Connected and Automated Vehicle Data Issues and Opportunities

---

Texas CAV Task Force White Paper Subcommittee on Data, Connectivity, Cybersecurity, and Privacy

Authors:
Data, Connectivity, Cybersecurity, and Privacy Subcommittee of the
Texas Connected and Autonomous Vehicles Task Force
Johanna Zmud, Texas A&M Transportation Institute

June 3, 2021

Table of Contents

List of Figures

List of Tables

Acknowledgments

The Texas Connected and Autonomous Vehicles (CAV) Task Force would like to acknowledge and thank all of its voting and participating membership and the members of this subcommittee for their hard work and many hours dedicated to developing this white paper. We would especially like to thank the contributing authors of this paper for taking the thoughts of so many and combining them into one well-written document. In addition, special thanks go to Beverly Kuhn, Ed Seymour, and Robert Brydia of the Texas A&M Transportation Institute for their management, creativity, and patience in assisting the Texas CAV Task Force Texas Department of Transportation team and subcommittee chairs. Finally, the Texas CAV Task Force would like to thank Texas Governor Greg Abbott and his staff for their guidance and vision in creating this Texas CAV Task Force. Texas is better prepared for CAVs due to their leadership.

Disclaimer

The contents of this white paper reflect the views of the Texas CAV Task Force members, who are responsible for the information presented herein. The contents do not necessarily reflect the official views or policies of the State of Texas or any Texas state agencies. The white paper does not constitute a standard, specification, or regulation, nor does it endorse standards, specifications, or regulations. This white paper does not endorse practices, products, or procedures from any private-sector entity and is presented as a consensus broad opinion document for supporting and enhancing the CAV ecosystem within Texas.

Texas CAV Task Force Charter

The Texas CAV Task Force was created at the request of Texas Governor Greg Abbott in January 2019. The Texas CAV Task Force is responsible for preparing Texas for the safe and efficient rollout of CAVs on all forms of transportation infrastructure.

The primary functions are:

1. Coordinating and providing information on CAV technology use and testing in Texas.
2. Informing the public and leaders on current and future CAV advancements and what they mean in Texas. This process includes reporting on the current status, future concerns, and how these technologies are changing future quality of life and well-being.
3. Making Texas a leader in understanding how to best prepare and wisely integrate CAV technologies in a positive, safe way, as well as promoting positive development and experiences for the state.

The Texas CAV Task Force is composed of a voting group of no more than 25 members and represents the full spectrum of CAV stakeholders.

Terminology Note

The Texas CAV Task Force addresses the full spectrum of connected, automated, and autonomous vehicles. An *automated vehicle* refers to a vehicle that may perform a subset of driving tasks and require a driver to perform the remainder of the driving tasks and supervise each feature's

performance while engaged. A *fully autonomous vehicle* refers to a vehicle that can perform all driving tasks on a sustained basis. These definitions are still blurred in common discussions and language. Currently, the industry is developing automated vehicle capability while pursuing fully autonomous vehicles. The white papers generally use the term *autonomous* to refer to the vehicles with fully autonomous capabilities and the term *CAV* to refer to the grouping of connected, automated, and autonomous vehicles. Please see the "CAV Terminology" white paper for a full listing of terms and definitions used in this developing technology ecosystem.

List of Terms and Acronyms

ATCMTD	Advanced Transportation and Congestion Management Technologies Deployment
AV	automated vehicle
BSM	basic safety message
CAV	connected and autonomous vehicle; also, connected and automated vehicle
CCPA	California Consumer Privacy Act
CV	connected vehicle
C-V2X	cellular vehicle to everything
DAVI	Data for Automated Vehicle Integration
DOT	Department of Transportation
DSRC	dedicated short-range communications
EDR	event data recorder
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FTC	Federal Trade Commission
GDPR	General Data Privacy Regulation
GPS	global positioning system
HAV	highly automated vehicle
HD	high definition
IEEE	Institute of Electrical and Electronics Engineers
ITS	intelligent transportation system
ML	machine learning
NCSL	National Conference of State Legislatures
NHTSA	National Highway Traffic Safety Administration
OBU	onboard unit
ODD	operational design domain
OEM	original equipment manufacturer
PII	personally identifiable information
RSU	roadside unit
SPaT	Signal Phase and Timing
TxDOT	Texas Department of Transportation
USDOT	U.S. Department of Transportation

V2C	vehicle to cloud
V2I	vehicle to infrastructure
V2N	vehicle to network
V2P	vehicle to pedestrian
V2V	vehicle to vehicle
V2X	vehicle to everything

Executive Summary

Automated vehicles (AVs) represent a switch in driving responsibility from human to machine to improve driving safety and efficiency. Connected vehicles (CVs), in contrast, have internal devices that enable wireless communication with devices internal and external to the vehicle for enhanced safety and other functionality. Questions about AVs and CVs do not now revolve around whether such technologies should or should not be implemented; they are already with us. Current decision making should revolve around how to shape their deployments to benefit Texas and its citizens.

In Texas, public agencies and private companies are partnering to ensure a safe and successful integration of both AVs and CVs into the state's transportation ecosystem. Such technologies bring opportunities to reduce crashes and improve roadway safety, along with quality-of-life, economic, and environmental benefits. However, a safe and successful integration depends on understanding and addressing an array of critical policy and planning issues related to vehicle data.

AVs and CVs use an array of sensors and other technologies to collect vast amounts of data from their own vehicles and the environment around them, as well as rely on volumes of different types of data from various sources to operate safely. Thus, data privacy, data security, and cybersecurity are important concepts in the context of AVs and CVs. *Data privacy* relates to the collection, access, and use of sensitive personal information, such as geolocation, driver behavior, or biometrics. Without necessary protections to prevent breach of personal information emanating within and from AVs and CVs, harm could occur to numerous individuals, organizations, and agencies. *Cybersecurity* refers to security protections for systems in the vehicle that actively communicate with other systems or other vehicles. Recent data indicate that cyberattacks aimed at vehicles are on the increase. Some of the biggest risks relating to data privacy or cybersecurity are related to data security (or access). Risks exist if AV or CV data are accessed by third parties that are not committed to privacy principles or that cannot protect vehicle systems from cyberattack.

AVs and CVs bring many data challenges due to the sheer volume of data that is involved. And the testing phases of AVs and CVs (which are where the industries are focused now) generate more data than the operational phases. Therefore, confronting the aforementioned data issues, as well as the critical issue of who owns these data, is a priority now. Data ownership directly affects who can collect, access, use, and benefit from vehicle data. It is an evolving challenge that needs to be understood and eventually resolved. Data ownership, and other data issues, requires ongoing collaboration among public- and private-sector stakeholders to address such questions as:

- Which entities are collecting, storing, and using what AV and CV data?
- What data gaps exist that hinder innovation and furthering the public interest?
- What data can be shared or exchanged to facilitate the safe and successful integration of AVs and CVs into the transportation ecosystem?

Answering these questions will begin to clarify how Texas can continue to be an innovation leader in these emerging vehicle technologies to the benefit all Texas citizens.

Introduction

In Texas, the push toward emerging transportation technologies, like connected vehicles (CVs) and automated vehicles (AVs), is strong. Such technologies have the potential to greatly reduce crashes and improve roadway safety over time. These technologies also provide opportunities to reimagine personal mobility and commercial transport with quality-of-life, economic, and environmental benefits.

Texas's push is guided by circumstances that make it among the nation's innovation leaders. The state has a start-up culture, world-class research universities, and a skilled workforce. Early on, the Texas Technology Task Force and the Texas Innovation Alliance established a solid foundation for research, collaboration, and innovation across the state. The Texas AV Proving Ground Partnership was one of 10 pilots designated by the U.S. Department of Transportation (USDOT) in 2017 to encourage testing and information sharing around these technologies. USDOT later rescinded all U.S. proving grounds. State laws allow automakers and others to test AVs without a driver inside and the use of connected braking systems on the state's roads and highways. Texas has an active 5.9-GHz intelligent transportation system (ITS) license and has numerous active CV deployments. The Texas Connected and Autonomous Vehicles (CAV) Task Force is building on the momentum already established in the state. This white paper presents a technical brief on key issues relating to CV and AV data, reflecting the combined perspective of a specialized subcommittee of the Texas CAV Task Force.

AVs and CVs are distinct technologies. AVs represent a switch in driving responsibility from human to machine to improve driving safety and efficiency. CVs, in contrast, have internal devices that enable wireless communication with devices internal and external to the vehicle for enhanced safety and other functionality. While CVs are expected to enhance the benefits of vehicle automation, the deployment of CV technology is not a precondition to the deployment of AVs. In other words, not all AVs will be CVs, and not all CVs will also be AVs. AVs and CVs use an array of sensors and other technologies to collect vast amounts of data from their own vehicles as well as the environment around them. The data that AVs and CVs capture, store, and share will play a critical role in their testing and deployment and in optimizing vehicle and network performance, enhancing the vehicle user experience, and improving safety. However, data-related technical and policy issues may pose challenges in both AV and CV development and public acceptance.

This paper starts with a brief description of AVs and CVs and related policy issues as foundational information for the subsequent discussion of data issues and to place the data issues in the context of the current state of technology development. The paper identifies the types of data that CVs and AVs use to operate safely, as well as data that they generate. The paper also raises opportunities and challenges, and provides examples of data-sharing and data-exchange activities. These technologies have facilitated (and will continue to enable) collaborative associations among automakers, other original equipment manufacturers (OEMs), technology firms, communications firms, and other businesses outside the realm of the traditional automotive industry; and among various public-sector entities.

Connected Vehicles

CVs have internal devices that enable wireless communication with devices internal and external to the vehicle for enhanced safety and other functionality.

