment facing Autonomous and Connected Vehicles represents a patchwork of federal and state legislation, regulatory guidance and other ancillary laws that might be extended to cover Autonomous and Connected Vehicles. 5

A. U.S. Federal Oversight

There is both pending legislation and regulatory guidance at the federal level that directly addresses data security and privacy issues in Autonomous and Connected Vehicles.

1. Federal Legislation

Congress has considered several bills concerning the regulation of autonomous vehicles such as the Let National Highway Traffic Safety Administration Enforce Autonomous Vehicle Driving Regulations Act (LEAD’R Act) (House) and the Renewing Opportunities for Automated Vehicle Development Act (the ROAD Act) (House). However, the House recently passed the Safety Ensuring Lives Future Deployment and Research in Vehicle Evolution (the “SELF DRIVE Act”), 6 and in the Senate, the Commerce Committee recently approved by voice vote the American Vision for Safer Transportation through the Advancement of Revolutionary Technologies Act (“AV START Act”) 7—the companion legislation to the SELF DRIVE Act.

(a) SELF DRIVE Act (House);

The House passed the SELF DRIVE Act on September 6, 2017. The Act would have federal officials set standards for self-driving cars and have regulators develop safety assessments and standards. Pursuant to Section 3, the bill preempts any state or local government

4 University of Michigan Transportation Research Institute, Hack my car? Most believe it can happen (Feb. 7, 2017), http://www.umtri.umich.edu/what-were-doing/news/hack-my-car-most-believe-it-can-happen.
5 Of course, worldwide privacy and data security regimes vary wildly. This whitepaper is strictly limited to U.S. related issues.
law regarding highly automated vehicles (“HAVs”). This bill does have both cybersecurity and privacy impacts.

Pursuant to Section 5, the bill requires a manufacturer to develop a cybersecurity plan including: (1) a written cybersecurity policy concerning the practices of the manufacturer for detecting/responding to cyberattacks, which must include a process for (a) identifying/assessing/mitigating “reasonably foreseeable vulnerabilities from cyber-attacks or unauthorized intrusions” and (b) taking preventative and corrective action to mitigate against vulnerabilities in a HAV or a vehicle that performs partial driving automation; (2) identification of the manufacturer’s point of contact for management of cybersecurity; (3) a process for “limiting access to automated driving systems,” and (4) a process for employee training and supervision with respect to the foregoing.

Under Section 12(1) of the bill (to be implemented by the National Highway Traffic Safety Administration (“NHTSA”)), before selling any HAV, vehicle that performs partial driving automation, or automated driving system, the manufacturer are required to have developed a privacy plan including: (1) how the manufacturer will collect, use, and store data; and (2) a method for providing notice to vehicle owners/occupants about the privacy policy. The bill also provides that the FTC shall treat a violation of the foregoing as an unfair or deceptive act or practice and is empowered to enforce its requirements.

Furthermore, companies are required to explain how customers will be informed about what they are doing with that data and what actions customers can take to prevent the data from being shared.

(b) AV START Act (Senate)

On October 6, 2017, the Senate Commerce Committee approved by voice vote S., 1885, the AV START Act, the companion bill to the SELF DRIVE Act. Like the SELF DRIVE Act, the Senate bill preempts, with a few exceptions, state and local governments from enacting laws or regulations regarding autonomous vehicles, unless identical to Federal Motor Vehicle Safety Standards (“FMVSSs”) issued by NHTSA. However, compliance with FMVSS still would not exempt tort liability at the common law (leaving open state law privacy claims).

While the Senate bill includes cybersecurity provisions, it does not legislate privacy concerns like the House bill. The provisions relating to cybersecurity (see Section 14), include the requirement that manufactures develop and implement cybersecurity plans for their vehicles. Furthermore, it would establish a working group tasked with making recommendations; the working group is required to consist of at least one member who represents a manufacturer of HAVs or automated driving systems. (See Section 10(c)(5)). Other provisions related to cybersecurity are similar, but not identical, to the House bill.

2. NHTSA Guidance

---

8 Note: commercial vehicles are not covered by either bill.
In the absence of federal legislation governing Autonomous and Connected Vehicles, NHTSA has issued several guidance documents in the space.

(a) **NHTSA Cybersecurity Best Practices for Modern Vehicles (October 2016)**

Issued in October 2016, this document sets forth NHTSA’s “non-binding guidance” to the automotive industry for improving motor vehicle cybersecurity. It explains that enhancing vehicle cybersecurity is a top priority of the United States Department of Transportation (“USDOT”) in order “to mitigate threats that could present unreasonable safety risks to the public or compromise sensitive information such as consumers’ personal data.” The document is vague on details, but sets forth general cybersecurity guidance (pp. 10-12), as well as guidance specifically for the automotive industry, including the need for a vehicle development process with explicit cybersecurity considerations in mind, for leadership to make product cybersecurity a priority, to share information related to cybersecurity risks and incidents (which NHTSA began to encourage by creating the Automotive Information Sharing and Analysis Center (“Auto ISAC”), a vulnerability reporting/disclosure program and response process, and self-auditing (pp. 12-17). In sum, NHTSA strongly encourages the automotive industry to collaborate in developing cybersecurity strategies.

The NHTSA document does, however, offer some specific guidance, providing a non-exhaustive list of actions “necessary for securing automotive computing systems,” while noting that all recommendations may not always be applicable (pp. 17-22). These actions include:

- **Electronic Control Units (“ECUs”)**: limit developer/debugging access in production devices;

- **Control Keys**: secure keys and ensure that “any key obtained from a single vehicle’s computing platform should not provide access to multiple vehicles”;

- **Control Vehicle Maintenance Diagnostic Access**: Limit diagnostic features and design diagnostic operations to eliminate or minimize dangerous ramifications occasioned by misuse or abuse;

- **Control Access to Firmware**: Employment of safe security coding practices that support security outcomes in development processes; consider utilization of encryption where possible and minimize/eliminate opportunities for unauthorized access to unencrypted firmware during software access;

---


10 Auto ISAC’s Cybersecurity Best Practices can be found at https://www.automotiveisac.com/best-practices/.
• **Limit Ability to Modify Firmware**: This would make it more challenging for malware to be installed on vehicles;

• **Control Proliferation of Network Ports, Protocols and Services**: use of network servers on vehicle ECUs should be limited to essential functionality; service over network ports should be protected, and any unnecessary network services should be removed;

• **Use Segmentation and Isolation Techniques in Vehicle Architecture Design**: Ensure that if access is gained to one system it will not allow for lateral movement to other systems;

• **Control Internal Vehicle Communications**: secure internal communications;

• **Log Events**: include logging activities to facilitate diagnostics for improvement and incident response;

• **Control Communication to Back-End Servers**: protect communications from the vehicle to other servers; and

• **Control Wireless Interfaces**: ensure that wireless interfaces cannot be used to perpetuate an attack or intrusion.

(b) **Federal Motor Vehicle Safety Standard ("FMVSS") 150**

On January 12, 2017, NHTSA issued a notice of proposed rulemaking to establish FMVSS 150, which would mandate vehicle-to-vehicle ("V2V") communications for new light vehicles and standardize the message and format of V2V transmissions. Among other things, FMVSS 150 contains more extensive privacy and cybersecurity requirements than in other NHTSA guidance documents.

*Privacy*: The FMVSS 150 begins with the assumption that "V2V systems would be required to be designed from the outset to minimize risks to consumer privacy." The standard contemplates: a) incorporating Privacy By Design, a well-known concept in the privacy community, into the development of V2V communications including removing vehicle identifying information from communications; b) increased transparency and choice on the

---

11 Information available at https://icsw.nhtsa.gov/safercar/v2v/


13 Although relevant to the criminal context, the U.S. Supreme Court in *Carpenter v. United States of America*, (No. 16-402), is deciding whether U.S. citizens have a reasonable expectation of privacy in the geolocation information as measured by Cell Site Location Information ("CSLI"). In general, the Telecommunications Act designates cell phone location information as a category of records that a telecommunication provider cannot disclose without the approval of the customer. 47 U.S.C. § 222(c)(1)-(2), (h)(1)(A). This information would be analogous to geolocation information being gathered by an automobile and could be subjected to similar restrictions based on similar bases.
vehicle owner’s part (specifically relying on the Alliance of Automobile Manufacturer’s Privacy Protection Principals discussed below); c) provides a Privacy Notice that manufacturers would be required to send to provide with the new vehicles; and d) calls for additional research and investigation to a number of areas impacting privacy.

Cybersecurity: The FMVSS also proposes a number of cybersecurity measures relating to not only the protection of the V2V communications themselves, but also to hardening of the vehicle’s architecture, protection against malware and other measures. In addition, the standard specifically calls out the National Institute of Standards and Technology (“NIST”) Cybersecurity Framework as a tool for the development of cybersecurity measures in this area.