According to the Institute of Electrical and Electronic Engineers (IEEE), the term *connected vehicles* refers to "applications, services, and technologies that connect a vehicle to its surroundings" (1). More specifically, a CV has various communication devices (embedded or portable) that enable in-car connectivity with other devices present in the vehicle and/or enable wireless connection of the vehicle to external devices, networks, applications, and services. In 1996, General Motors, working with Motorola, pioneered the first CV service. Its OnStar telematics system was a subscription-based safety service that enabled voice calls to a call center that contacted emergency responders when an airbag was deployed (2). Over time, the functions supported by vehicle connectivity have changed. For example, soon after the OnStar launch, global positioning system (GPS) locational systems were added to support navigation, safety, and anti-theft services. The increased functionality occurred as an ever-increasing collection of technologies has been pushed to market by OEMs and other entities, such as navigation services (e.g., Garmin) and technology companies (e.g., Apple CarPlay and Android Auto).

Types of CV Applications

Today, CV systems support a variety of safety, convenience, navigation, infotainment, and vehicle diagnostics applications. Because the CV ecosystem is complex, there have been many proposed approaches for categorizing the functions supported by CV systems. The Information Technology and Innovation Foundation identified four types of CV applications based on how they connect with the vehicle, the user, a service, or other vehicle and infrastructure systems (3). The four types are described as follows and also summarized in Table 1:

- **In-vehicle** applications involve communications that primarily occur within the vehicle between its various parts and are oriented toward safety or maintenance. Since 1996, cars have been legally required to have onboard units (OBUs), which gather information on engine problems, maintenance status, fuel efficiency, etc. These data are sent wirelessly to vehicle manufacturers or their third-party suppliers, and also may be accessed by drivers through aftermarket devices and smartphone apps.
- **Driver and passenger** applications relate to navigation, entertainment, or remote control of the vehicle. These applications also connect directly to personal devices, enabling internet services within the vehicle.
- **Third-party service** applications support a range of both private-sector services (e.g., in-car payment services, vehicle recovery systems, roadside assistance apps, and insurance) and public-sector services (e.g., mileage-based usage fees, road pricing fees, and smart parking).
- **Infrastructure and other road user** applications refer to an evolving group of vehicle communications, known as vehicle-to-everything (V2X) technologies.

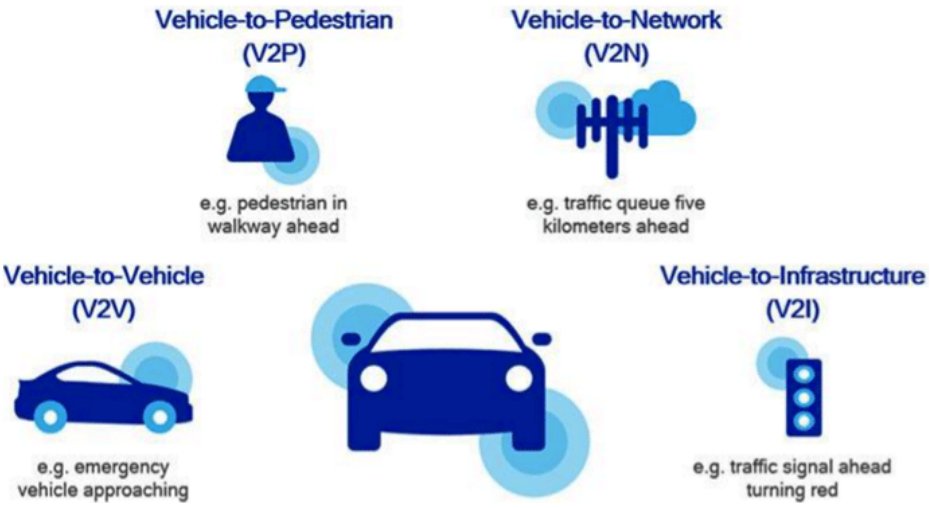
Table 1. Types of CV Applications Based on Type of Interaction.

Type of CV Application	Description	Examples
In-vehicle	Applications that involve interactions between different components within the vehicle	Diagnostics, predictive maintenance, and safety applications such as blind-spot warnings
Driver and passenger	Applications that involve interactions with a user within the vehicle	Entertainment, navigation, personal device integration, remote control, Apple Car Talk, and Google Android Auto
Third-party service	Applications that facilitate transactions with third parties using the vehicle	In-car payment services, roadside assistance, insurance, and tolling
Infrastructure and other road user	Applications that primarily operate through interactions with other vehicles and connected infrastructure; also known as V2X	Crash response, adaptive traffic lights, emergency vehicle warnings, queue and work zone warnings, and integrated smart home technologies

Source: McQuinn and Castro (3)

The fourth type of CV applications, V2X, is powerful because it takes advantage of the synergy between different communications technologies, making the whole greater than the sum of its parts (see Figure 1). Such communication technologies include (4):

- **Vehicle to vehicle (V2V)** enables vehicles to exchange data (e.g., speed, location, and heading) wirelessly in real time for safety purposes via the 5.9-GHz spectrum band.
- **Vehicle to infrastructure (V2I)** enables vehicles to exchange data with road infrastructure and roadside units (RSUs) for safety, environmental, mobility, and other benefits.
- **Vehicle to pedestrian (V2P)** enables network infrastructure to communicate vehicle actions to different vulnerable road users, such as pedestrians and bicyclists.
- **Vehicle to network (V2N)** allows vehicles to use cellular networks to communicate with a V2X management system or enables vehicles to interact with other vehicles and road infrastructure.
- **Vehicle to cloud (V2C)** leverages V2N access to broadband cellular mobile networks to offer data exchange with the cloud. Many of the V2V, V2I, or V2P applications conceptualized as being handled via OBUs/RSUs can be handled via these cellular vehicle-to-everything (C-V2X) connections.



Source: Malinson (5)

Figure 1. V2X Communication Technologies.

CV Connectivity

Connectivity for the different types of applications is enabled through various means. At its simplest, some CVs offer Bluetooth® to link wirelessly to other devices, such as smartphones, within short distances of the vehicle to enable hands-free calling, locking and unlocking mechanisms, etc. Beyond this, there have been two categories of vehicle communications (6).

The two basic types of V2X communications are:

- *DSRC using the underlying radio communications provided by IEEE 802.11p.*
- *Cellular-based V2X (C-V2X).*

The first is dedicated short-range communications (DSRC), which uses the underlying radio communication provided by IEEE 802.11p. It has extremely low latency (i.e., it is fast) and has minimum delay (i.e., enables high data transmission rates), which are required to safely manage multiple vehicles in traffic in real time. Up until recently, DSRC has been the only V2X communication technology available.

The second is C-V2X. In 2016, the standards organizations that develop protocols for mobile telecommunications (3rd Generation Partnership Project) published V2X specifications based on wireless broadband communication as the underlying technology, known as C-V2X. In addition to the direct communication (i.e., V2V and V2I), C-V2X also supports wide-area communication over a cellular network (V2N). 5G is expected to be a key enabler of more reliable cellular communication for V2X applications. With lower latencies, C-V2X may allow more robust V2C operations (i.e., direct from the cloud to vehicles) (7). As discussed in a subsequent chapter, the Federal Communications Commission (FCC) adopted new rules in November 2020 opening up the communications spectrum once reserved for DSRC to include 5G communications, which will have the long-term effect of sunsetting DSRC in favor of C-V2X.

A third connectivity path is also emerging; in-vehicle Wi-Fi is becoming standard in many newer vehicles.

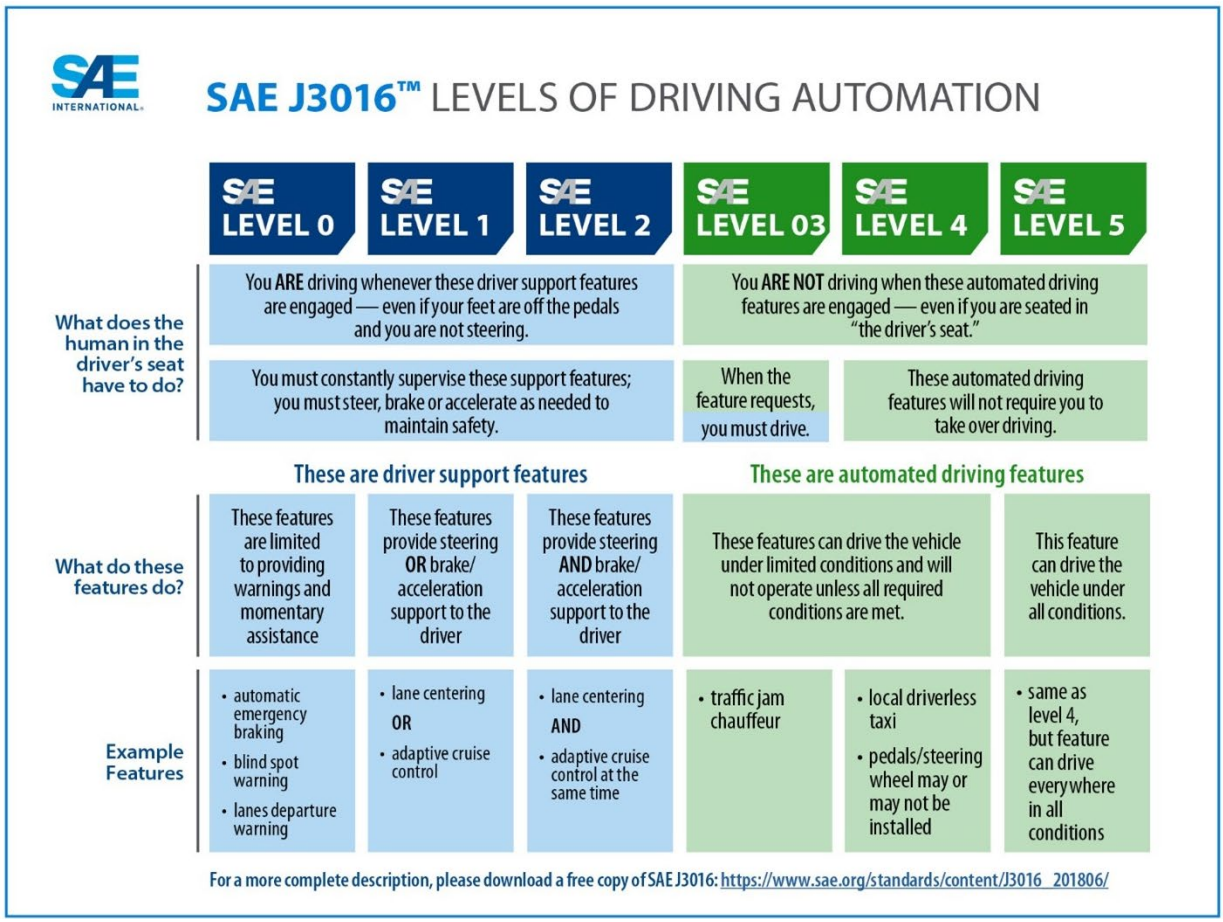
Automated Vehicles

While CVs offer potential safety and other benefits by communicating with other vehicles, road infrastructure, cellular networks, and the cloud, AVs offer potential safety and other benefits by gradually removing the primary source of driving accidents and crashes: a human driver. AVs represent a switching of the responsibility for the driving task from human to machine.

AVs represent a switch in driving responsibility from human to machine to improve driving safety and efficiency. While CVs may enhance the benefits of AVs, they are not a precondition for AV deployment.

Levels of Automation

As Figure 2 illustrates, SAE International has developed six levels of automation, which are differentiated based on whether the human in the driver's seat needs to drive or not (8). AVs comprise Levels 1–5. Autonomous vehicles (i.e., capable of operating without human involvement) comprise Levels 4 and 5. Level 0 does not qualify as an AV since the technology does not drive the vehicle. The current fleet operating on U.S. public roads consists primarily of vehicles ranging from Levels 1 to 3.



Source: SAE International (8)

Figure 2. SAE Levels of Driving Automation.

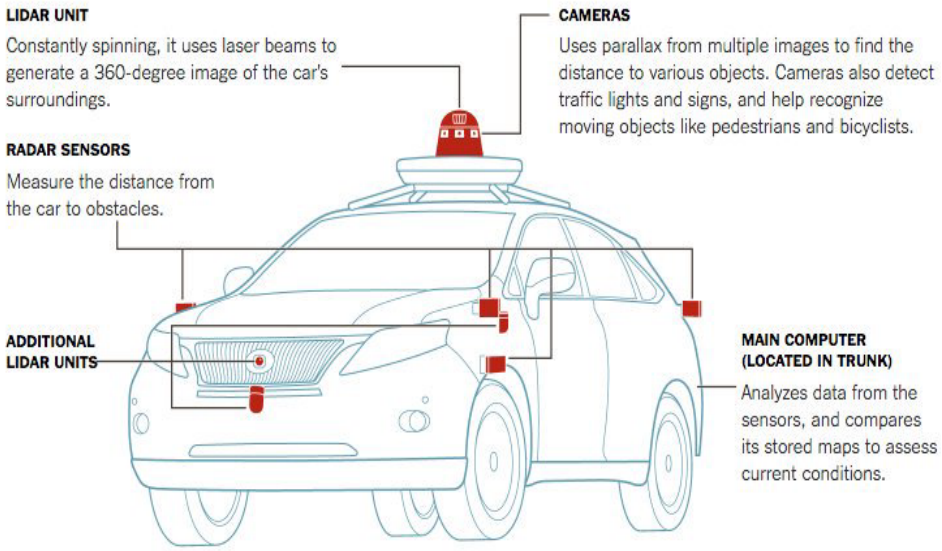
Highly automated vehicles (HAVs) rely heavily on machine learning (ML) systems. AVs are first programmed with basic knowledge, and then through ML they draw from both accumulated experiences and continual feedback to detect patterns, adapt to circumstances, make decisions, and improve driving performance to achieve the performance level of an HAV.

Although in 2016 many auto industry leaders expected Level 4 AVs to be commonplace on highways in the early 2020s, this does not seem as likely today. Acknowledging that building ML systems for AVs that can replicate the nuanced cognitive decisions made by human drivers is more difficult than originally claimed, OEMs are pushing out their timelines for higher-level AVs (9). However, there are many current demonstrations of Level 4 fleet services. For example, robotaxis in the form of minivans are serving paying customers without a trained vehicle operator through a smartphone app in Chandler, AZ (10). In Texas, autonomous shuttles are currently serving passengers at the Dallas-Fort Worth, TX, airport (11) and delivering groceries for Kroger in Houston, TX (12). The next section discusses the regulatory environment that is enabling testing and demonstrations of higher levels AVs in Texas.

Technologies Enabling AV Driving

AV driving functionality is handled through a variety of technologies (see Figure 3), including the following (13):

- **Radar** (radio waves) measure distances between the car and obstacles around it.
- **Lidar** (laser sensors) build a 360-degree image of the car's surroundings.
- **Cameras** detect people, lights, signs, and other objects.
- **Satellites** enable GPS to pinpoint a vehicle's position.
- **High-definition (HD) maps** determine and modify routes the car takes.



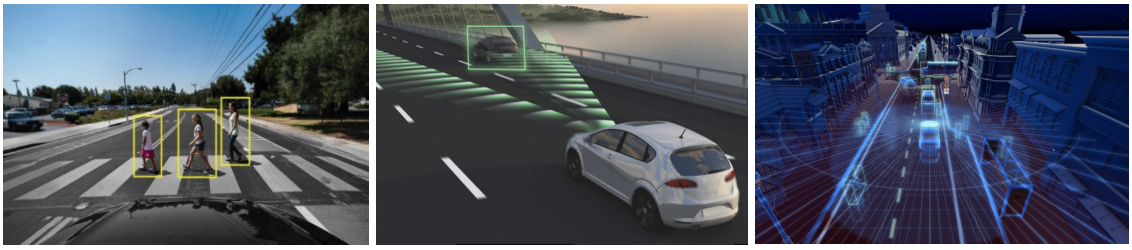
Source: Gates (12)

Figure 3. AV Technologies.

To attain human-like perception, AVs need to capture extensive surrounding information from the myriad of its AV technologies. Each of the radars, cameras, and other sensors used by the vehicle for autonomous driving purposes has limitations, so the sensor data need to be combined in order to achieve safe-driving functionality. For example, while camera systems can recognize other vehicles, lidar applications are better for accurately calculating the position of the vehicles, and radars are better at estimating speed (14). Each of these sensors compiles a lot of data because AVs rely heavily on ML algorithms, and ML in turn relies heavily on observed data. Vehicles at lower levels of automation may rely on one or more data inputs to enhance driving safety. However, at the higher levels of automation, vehicles must be able to make sense of a constant flow of information.

The function, hardware, and software of AV systems vary widely across the industry, but the way in which they operate is largely consistent (15):

1. The environment is monitored using a combination of sensors (e.g., cameras, radar, and lidar) (see Figure 4).
2. An onboard computer processes the information relayed from the sensors and combines it with GPS data, the known vehicle state (e.g., speed, orientation, steering, and brake application), and three-dimensional mapping data to estimate the vehicle's absolute position.
3. These steps create a virtual representation of the world, which includes the subject vehicle and all other road users, objects, and their intended path.
4. The vehicle determines an appropriate course of action (e.g., avoiding a collision) while obeying traffic laws.



Source: Burke (16)

Figure 4. AV Images from Camera, Radar, and Lidar, Respectively.

The onboard computer processes the different data inputs in step 2 using sensor fusion (14). The sensor inputs and other information, such as digital maps, feed into a high-performance, centralized computer that combines the relevant portions of data for the vehicle to make driving decisions. Given the number of sensors built into autonomous vehicles and the amount of data they generate, affirming data ownership (e.g., the owner of the vehicle or the company operating the AV fleet) of the synthesized or fused data and determining relevant privacy protections are important but as of yet unresolved considerations, as discussed in a subsequent chapter.

In addition to the aforementioned policy issues, there are unresolved technical issues associated with onboard sensor fusion. For example, the data streams processed using data fusion are different from each other in many ways, such as in the format of the data or in their temporal/spatial

resolution. The data streams need to be aligned with each other to make autonomous driving reliable, accurate, and safe.

There are several initiatives to develop open data standards to make fusion efforts easier while offering data privacy protections. For instance, a consortium comprised of German companies and research institutions has developed a fusion platform with open interfaces (i.e., Open Fusion Platform) that enables automobile manufacturers and suppliers to cost-effectively integrate data from highly and fully automated self-driving technologies (17). In addition, AV companies, such as Waymo, Audi, Ford, Toyota, Lyft, Argo AI, and NuTonomy, are opening up their AV data sets to tackle ML challenges (18, 19). The most prevalent model for this is a data exchange, a form of data sharing, in which free, curated data sets reveal a segment of a company's data while proprietary information is protected.

Government Regulation of CVs and AVs

The United States has a complex regulatory environment, with local, state, and federal government agencies, as well as Congress, having authority to create rules that may govern CV and AV operations.

In general, development and deployment of CVs and AVs can be shaped to benefit society through positive collaboration among stakeholders, appropriate policies over time, and regulation when needed. The United States has a multilayered environment for regulation of vehicles and infrastructure, with federal, state, and local government creating rules for various aspects of vehicle travel and its supporting technology. In addition, Congress has the authority to establish federal regulatory frameworks or standards for vehicles, such as safety or emissions standards.

USDOT, through the National Highway Traffic Safety Administration (NHTSA), has responsibility for the safety of motor vehicles (20). FCC is responsible for management of the electromagnetic spectrum, upon which many of the technologies central to enabling CV and AV functionality depend (21). States are responsible for such items as licensing of vehicles and operators, minimum vehicle standards, insurance, roadway usage, and traffic laws, as well as other issues including privacy, security, criminal law, and environmental regulation (20). Unless states adopt laws that override local regulation, local ordinances govern many aspects of everyday vehicle use, such as speed limits, parking, ride services, and the like. In addition, states and local governments are responsible for planning, building, managing, and operating transit and the roadway infrastructure.

Federal Activities

Connected Vehicles

In December 2019, FCC adopted a notice of proposed rulemaking that would split the 5.9-GHz band between ITS uses like safety-related vehicle communications and unlicensed operations like Wi-Fi (22, 23). The proposal reduces the amount of spectrum available for ITS uses from 75 MHz to 30 MHz and would allow both C-V2X devices and DSRC devices to use it. The residual 45 MHz would be opened up to non-transportation uses. Two decades ago, the 5.9-GHz band was reserved solely for DSRC to enable safety-related vehicle communications, but FCC reasoned that it has remained largely untapped for that purpose and wanted to spur innovation in cellular and Wi-Fi technologies.