NHTSA has received numerous comments regarding FMVSS 150, many of which raise additional privacy concerns, including that FMVSS may fail to contain adequate measures to protect consumer privacy from third parties—specifically, that the privacy protections “may be easily circumvented” by parties seeking to perform large-scale, real-time tracking of multiple vehicles, and that the proposed privacy statement fails to adequately disclose these threats to consumers.14

(c) Automated Driving Systems: A Vision for Safety 2.015

On September 12, 2017, NHTSA released new “voluntary” federal guidance:16 Automated Driving Systems: A Vision for Safety 2.0. Generally speaking, this guidance document advocates that the automotive industry, state and local governments, safety and mobility advocates and the public work together “to lay the path” regarding the deployment of autonomous vehicles. It does contain a section that specifically addresses cybersecurity. However, much like other NHTSA guidance documents, it simply encourages the creation of product development processes that minimize cybersecurity threats and vulnerabilities, which should include a “systematic and ongoing” safety risk assessment for all automated driving systems (“ADSs”) and to follow established best practices, such as those promulgated by the NIST, NHTSA, SAE International, the Alliance of Automobile Manufacturers, the Association of Global Automakers, and Auto ISAC.

The document further encourages entities to document


16 Available at https://www.nhtsa.gov/technology-innovation/automated-vehicles
how vehicle cybersecurity considerations are incorporated into their ADSs, and, like other guidance documents discussed herein, to engage in information sharing. Finally it suggests that entities should consider adopting a “coordinated vulnerability reporting/disclosure policy.”

B. Few States Have Directly Relevant Laws

Much like at the federal level, state governments have done little, if anything, to clarify requirements related to privacy and cybersecurity policies and procedures for autonomous and connected vehicles. According to the National Conference of State Legislatures,\(^\text{17}\) thirty-three (33) states introduced legislation related to autonomous vehicles in 2017 alone, twenty-one (21) states\(^\text{18}\) (as well as Washington D.C.) have already passed legislation related to autonomous vehicles, and governors in five (5) states\(^\text{19}\) have issued executive orders related to autonomous vehicles. However, nearly all of the legislation is related to testing Autonomous and Connected Vehicles and generally do not address specifics related to data privacy or cybersecurity issues or requirements.

Those bills that do discuss privacy or data security typically lack much detail. For example, Michigan Senate Bill No. 996 simply requires automakers to “make publicly available a privacy statement disclosing its data handling practices . . .” Michigan Senate Bill No. 996 at Section 665b(3)(f). On the other hand, several states have established various groups to study the subject. Delaware established an Advisory Council on Connected and Autonomous Vehicles that tasks the advisory group to issue recommendations relating to “Technology, security and privacy.” Executive Order 14.

Of course, if the Federal AV START Act or the SELF DRIVE Act pass in their current form, state and local regulations will be preempted.

C. Ancillary Rules and Regulations Potentially Impacting Autonomous and Connected Vehicles

In addition to rules and regulations that are directed to Autonomous and Connected Vehicles, there are a number of other sources of rules and regulations that the industry may face.

1. Federal Trade Commission

The Federal Trade Commission has authority under Section 5(a) of the Federal Trade Commission Act (FTC Act) to prohibit “unfair or deceptive acts or practices in or affecting


commerce.” (15 USC §45). The FTC has applied this over the last decade to a number of privacy and data security investigation and enforcement actions. 20 The area where the FTC is most likely to assert its powers would be instances where Autonomous and Connected Vehicle privacy notices do not match up with manufacturers actual practices (deceptive trade practices) or where manufacturers are using vehicle data for improper purposes that the drivers would not have reasonably contemplated and cannot stop (unfair practices).

### 2. State Privacy Laws

Many states have laws that impact privacy (invasion of privacy) or cybersecurity (data breach and negligence laws). In terms of an individual’s expectation of privacy, generally all states agree that there are no restrictions if the persons or property are in a public place. Generally speaking, when an individual is out on public streets, open-air parking lots, and other places generally open to the public they have no expectation of privacy. The same is true for license plate numbers, other identifying markings, etc. that are visible in public. Therefore, any camera footage captured or stored by the Autonomous or Connected Vehicles in those places should not pose a privacy issue. However, individuals (particularly those who are not the driver and are unaware that they are being recorded) may have an expectation of privacy in certain traditionally private places, such as in their home, private parking garages, etc. While these laws differ from state to state, Autonomous and Connected Vehicle manufacturers should be aware that video or audio information may contain information that could be construed as private depending on when and where it is collected.