FCC adopted the new rules in November 2020 in order to, as it stated in its order, "begin the transition away from DSRC to C-V2X technology" (24). Under the new rules, ITS services must vacate the lower 45 MHz of the band within one year.

In 2016, NHTSA and USDOT released a notice of proposed rulemaking that would require all new light vehicles, after the year 2023, to be equipped with V2V communication technology for safety purposes. However, this mandate was not enacted. While the clear intent of USDOT is to facilitate CV development and testing, it is being done without rulemaking in the following ways:

- **USDOT's Connected Vehicle Pilot Deployment Program** has been sponsoring CV projects in New York, NY, Tampa, FL, and Wyoming. The pilots focus on testing V2I, V2V, and V2X applications that could facilitate safety, mobility, and environmental benefits. Findings from the pilots should be available in 2022. (More information is available at https://www.its.dot.gov/pilots/.)
- **USDOT's Advanced Transportation and Congestion Management Technologies Deployment** (ATCMTD) grants have been funding projects for the past five years that deploy cutting-edge technologies, including CV technologies. Eligible grantees include state departments of transportation (DOTs), local governments, transit agencies, and metropolitan planning organizations. (More information is available at https://cms8.fhwa.dot.gov/newsroom/us-department-transportation-awards-433-million-advanced-transportation-and-congestion.)
- **A Signal Phase and Timing (SPaT) challenge** was issued by the V2I Deployment Coalition to state and local DOTs to achieve deployment of DSRC-enabled infrastructure with SPaT broadcast capability. The goal was approximately 20 signalized intersections in each of the 50 states by 2020. (More information is available at https://transportationops.org/spatchallenge.) Austin was the first city in Texas to enter the challenge; it was succeeded by Houston and San Antonio (25).
- **A CV Pooled Fund Study** has been created by a group of state, local, and international transportation agencies and the Federal Highway Administration (FHWA) in order for infrastructure providers to play a leading role in prototyping and testing practical, infrastructure-oriented CV applications that lead to deployment. Twenty-five state DOTs (including the Texas Department of Transportation [TxDOT]), one county DOT in Arizona, and Transport Canada are involved. (More information is available at https://highways.dot.gov/research/projects/connected-vehicles-pooled-fund-study.)
- **FHWA's National Highway Performance Program** allows funding for infrastructure-based ITS capital improvements, including the installation of V2I communication equipment, as does **FHWA's Surface Transportation Block Grant Program.** (More information is available at https://www.fhwa.dot.gov/fastact/factsheets/nhppfs.cfm and https://www.fhwa.dot.gov/fastact/factsheets/stbgfs.cfm.)

As of August 2020, USDOT estimated that there were 67 operational and 76 planned CV deployments in the United States (26). Many of these are associated with testbed, SPaT, and ATCMTD deployments. Texas has three ATCMTD grants:

- 2016—ConnectSmart: Connecting Transportation System Management Operations and Active Demand Management.

- 2017—Texas Connected Freight Corridors: A Sustainable Connected Vehicle Deployment.
- 2018—I-10 Corridor Coalition Truck Parking Availability System.

Despite two decades of federal efforts and funding, V2I technology has been slow to become extensively deployed. There is a financial aspect to this. Financing V2I technology requires large upfront investments of capital and resources, along with ongoing maintenance and operations. But there are also institutional issues that some suggest stem from a lack of clearly defined government and private roles (27).

Automated Vehicles

So far, NHTSA has not issued safety regulations or standards that specifically regulate driverless vehicles (19). In 2017 and 2018, NHTSA offered voluntary guidelines for industry in designing best practices for testing and deploying AVs on the surface transportation system (28, 29). In 2019, NHTSA detailed principles to protect users and communities (e.g., safety, cybersecurity, and data privacy), promote efficient markets (e.g., remain technology neutral), and facilitate coordinated efforts among federal agencies to support AV technology growth and leadership (22).

However, in early 2020, NHTSA issued a notice of proposed rulemaking that would modernize numerous Federal Motor Vehicle Safety Standards for vehicles equipped with automated driving systems (30). For example, NHTSA proposed to apply front passenger protection requirements to the traditional driver seating position when a steering wheel is not present in the vehicle. Also, in November 2020, NHTSA requested comment on the development of a framework for automated driving system safety, which would define, assess, and manage the safety of automated driving system performance while ensuring the needed flexibility to enable further innovation. (More information is available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/ads_safety_principles_anprm_website_version.pdf.)

Around the same time as USDOT's early guidance documents were being released, Congress was attempting to address the need for a federal framework for autonomous vehicle regulation. The House of Representatives passed the SELF DRIVE Act, and a separate bill, the AV START Act, was reported from a Senate committee. Neither bill was enacted. However, in September 2020, the SELF DRIVE Act was reintroduced with the rationale that the coronavirus crisis has made the need for self-driving cars more apparent as people seek contactless ways to get around and have goods delivered (31).

State and Local Activities

Connected Vehicles

The National Conference of State Legislatures (NCSL) provides current information on state legislative efforts related to CVs and AVs. (More information is available at https://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx.) According to this database, eight states have pending legislation relating to infrastructure and CVs. These tend to address cybersecurity and privacy, as well as enable vehicle platooning and sensor connectivity. Four states (including Texas, as discussed in the next section) have enacted legislation.

Automated Vehicles

To date, 29 states and Washington, DC, have passed legislation relating to AVs. Most of these legislative and regulatory actions solely address testing and liability issues within the state. So far, legislation has been state specific, with no attempt at coordination across states. To expand AV ubiquity in the future, states will need to come to agreement on how vehicles should behave when operating autonomously to facilitate AV travel across state lines.

Texas Context

Connected Vehicles

Texas is one of 32 states with an active 5.9-GHz ITS license and has numerous active CV deployments. In addition to the three ATCMTD projects listed previously, Signal Phase and Timing (SPaT) and connected corridor projects are operating in Arlington, Austin, College Station/Bryan, Houston, and San Antonio. (More information is available at https://www.txdot.gov/inside-txdot/division/planning/innovative-projects.html.)

In Texas, the push toward AVs and CVs is strong with a market-based regulatory approach that is enabling many pilot deployments for AV and CV technology advancements.

According to the NCSL database, in 2017, Texas enacted legislation that defined a "connected braking system" as a system by which the braking of one vehicle is electronically coordinated with the braking system of a following vehicle, and allowed the use of a connected braking system on states roads. In 2019, a bill failed that would have regulated the operation of public transit vehicles equipped with connected braking systems.

Automated Vehicles

Until 2017, Texas law did not authorize AVs for testing or operation on Texas roads (32). However, during the 2017 legislative session, lawmakers passed a bill that allowed AVs to test and drive on Texas roads. The law required AVs to follow the authorized rules of the road in the state, to be insured, and to be equipped with an electronic recording device. This law defined an "automated motor vehicle" as having an automated driving system, which was itself defined as hardware and software that are collectively capable of performing all aspects of an entire driving task without the intervention or supervision by a human operator. The law also specified that the automated driving system is considered to be licensed to operate the vehicle as long as it is engaged (32).

In the last legislative session, two bills were filed but failed to be enacted. The bills were meant to tweak Texas's self-driving car laws. One would have increased liability of manufacturers in the event of a crash involving an AV, and another would have required providers to equip vehicles with a failure alert system and the latest software.

Since 2017 when AV testing was authorized under state law, Texas has had more than 20 AV pilots and demonstrations. (More information is available at https://cavtaskforce.texas.gov.) They have primarily been pilots in simplified or geofenced operational design domains (ODDs) like university campuses or business/entertainment centers. The ODD specifies the conditions under which the vehicle is able to operate with respect to roadway types, speed range, weather conditions, and other

constraints. The majority of these AV pilots have been either to test and enhance the safety functionality of the vehicle or for data collection to train the vehicle's ML algorithms to accurately detect and decode objects such as pedestrians, street signs, and lane markers.

Data Privacy, Data Security, and Cybersecurity

Data Privacy Risks

Data privacy is defined as the capability of individuals to "determine for themselves when, how, and to what extent information about them is communicated to others" (33). It is important to consumers because a breach of personally identifiable information (PII) can cause harm, such as the risk of identity theft and other types of fraud. But it is also important to organizations and agencies because unauthorized collection or inadequate protection of PII introduces multiple risks like reputational damage, fines, lawsuits, and other possible penalties.

> ***Data privacy*** *relates to the collection, access, and use of sensitive personal information.* ***Data security*** *refers to the processes that limit access to sensitive personal information.* ***Cybersecurity*** *refers to measures used to protect a computer system (including a vehicle) against unauthorized access by a hacker.*

Data privacy is associated with data ownership. The question of data ownership directly affects who controls PII and, therefore, who can collect, access, use, and benefit from it. Individuals are assumed to own personal information about themselves, and thus are typically asked to opt in or give consent for activities (e.g., for telematics applications) that may capture it.

As vehicles become increasingly connected and automated, the volume of data they collect, combine, store, and communicate increases. Complex questions arise as to whether such data constitute PII and are subject to privacy protections (34). A single piece of data can be PII, such as a Social Security number. Likewise, multiple pieces of data when merged can be PII, even when the individual pieces would not be. As an example, a license plate number does not identify a specific person; rather, it identifies a vehicle. However, the license plate number may be linked or associated with an identifiable person through a linkage with other information, such as date of birth, gender, and zip code. Once information is associated with a specific individual, it becomes PII. With all the data collected by AVs and CVs, identifying the driver (and even the passengers) is possible although OEMs and companies operating fleets seek to mitigate this risk.

Often, we think that the privacy impact of collecting personal data can be reduced if data are anonymized (i.e., identifying information is removed) prior to subsequent processing and use of the data. But in recent years with increasing implementation of data science (which involves algorithm development, data inference, and predictive modeling), researchers have shown that anonymized data can be easily re-identified through linkages among multiple data. For example, European researchers have shown that a data set with 15 demographic attributes would identify 99.9 percent of Massachusetts residents and that fewer attributes would be needed for smaller geographies (35). As another example, Massachusetts Institute of Technology researchers used just four anonymized spatiotemporal data points (i.e., a person's location at a given time) to uniquely re-identify 90 percent of the 1.1 million individuals in a financial transaction database (36). Moreover, the

researchers found that knowing the price of a transaction dramatically increased the likelihood that someone could be re-identified. The implication for CV and AV data is that even if PII is stripped from an original data set, a risk of exposure of sensitive information still exists if those data are stored, analyzed, and reused without adequate protections.

Data Privacy Protection

In the United States, there is no comprehensive federal law governing the collection, use, and sale of personal information, such as the European Union's General Data Privacy Regulation (GDPR). (More information is available at https://gdpr-info.eu/.) The GDPR was designed to harmonize data privacy laws across all European Union member countries and to provide broad data protections and rights to individuals. There is the potential for large fines and reputational damage for those businesses found in breach of the GDPR.

The United States has a patchwork of federal and state laws to address data privacy protections.

In early 2020, the European Data Protection Board published draft guidelines on the processing of personal data in the context of CVs and mobility-related applications. Notably, the draft guidelines require granular consent to collect both personal and non-personal data from CVs. Companies appear to be complying with these requirements. (More information is available at https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.)

Federal Statutes

Unlike the comprehensive approach to data privacy regulation in Europe, federal statutes and regulations addressing privacy issues in the United States are generally tailored to specific sectors, purposes, and types of information. The Driver Privacy Act of 2015 is one example. It stipulates that a vehicle's event data recorder (EDR) data, which is produced immediately before and during an accident such as the date, time, vehicle, and engine speed, belong to the owner or the lessee of the vehicle in which the EDR is installed (37). There is no similar type of law that pertains to other types of data coming from vehicles. Another example is the Health Insurance Portability and Accountability Act, which governs the use and disclosure of an individual's health information (37).

Those entities not subject to industry-specific regulation typically use the Federal Trade Commission's (FTC's) *nonbinding* Fair Information Practice Principles to guide their data privacy practices (34):

- **Notice:** Provide clear and conspicuous notice of what information is collected, how it is collected, how it is used, and whether it is shared with other entities.
- **Choice:** Offer choices as to how PII is used beyond the use for which the information was provided (e.g., to consummate a transaction).
- **Access:** Provide reasonable access to the information that is collected, including an opportunity to review information and to correct inaccuracies or delete information.
- **Security:** Take steps to protect the security of the information collected from consumers.

Federal law does not require companies to have a privacy policy or to notify consumers of their privacy practices.

State Statutes

States laws have added to the patchwork approach to privacy protection in the United States. Many individual states have adopted their own privacy protection laws. The California Consumer Privacy Act (CCPA), which was inspired by the European Union's GDPR, is the most comprehensive of the state legislation. The CCPA began being enforced on July 1, 2020 (38). Although this law was not designed specifically for vehicles, it covers the collection of PII by vehicle systems and through phone or telematics connections (39). The law grants California residents several rights, including the right to request what PII a business has about them, to opt out of the sale of their PII, and to request their PII be deleted. Nevada and Maine have also recently passed stringent data privacy laws, but these laws apply only to online data collection. California's law pertains to online and offline businesses.

At least 11 states, including Michigan, Massachusetts, Hawaii, Minnesota, and Washington, have proposed data privacy laws during the 2019 or 2020 legislative sessions. None were signed into law. Of all the states, North Dakota has considered what happens to the data produced by self-driving cars (40). A bill, enacted in 2017, calls for the state DOT to study "the data or information stored or gathered by the use of those vehicles." A failed bill from the same year would have granted ownership of data to the vehicle's owner and allowed sharing of data with the consent of the customer.

Texas's data privacy legislation is confined to breach notification (which really pertains to data security) and requires businesses to disclose "as quickly as possible" any breach to individuals whose sensitive personal information was, or is believed to have been, acquired by an unauthorized person (41). An enacted 2019 bill introduced a timing requirement for notification of 60 days of a breach occurring. Separately, the bill created an advisory council to study data privacy laws and produce recommendations regarding protections.

Industry Efforts

Twenty OEMs developed privacy principles for vehicle technologies and services in 2014 and reviewed these again in 2018 (42). The auto industry privacy principles have been in effect for all model year 2017 vehicles and beyond. Overall, the privacy principles require clear and prominent notices about the collection of information, the purposes for which it is collected, and the types of entities with which the information is shared. The OEM's privacy principles require consent from the vehicle owner for sharing information with third parties. These privacy principles are enforceable against the signatory OEMs by FTC. The auto industry was considered to have addressed protecting consumer privacy in a proactive manner by developing and committing to the privacy principles, which were still considered best in class at the 2018 review compared to other industries.

Data Security

Data security is directly associated with data access. *Data access* refers to a user's ability to retrieve data stored within a database or other repository. Entities that have data access can move, use, or manipulate the stored data. There are varying levels of data access that range from totally open to restricted access (34). EDR data are an example of data with restricted accessed; that is, the data are only accessed via specialized software with the expressed consent of the vehicle owner or lessee.

At the other end of the spectrum is open data, which implies that data are available to be freely used, reused, and redistributed by anyone. (More information is available at http://opendatahandbook.org/ guide /en/what-is-open-data/.) OpenStreetMap, a collaborative project to use crowdsourced geodata to create a free editable map of the world, is an example of totally open data. (More information is available at https://www.openstreetmap.org/about) Standards for open data are critical to ensuring privacy protection.

Levels of data access between open and controlled require some sort of membership or user authentication. An example is Uber Movement data where Uber makes its trip data available via a public website to users who request and receive approval to access it. (More information is available at https://movement.uber.com/?lang=en-US) Another example is the General On-Demand Feed Specification, which is a membership-based organization that is developing an application programming interface to enable discoverability of on-demand vehicles. (More information is available at https://mobilitydata.org/.) The Open Fusion Platform is a type of access-controlled secure data platform.

Cybersecurity Risks and Protections

Cybersecurity, in the context of vehicle systems, refers to security protections for systems in the vehicle that actively communicate with other systems or other vehicles (43). In 2019, there were 176 digital and electronic cyberattacks aimed at vehicles, more than double the 78 attacks from the previous year (44). The incidents ranged from stealing cars by hacking keyless entry fobs to tracking trucks by compromising online fleet services. More attacks were conducted by malicious actors than by researchers and white-hat hackers.

Three main risks are associated with hacking CVs or AVs:

- The hacker might gain access to the vehicle through keyless entry bypass.
- The hacker might attempt to take control of the vehicle remotely.
- The hacker might attempt to access the user's personal (or sensitive) information, which could then be used for phishing attempts or other kinds of fraud.

While cybersecurity issues are a challenge for CVs, security becomes a bigger concern with Level 4 and Level 5 AVs, in which software and connectivity play a much bigger and more critical role for the safe driving of vehicles. Unlike traditional vehicles, CVs and AVs may also be vulnerable to cyberattacks that can spread from vehicle to vehicle.

Underscoring the increasing severity of vehicle cybersecurity risks, in 2020 the United Nations issued—and 53 countries adopted—a new regulation that requires vehicle makers in jurisdictions in Japan, South Korea, and the European Union to secure CVs from cybersecurity threats (45). While the United States participated in discussions, it did not vote. Therefore, U.S. vehicle manufacturers are not held to the United Nations regulation. However, those that sell vehicles in jurisdictions under the cybersecurity regulation must comply.

In the United States at the national level, NHTSA has issued nonbinding guidance to the automotive industry for improving motor vehicle cybersecurity (46). NHTSA's guidance focuses on a layered

solution to harden the vehicle's electronic architecture against potential attacks and to ensure vehicle systems take appropriate actions in the event that an attack is successful. The guidance suggests that the automotive industry follow the National Institute of Standards and Technology's documented Cybersecurity Framework, which is structured around the five principal functions—identify, protect, detect, respond, and recover—to build a systematic approach to developing layered cybersecurity protections for vehicles. In addition, both FTC and USDOT have endorsed voluntary information sharing of cybersecurity threats through industry groups. The SELF DRIVE Act, reintroduced in 2020, will require manufacturers to create cybersecurity policies on how they will respond to cyberattacks for vehicles that are highly automated.

Cybersecurity protections have also been introduced at the state level. In 2020, California became the first state to regulate the cybersecurity standards of connected devices (47). It requires reasonable security on any Internet of Things device to prevent unauthorized access, modification, or information disclosure. Oregon passed a similar law soon after.

Some of the biggest challenges relating to data privacy or cybersecurity protection are related to data security. Risks are associated with who has access to or can access sensitive data, such as geolocation, driver behavior, or biometrics. Risks exist if such data are accessed by third parties that are not committed to privacy principles or who cannot protect the data from a hack. As an example, in November 2020, Massachusetts passed a ballot measure to require auto manufacturers that sell vehicles with telematics systems in the state to equip them with a new standardized open-access data platform (48). Beginning with model year 2022, vehicle owners and independent repair facilities will be able to retrieve a vehicle's mechanical data and run diagnostics through a mobile-based application. A concern is that auto repair facilities without robust security processes could leave consumer data—and the vehicles themselves—vulnerable to cybersecurity threats. NHTSA has raised concerns this ballot initiative would prohibit manufacturers from complying with both existing federal guidance and cybersecurity best practices.

CV and AV Data Use and Data Generation

Data Used by CVs and AVs

CVs and AVs, in similar and different ways, combine a variety of technologies and sensors to transmit information about their position and to perceive their surroundings, including DSRC and cellular communications, radar, lidar, computer vision, sonar, and GPS, among others. Shimada et al. (49) identified four types of data that CVs and AVs use to operate safely. Table 2 presents these data types and offers descriptive information about them. Not all entities conducting testing may be using all of the types of data listed.

The data are both static and dynamic (50):

- Static data are collected from various sources over time, stored, and subsequently analyzed and/or aggregated.
- Dynamic data, sometimes referred to as *data in transit*, are often used in real time without necessarily being stored. This results in hyper-local and hyper-current data.