### 3. Wiretap Laws

Autonomous and Connected Vehicles might incorporate audio recording inside the vehicle for a variety of reasons including to provide hands free access to vehicle or smart phone controls. Many of these kinds of systems record and/or transmit this audio information and may implicate federal and state wiretap laws. Federal law (and, in particular, 18 U.S. Code § 2511(2)(d)) permits recording of communications (wire, oral, etc.) so long as (a) the person doing the recording is a party to the communication or (b) one of the parties to the communication has given prior consent to such recording. This is commonly referred to as "one-party consent." This law does not cover video recordings. In this context, as long as one passenger of the car (likely the vehicle owner or someone made aware by a disclosure) is aware that the conversations inside the car are being recorded, then the one-party consent laws are satisfied.

With respect to state wiretap laws, most states are also one-party consent states like the federal law. That said, at the current time, 11 states (California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, and Pennsylvania) require that all parties consent to the recording (and such states are generally referred to as "all-
party” states). Therefore, all passengers of the car would need to be notified that their conversations were being recorded.

4. **Event Data Recorder Laws**

“Event data recorders” are regulated devices in the United States. *See 49 CFR § 563.* Autonomous or Connected Vehicles would generally speaking, not be "event data recorders" under U.S. law because of the substantial capabilities of the vehicles, *i.e.* they are not simply designed to capture crash information (such as the change in vehicle speed, airbag deployment, etc.) during a crash event.

However, a strict reading of parts of federal or state law could include Autonomous and Connected Vehicles because they may store changes to vehicle speed before, during and after a crash. However, a practical reading of the applicable law and National Highway Traffic Safety Administration guidance suggests strongly that its primary focus is on OEM installed event data recorders intended to store information on crash events only (which the car would have in addition to its internal systems). If Autonomous and Connected Vehicles are found to be event data recorders under the law, the law would require the vehicle systems to both be engineered to withstand a car crash and to capture much more data about the crash than is currently intended.

5. **PCI-DSS** and Other Financial Laws

To the extent that vehicles begin to store credit card, financial account or other payment information (for example to expedite checkout at drive-thrus), they may become subject to standards like PCI-DSS or other financial laws.

**IV. BEST PRACTICES**

Because the legislative, regulatory and technical landscape continue to change, Automated and Connected Vehicle manufacturers will need to be very forward thinking in implementation of policies and practices that anticipate where the industry will be in the future not where it is now. Below are a number of suggested best practices.

A. **Understand What Kind Of Data And Communications Are At Issue**

Obviously, the first step in any privacy or data security analysis is to understand what kinds of data are being collected, how (and for how long) they are being retained and what the information is being used for. Whenever possible, organizations should conduct a thorough data inventory and mapping exercise. It is very common for even the most involved and educated business or technical members of the team to be unaware of what data is collected and how it is being used outside of their direct universe – particularly in complex organizations. Moreover,

---


22 [https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf](https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf)
this inventory should be updated periodically to reflect the most up to date snapshot of the organization.

In the context of Autonomous and Connected Vehicles, it is also helpful to be able to categorize this data into broad uses. Although not directly relevant to vehicles sold and operated in the United States, the French Data Protection Authority, (the “Commission Nationale de l’Informatique et des Libertés” or “CNIL”), recently published a connected cars compliance package that provides a useful framework for categorizing data that may help narrow the cybersecurity and privacy implications of various pieces of information.23

In particular, the compliance package differentiates between three general types of information:

- **In-In**: This is information which is generally created by the vehicle and stays within the vehicle (or only provided to the user’s smartphone or other device). Cybersecurity would mostly be focused on the vehicle architecture itself. In addition, this would likely be the most closely guarded information given the automobile user’s expectation of privacy.

- **In-Out**: This is information that is transmitted from the vehicle to a service provider. Examples would include driving information to be used by insurers for determining policy rates, etc. Cybersecurity concerns are broadened beyond the vehicle itself to the communications pathways and protections at the service provider’s location as well. Key privacy issues here involve transparency and choice given the uses of the information. The uses of the data will likely be more limited given the specific expectation of the driver that it will be used for particular purpose (i.e. insurance rate information only).

- **In-Out-In**: These are communications that originate in the vehicle, are transmitted to a service provider who processes the data and then returns new information to the vehicle. Examples of In-Out-In data may include analyzing error information and alerting the driver that parts of the vehicle may need repair or providing real-time traffic and routing information. Like In-Out communications, the cybersecurity concerns are much broader given the stream of data to and from the vehicle. Key privacy issues here remain transparency and choice. However, given the interactive nature of much of this information, drivers and users of the vehicle might be willing to accept broader uses of their data (such as contacting the nearest service center or an appointment or suggesting local restaurants along an anticipated route).