Table 2. Types of Data that CVs and AVs May Use to Operate Safely.

Data Type	Description	Example	Source	Use
Permanent static	Digital map data	HD geospatial detail for streets	• Private third party • Generated by vehicle sensors	Enable lane-accurate positioning/localization
Transient static	Roadside infrastructure	Road signs, landmarks, and permitted routes	• Road operators	Parking/no-parking zones and notice of speed changes
Transient dynamic	Traffic conditions, road conditions, and environmental conditions; traffic signals	Existence of a slippery road	• Road operators • Private third party • Generated by vehicle sensors	Existence of work zones/lane changes; enable V2I signal phase
Highly dynamic	Movements of vehicles, pedestrians, etc.	Wrong-way driver	• Generated by vehicle sensors	V2V and V2P warnings

Source: Shimada et al. (49)

As Table 2 shows, CVs and AVs use data from different sources to operate safely. Generally, the sources are either on board (i.e., generated by) the vehicle or externally sourced from other vehicles, private third-party providers, or road operators. When operating, the vehicle prioritizes or first acts on the onboard data, that is, the data coming from vehicle sensors, cameras, etc. (51). When externally sourced data are available, such as HD maps, the vehicle uses them to support or complement the sensor data. Such redundancy is important. The trick is diversity (i.e., different types of sensors and data) and redundancy (i.e., overlapping sensors and data) that can verify that what a car is detecting is accurate (13).

Data Generated by CVs and AVs

As vehicles continue to become more automated and more connected to each other, surrounding infrastructure, mobile devices, the cloud, they will use significantly more data to operate safely. They will also generate and record many types of data as they operate on roads. Some of these data are user generated such as driver/passenger identity, use patterns of in-vehicle apps, service information (e.g., payment of tolls and parking reservations), or direct communications from the vehicle (e.g., calls, texts, and emails). These data can be provided by pairing the vehicle with a mobile phone device or through user interaction with the vehicle. Other data are vehicle generated. These data include vehicle measures, vehicle safety data, environmental probe data, vehicle diagnostics data, vehicle emissions data, and biometrics data (e.g., fingerprints or facial patterns). The vehicle-generated data are produced from advanced sensors, processors, enhanced driver interfaces, and other OBUs that are able to record and deliver data internal and external to the vehicles, such as ITS equipment distributed along the roadside such as traffic detectors and traffic signals.

Data ownership is an important aspect of data generated by CVs and AVs. Data ownership is complicated and nuanced, and often data ownership is in the eye of the beholder. Research among OEMs, data aggregators, and owner/operators found that (34):

- OEMs acknowledge that the owner or lessee of the car is the owner of the connected car data; however, OEMs are able to access and control the data through user agreements. Privacy principles are used to provide transparency to their data collection, use, and sharing practices so as not to discourage customers from opting into the agreements. Customer trust in terms of opting in is essential for the OEMs' ongoing use of the data to improve their automotive products and develop new customized offerings.
- Data aggregators consider themselves to be the owners of the information that they sell that is derived from the CV or AV data. These data have been gathered from many sources, processed, and formatted into new information products. While they may not be the owners of the source data, they believe they are the owners of the new information products that they create.
- Owner-operators consider themselves to be the owners of the data collected by their sensors. Since the data are recorded by sensors outside the vehicle, they view the data as fair game. Broadcast data are viewed as public information.

Given these different views on data ownership, does it matter? It matters because ownership of data is tantamount to control, determining who can process, use, and share the data. Ownership also implies who can profit from it. However, just as important, ownership implies a broader responsibility—data stewardship—where the owner must consider the consequences of how the data are used, particularly how a particular use might impact data privacy or data security.

Table 3 identifies and describes the main types of CV- and AV-generated data. The information is presented to reflect the type of data that *might be possible* to collect and share; not all AV and CV companies conducting testing will be collecting all of the data identified. In addition, while immediate owners/stewards are identified in the table, there may be additional owners and nuances to ownership that are not referenced and that will need to be addressed in the long term.

A comparison of Table 2 and Table 3 shows much overlap in the data a vehicle uses to operate safely and the data generated while it is operating.

Table 3. Main Types of Data Generated by CVs or AVs.

Data	Description	Owner/Steward	Potential Users
Safety	Static data. Environment and vehicle data associated with safety situations.	• Vehicle owner/ OEM of vehicles • Application developer	• State and local policy makers • Federal policy makers • State and local transportation infrastructure owners and operators • Law enforcement • Insurance companies
Diagnostic	Static data. Technical vehicle status (e.g., engine performance and tire pressure level).	• Vehicle owner/OEM	• OEM • Current vehicle owner • Auto repair facilities • Vehicle inspection agencies
Road infrastructure	Static data. Road infrastructure conditions (e.g., road geometry and markings).	• Vehicle owner/OEM • Manager of back-office data management system or data warehouse	• Traffic data aggregators • State and local infrastructure owners and operators • Mapping aggregators
Biometrics data	Static data. Face, iris, voice, and fingerprints.	• Vehicle owner/OEM	• Law enforcement • Insurance companies • Health or medical companies
Location	Static and dynamic data. GPS coordinates, mileage, routes taken, and time spent at locations.	• Vehicle owner/OEM	• Traffic data aggregators • Mapping aggregators • State and local transportation infrastructure owners and operators • Insurance companies
Driving behavior	Static and dynamic data. Speed, acceleration, travel times, volumes, occupancy, and use of autonomous functions.	• Vehicle owner/OEM • Manager of back-office data management system or data warehouse	• Traffic data aggregators • State and local transportation infrastructure owners and operators • Insurance companies
Service information	Static and dynamic data. Payment of tolls, calculation of insurance premiums, and parking reservations and fees.	• Vehicle owner/OEM • Application developer	• Toll road or road pricing operations • Parking lot owners • Insurance companies • Location-based services
Traffic and road conditions	Dynamic data. Vehicle, people movements, wait time in highway entrance/exit, traffic density per highway lane, average time for red traffic lights, and road surface weather conditions (e.g., icing).	• Vehicle owner/OEM • Manager of back-office data management system or data warehouse	• Traffic data aggregators • State and local transportation infrastructure owners and operators

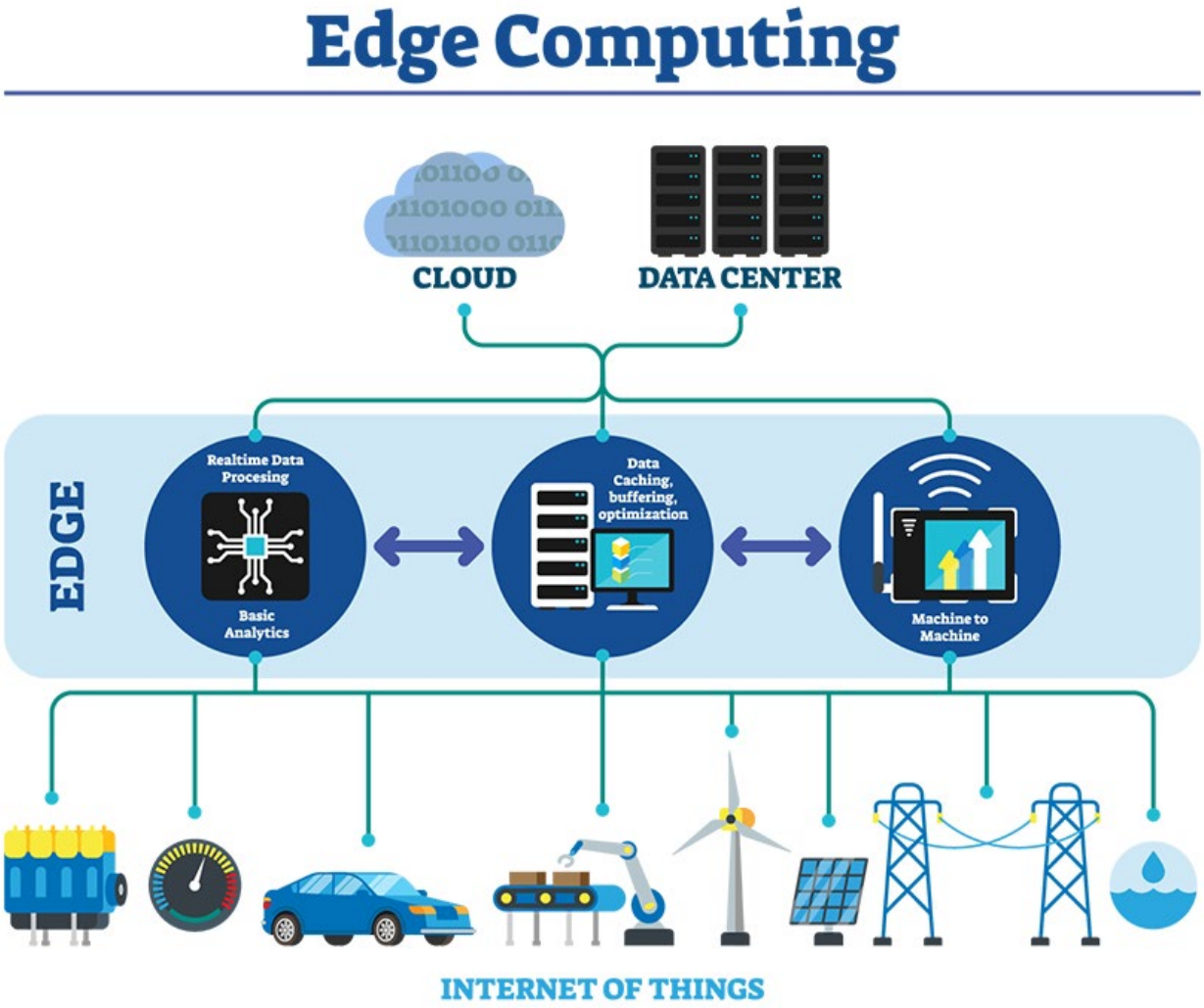
Sources: Synthesized from Hong et al. (50), Somers (51), and Zhang (37)

Data Management Challenges

As noted in Table 3, CV and AV technologies generate large volumes of data from a vehicle's sensors, which can be outward looking (e.g., cameras, radar, and lidar instruments) and also inward looking (e.g., logged engine output and exhaust emissions). CV and AV technologies also rely on large volumes of data for safe operation, like HD map information. This volume of data creates increasing data storage and data management challenges. While innovations in data optimization, connectivity choices, and data storage locations are expected to mitigate these challenges, some uncertainties are still to be worked out. As of yet, there is no consensus on just how much data CVs and AVs will generate and therefore what the data storage needs will be (52). Expert estimates range from less than 1 terabyte per day to as much as 32 terabytes per day. As a comparison, in 2018 Twitter's 336 million active users were estimated to generate 12 terabytes of data (53).