Autonomous and Connected Vehicle manufacturers may want to take this more nuanced approach to their privacy and data security programs to balance the privacy and security of the data with the commercial uses of the information being generated.

---

B. “Reasonable” Cybersecurity

A recommendation regarding the specific cybersecurity protocols is both beyond the scope of this whitepaper and would, in all likelihood, quickly be outdated by advances in security technology and threats. However, in the absence of specific requirements in either regulatory guidance or legislation, companies will need to adopt “reasonable” cybersecurity practices. Both existing Autonomous and Connected Vehicle guidance and pending legislation, along with, established cybersecurity practices in other areas provide some insight into what would be reasonable.

Follow An Accepted Standard: The FMVSS specifically calls out the use of various standards including the NIST Cybersecurity Framework. Similarly, in other contexts, governmental entities have encouraged the use of the Center for Internet Security (“CIS”) Standards (CIS Controls and CIS Benchmarks), which are considered industry best practices that may meet the reasonableness test.

Keep Up to Date: Both technical and legislative developments will continue to change what may be considered reasonable. Companies will need to ensure that they have an effective program in place to identify and adapt to changes in this space.

Systems Need To Be Adaptable: Systems must be able to be easily updated to keep up with new and more sophisticated threats. As recent security research on the vulnerabilities of the CAN communications protocol make clear, low level protocols that are difficult, or even impossible, to update can become enormous targets for hackers. From a security perspective, advances in vehicle communications pose a double-edged sword here. On the one hand, they allow for systems to be updated without trying to force owners to physically bring their vehicles in for service. On the other hand, these over the air communications provide an attack vector for hackers.

C. Establishing a Privacy Framework for the Future

Like cybersecurity, Autonomous and Connected Vehicles are subject to very few privacy restrictions. But that does not leave manufacturers completely without guidance.

1. Consumer Privacy Protection Principles

On November 14, 2014, members of the Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc. issued their Consumer Privacy Protection Principles:

---

25 https://www.cisecurity.org/controls/
26 https://www.cisecurity.org/cis-benchmarks/
Principles For Vehicle Technologies And Services. Given the public nature of the document, the FTC may seek to enforce it in a way similar to a privacy notice on a website. The document sets out seven principles:

1. Transparency: Owners and registered users should have “access to clear, meaningful notices about Participating Member’s collection, use and Sharing of Covered Information.”

2. Choice: Owners and registered users should have “choices regarding the collection, use and sharing of Covered Information.”

3. Respect for Context: Information should be used and shared consistent with the context in which it was collected.

4. Data Minimization, De-Identification and Retention: Vehicle manufacturers should only gather as much information as needed and only keep it as long as is needed.

5. Data Security: Vehicle manufacturers should adopt “reasonable measures” to protect Covered Information.

6. Integrity and Access: Vehicle manufacturers should try to ensure that the data gathered is correct and give owners and registered users the ability to review and correct the data.

7. Accountability: Vehicle manufacturers should ensure that they commit and adhere to the principles.

These are concepts that are relatively familiar to many privacy professionals and have been implemented in many other concepts.

2. Privacy by Design

One way to ensure that privacy considerations are regularly included in Autonomous and Connected Vehicles is to adopt a Privacy by Design philosophy in the design and development process (specifically required in FMVSS). Privacy by Design is an approach to engineering which takes privacy into account throughout the whole engineering process. Depending on the nature of the information being assessed, privacy could either be presumed to be the default setting (i.e. all things will be private) or simply that privacy principles will be assessed at each stage of the review. Ensuring that a seasoned privacy professional is involved in the process can inject and import and healthy debate into how consumer and driver’s information can, and should, be used.

---


29 Covered Information generally includes identifiable information and subscription information. Id. at page 4.
Nevertheless, Autonomous and Connected Vehicles do pose particular issues that are more in line with privacy concerns in the smartphone industry. For example, how can the driver be presented with this information on relatively small screens so that they can be updated as the policy changes. Similarly, what kind of privacy concerns arise when people other than the owner use the car? These are logistical issues that should be taken into account in the design of a privacy program and reference to other industries’ best practices can be helpful.

V. CONCLUSION

As with so many other areas, the rapid advances in technology have outpaced federal and state legislatures ability to regulate privacy and data security concerns in Autonomous and Connected Vehicles. However, that does not mean that vehicles are without any regulation and Autonomous and Connected Vehicle manufacturers will need to be similarly forward thinking in the way they address the emerging regulatory and technical landscape.