The amount of data generated is expected to vary from vehicle to vehicle based on the number and types of sensors and other technologies on the vehicle. Current prototype versions of fully autonomous vehicles can have anywhere from 20 to 40 different kinds of sensors (54). Also, the data generation between consumer-owned AVs (and CVs) and robotaxi vehicles will differ. The latter are expected to be operational for more hours each day than the average consumer and so will generate more data (54). In addition, experts have noted that testing phases of AV and CV development will generate more data than the operational phases. For example, during the testing phase, an AV is collecting as much data as possible about its surrounding environment to train its ML systems (52). Once the systems have been adequately trained, the vehicle just scans the environment to monitor the accuracy of system performance and to identify unknown objectives or situations, thus generating and using less data.

Also, experts disagree about how much data will be stored in the vehicle versus in the cloud or in another distributed network infrastructure (52). How the data are stored will depend on the vehicle system or functionality being supported. Most experts agree that automated driving systems will need to process large volumes of data on board the vehicle in real time to provide driving functions such as collision avoidance, automatic braking, and adaptive cruise control (55). The need for in-vehicle storage grows as the car achieves greater levels of autonomous driving capabilities. Other functions, such as V2X, communicate in a peer-to-peer network that requires storage with low latency, such as edge computing (56). As illustrated in Figure 5, edge computing brings data storage and computation closer to the devices that are generating the data, rather than relying on a central location, such as in the cloud, which can be farther away (57). Edge computing helps decentralize data processing and lower dependence on the cloud (58). This is done so that data, especially real-time data, do not suffer latency issues that can affect an application's or system's performance. Also, according to IEEE, traditional cloud computing is plagued by growing operational costs and greater data security threats.



Source: IEEE (58)

Figure 5. Edge Computing versus Cloud Computing.

The need and desire for data must be coupled with a stakeholder's ability to manage them. For example, one OEM, as it ramped up to launch its autonomous prototype vehicles, spent nearly $300 million on two new data warehouses in the cloud (54). This explains the growing interest among OEMs and other CV or AV developers to explore avenues for monetizing data that have commercial value, such as driving behavior data (34). Such data have a bigger impact on OEMs' internal systems and have a higher value for monetization. As another example, U.S. federal law does not assign ownership, access, and use limitation to broadcast data, that is, a defined data packet that is broadcast to many recipients, such as a basic safety message (BSM). For V2V messages, BSMs are non-identifiable data communicated by a vehicle providing location and speed but not the vehicle identification number or license plate number. An example is a vehicle broadcasting a message that "I am here," "I am moving in this direction at this speed," or "I just slammed on my brakes." As a result, USDOT and FHWA do not currently have a specific policy assigning data ownership or limiting access to BSM data (59).

The relevant stakeholders in a CV deployment must be able to provide strong data security and well-structured policies for each step in a data management life cycle. This was the experience during the New York City CV Pilot Deployment (60). The volume of new V2X data introduced privacy challenges for the deployment team (e.g., ensuring anonymity and the inability to track), as well as data management challenges, in order to obfuscate the correlation of individual drivers with any raw or processed data. These challenges, which required the agreement on data security methods from all V2X stakeholders (e.g., the traffic system operators, cities, counties, fleet operators, researchers, and third-party data providers/consumers), significantly delayed the CV pilot deployment.

Many state and other public agencies have existing programs to manage ITS and traffic planning data. While most have *considered* the benefits and challenges of integrating AV or CV data into existing data programs, few have specific plans to add such data to their data management platforms and processes (61). Rather, according to MetroPlan Orlando's best practices review, most agencies are just beginning to explore how CV and AV data might be used to improve real-time operations and enhance near- or long-term transportation planning. For example, traffic engineers have suggested that vehicles equipped with traffic light information applications could facilitate the management of traffic flow and reduce congestion.

Opportunities and Challenges for Data Sharing and Data Exchange

Opportunities for Data Sharing and Data Exchange

The vast amount of data used by CVs and AVs, as well as the data that are generated by them, can be useful to a range of stakeholders representing both public and private interests, as Table 2 and Table 3 show. Some data elements are critical for public-sector organizations to better serve the traveling public, while others are critical for private-sector developers and operators to further develop their CV and AV technologies. With this in mind, it is important for stakeholders to identify exactly what data they need and for what purposes, rather than trying to get access to all data. As mentioned previously in this paper, tough challenges are associated with the sheer volume of vehicle data and the lack of standardization. In addition, the CV and AV ecosystems are rapidly evolving, making it extremely difficult for states to enact policies that balance the needs of all stakeholders. USDOT, in its guidance documents of 2016 (62), 2017 (27), 2018 (28), and 2019 (20), has tried to balance the government's interest in safety and industry's desire for flexibility for profitable innovation. USDOT encourages the sharing of relevant data and believes it is important in the introduction of CVs and AVs to transportation systems.

Data sharing and data exchange are not the same thing (63). **Data sharing** happens when the same data resource is shared among multiple applications or users. Data sharing describes a system that accommodates participation by several organizations—all having joint control and continual access to the data, and all deriving mutual benefit from the use of the data. The following are some examples of mutually beneficial data-sharing activities:

Data sharing and data exchange represent two different approaches for access and use of the same data resource.

- **USDOT's Secure Data Commons** is a cloud-based analytics platform for sharing data and collaborating on improving research, tools, and algorithms relating to the shared data sets.

Currently, it features data sets from the Waze Connected Citizen Program, the Connected Vehicle Pilot Deployment Program, and the American Transportation Research Institute Freight Mobility Initiative. (More information is available at https://www.its.dot.gov/about/its_jpo.htm.)

- **On-Farm Data Sharing** is a shared database on crop yields among farmers' networks that facilitates analyses across space and time, and provides much more useful and robust answers to crop production questions than data from one farmer's field alone. (More information is available at https://www.rd-alliance.org/groups/farm-data-sharing-ofds-wg.)
- **The U.S. Electric System Operating Data Tool**, sponsored by the U.S. Energy Information Administration, makes consistently formatted and hourly electricity operating data from the contiguous 48 states, including actual and forecast demand, net generation, and the power flowing between electric systems, available to the electric system balancing authorities in those states. (More information is available at https://www.data.gov/energy/.)
- **DataSphere**, an initiative of the CEO Roundtable on Cancer, relies on chief executive officers to provide data on cancer drug trials and works with third-party data aggregators to pool the information on the hundreds of cancer drugs being developed at any given time in meaningful ways for shared use by all the chief executive officers. (More information is available at https://www.projectdatasphere.org/data-platform/access-data.)

Data exchange is a form of data sharing, but unlike with data sharing, the benefits derived from a data exchange are not necessarily reciprocal (63). Each organization may receive some type of benefit from the exchange, but these are not necessarily the same shared benefit. In a data exchange, one organization transfers data to another organization as a one-to-one, episodic exchange with no further interaction or updating of the data by the sourcing organization (63). In the exchange, the sourcing organization can be compensated for the data or not. Once in the hands of the consuming organization, the data are processed and manipulated by the consuming organization without the direct participation of the sourcing organization. The following are examples of data exchange:

- In **Uber Movement**, Uber makes its trip data available via a public website to users who request and receive approval to access it. (More information is available at https://movement.uber.com/?lang=en-US.)
- **Facebook's Data for Good** program provides access to publicly available aggregated mobility data that come from Facebook subscribers. Facebook also provides access to non-publicly available data to researchers. (More information is available at https://dataforgood.fb.com/docs/facebook-data-for-good-publicly-available-data/.)
- **Cuebiq** provides access to mobility flow and location-based data for analyses related to COVID-19 impacts. (More information is available at https://www.cuebiq.com/.)

USDOT's Data for Automated Vehicle Integration (DAVI) addresses AV data-sharing and -exchange needs across modes of transportation. (More information is available at https://www.transportation.gov/av/data,) The DAVI framework identifies four types of data-sharing/exchange opportunities.

- **Business to business:** Key stakeholders are OEMs, shared transportation service providers, and insurance companies for purposes of mitigating cyber threats, increasing safety through shared learning, and informing insurance and liability issues.
- **Business to government:** Key stakeholders are OEMs, shared transportation service providers, state and local governments, and federal government agencies for purposes of understanding performance during testing phases and informing policies and investments.
- **Infrastructure to business:** Key stakeholders are infrastructure owners and operators, infrastructure technology companies, in-vehicle and aftermarket services, OEMs, and shared transportation service providers for purposes of increasing safe navigation, mitigating congestion, and optimizing infrastructure investments.
- **Open training data:** Key stakeholders are government, industry, academia, and individuals for purposes of improving safety performance in common safety-critical scenarios and supporting basic research and education.

To advance data sharing or data exchange among the identified stakeholders *in each type*, it is necessary to determine:

- Which entities are collecting, storing, and analyzing what data?
- What data are the entities not collecting (whether due to regulation, industry-imposed standards, or not being of value to them)?
- What data gaps exist that hinder innovation and furthering the public interest?

Answering these questions would be especially important for data that might be of use to both the public and private sectors. These data could include accident or traffic flow data, which might be monetized and also used to promote public safety, and anonymized collision data, which could be useful to insurers to determine claims payments, OEMs to evolve their technology, and public-sector entities for incident mitigation.

Whether to seek data-sharing or -exchange opportunities depends on the needs of participating entities and their intended uses of the data. For example, stakeholders across sectors and industries who have different needs for the same data might want a data-exchange approach. On the other hand, when the data-based solution can be applied to problems that plague all stakeholders, more generalized data-sharing models may be appropriate.

> *Data exchange may be more appropriate when stakeholders across sectors and industries have different needs for the same data. Data sharing may be more appropriate when data can be applied to problems that plague all stakeholders.*

Toward that latter end, several initiatives in the United States and elsewhere have sought to identify high-priority data for data sharing (51, 64). Data are generally viewed as higher priority for private- or public-sector interests when associated with situations that present a significant safety issue. Table 4 presents these high-priority data categories, along with their potential owners. In June 2020, USDOT published a notice of funding opportunity for Work Zone Data Exchange demonstration grants. While the title says data exchange, it is really a data-sharing opportunity for public infrastructure owners and operators to make harmonized work zone data feeds ubiquitously available for use by third parties. The closing date for applications was in August 2020.

Table 4. High-Priority Data-Sharing Opportunities.

Data Type	High-Value Data	Owner/Steward
Work zones	Work zone locations, planned duration of project, planned lane changes/closures, and change in signage	• State and local transportation infrastructure owners and operators • Highway construction firms
Real-time traffic and road conditions	Traffic congestion variances, missing traffic signs or lane markings, potholes, and emergency road closures and detours	• Traffic data aggregators • Regional and local traffic management centers • State and local infrastructure owners and operators
Roadway inventories	Edge-to-edge data on roadways, such as curbs, bicycle lanes, pedestrian walkways, transportation network company/taxi pickup/drop-off zones, bridge heights and weights, overpass heights, road elevation, highway dividers, and parking/no-parking areas	• Mapping aggregators • State and local transportation infrastructure owners and operators
SPaT	State of the signalized intersection and how long the state will persist for each approach and lane that is active; usually used along with the geometry of the intersection	• State and local transportation infrastructure owners and operators
Cybersecurity	Incident types, source, target, duration, and implications	• OEMs • Shared transportation service providers • Commercial fleet operators • State and local transit agencies • State and local transportation infrastructure owners and operators
Safety performance	Environment and vehicle data associated with safety situations, AV disengagement/ re-engagement, and crash reports	• OEMs • Shared transportation service providers • Commercial fleet operators • State and local transit agencies

Sources: Somers (51) and USDOT (64)

Data-Sharing or Data-Exchange Models

Virtually all CV or AV data-sharing or data-exchange initiatives in the United States have been voluntary. The exception pertains to AV testing in California, where California regulations state that every manufacturer authorized to test autonomous vehicles on public roads must submit an annual report summarizing the disengagements of the technology during testing. (More information is available at https://www.dmv.ca.gov/portal/vehicle-industry-services/autonomous-vehicles/testing-autonomous-vehicles-without-a-driver/.) Reports are posted on the California Department of Motor Vehicles website. No other state mandates the sharing of AV testing data, and no federal rule requires AV companies to submit information about their testing activities to the government. USDOT, through its AV guidance documents, requests that companies that are testing self-driving cars submit voluntary safety reports. In 2020, NHTSA launched the Automated Vehicles Transparency and Engagement for Safe Testing Initiative, which established an online platform to facilitate sharing of high-level, on-road test data by participating AV companies. (More information is available at https://www.nhtsa.gov/automated-vehicles-safety/av-test-initiative-tracking-tool.)

Other voluntary national-level data-sharing activities in transportation include the following.

- In **NHTSA's Partnership for Analytics Research in Traffic Safety**, at least six OEMs and NHTSA share de-identified and anonymized data to examine the effectiveness of crash avoidance systems and to benchmark safety impacts. (More information is available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/parts_program011520.pdf.)
- **The Automotive Information Sharing and Analysis Center** is a central hub for sharing, tracking, and analyzing intelligence about potential cyber threats, vulnerabilities, and incidents related to connected vehicles. (More information is available at https://www.automotiveisac.com.)
- **The National Transit Map** collects and synthesizes public data using a common format to create and display a comprehensive map of fixed transit options in the United States. (More information is available at https://www.bts.gov/geography/geospatial-portal/national-transit-map)
- **The Federal Aviation Administration Aviation Safety Information Analysis and Sharing System** integrates and analyzes private- and public-sector data to plan for potential safety concerns in aviation. (More information is available at https://www.asias.faa.gov/apex/f?p=100:1.)
- Tri-Met, the transit agency in Portland, OR, worked with Google to develop the **General Transit Feed Specification,** which allows public transit agencies to publish their transit data in a format that can be consumed by a multitude of transit operators and a wide variety of software applications. (More information is available at https://gtfs.org/.)

Voluntary data-sharing initiatives have also occurred at the state level. MetroPlan Orlando's best practices review identified the following (61):

- **The Virginia Department of Transportation's SmarterRoads.org data portal**, which provides free, widespread access to roadway and transportation information.
- **The Florida Department of Transportation's Data Integration and Video Aggregation System**, a centralized data hub for the aggregation, fusion, and dissemination of near real-time transportation information and live-streaming video.

TxDOT has its own data-sharing initiatives**.** For example, TxDOT is sharing Inrix data with metropolitan planning organizations and other public agencies. The following are additional data-sharing activities:

- **The DriveTexas.org website** offers information about road closures, construction zones, flooding, damage, and accidents. Data are as close to real time as possible, and the website is a vital tool for the public during emergency situations. (More information is available at https://www.txdot.gov/inside-txdot/media-center/statewide-news/2017-archive/019-2017.html.)
- **The TxDOT Open Data Portal** is the agency's platform for sharing geographic information system data. (More information is available at https://gis-txdot.opendata.arcgis.com/.)
- **The Texas Connected Freight Corridors project** is Texas's largest deployment of CV technology. Through the deployment, TxDOT will acquire a rich set of traffic conditions data, including parking availability and border crossing times, and will share this information with other state agencies, metropolitan planning organizations, cities, and counties along the

I-35, I-10, and I-45 corridors; trucking/freight companies; trucking/freight manufacturers and equipment companies; and the traveling public. (More information is available at https://ftp.dot.state.tx.us/pub/txdot-info/trf/freight-corridors/faq.pdf.)

Challenges for Data Sharing and Exchange

Data sharing or exchange is both an opportunity and a risk. While CV and AV data are essential to planning and operations for the public and private sectors, sharing or exchanging data can be a risk depending on their use, accuracy, and whether the user understands the limitations of the data and uses them appropriately. For these reasons, many public agencies avoid situations that may present liability issues in terms of data quality or accuracy (61).

In addition, public agencies need to confront tensions related to data ownership, access, privacy, and security before considering opening data-sharing or -exchange platforms. Voluntary data-sharing initiatives are brokered on mutual benefit among all engaged stakeholders. However, many private companies are in direct competition and are therefore sensitive to sharing data they may see as proprietary in a public setting. Many vendors are more willing to share data when they are contracted to provide a service and under a nondisclosure agreement, but they are unlikely to share all data even under these conditions. For example, the Washington State GPS Freight Performance Measures project uses data from commercial fleet management GPS devices in trucks to develop statewide freight performance measures that in turn improve the performance of the system for trucks using it. The DOT assures the vendors that the GPS data is used for freight performance measurement only and not for regulatory or enforcement purposes. This addressed some concerns about providing an individual company's business-sensitive information, but the private-sector entities still required nondisclosure agreements.

The reluctance to share information pertains to the OEMs as well. Following an AV crash in 2015, the OEM used the raw data from the vehicle to determine what went wrong and to upgrade its software to include an improved algorithm (65). But the OEM did not share the improved algorithm with other OEMs, and as a result, the improved software algorithm remains a secret. By federal legislation, law enforcement does have access to EDRs for crash reconstruction and crash-reporting purposes, but would not have access to proprietary algorithms. Following the lead of USDOT, state legislatures, with the exception of California, have shied away from enacting comprehensive data-reporting laws because they want to encourage innovation in their states and so rely on voluntary reporting. There is recognition of the highly competitive nature of this technology and research and development. Each developer has proprietary systems and intellectual property that it must protect. Developers also have nonbinding commitments to protect data privacy, data security, and cybersecurity that need to be acknowledged.

Summary and Conclusions

This white paper discusses high-level data issues and opportunities, the regulatory environment in which CVs and AVs operate, data used and produced by CVs and AVs, and influences on data ownership, data privacy, and data sharing and exchange. AVs and CVs represent symbiotic but uniquely different technologies. Without a federal mandate, CV deployments are slowly proceeding through a few federal and state initiatives. However, USDOT initiatives are increasing the number of CV deployments. The advancements are also influenced state and federal rule making, such as FCC rule making regarding allocation of the spectrum. Advancements in AV technology are more ubiquitous, largely through private-sector activities in testing and deployment; still, the time frame for the transition to higher-level AVs is not clear.

This white paper represents the combined work of a subcommittee of the Texas CAV Task Force. This subcommittee is a dedicated group of public- and private-sector experts in CV and AV technologies, with an overarching and continuing responsibility to ensure the safe and efficient deployment and advancement of these technologies in Texas.

The United States has a complex regulatory environment, with local, state, and federal government agencies, as well as Congress, having authority to create rules that may govern CV and AV operations. Congress has authority to establish federal regulatory frameworks or standards. NHTSA has responsibility for the safety of motor vehicles. FCC manages the electromagnetic spectrum and has new rules on the splitting of the 5.9-GHz band between vehicle safety communications and unlicensed operations as of November 2020. States are responsible for operations of vehicles on public roads. Texas law has allowed automakers and others to test AVs without a driver inside and the use of connected braking systems on the state's roads and highways. In Texas, since CVs and AVs have been allowed to operate, more than 20 AV pilots and multiple CV pilots have operated, bringing with them opportunities for data sharing and exchange among private- and public-sector stakeholders.

Data privacy, data security, and cybersecurity are important concepts in the context of AVs and CVs. Data privacy relates to the collection, access, and use of sensitive personal information. Data privacy prevents a breach of PII that can cause harm to individuals, organizations, and agencies. Unlike widely thought, with data science analytics, anonymizing data no longer mitigates data privacy issues. In the United States, there is no comprehensive approach to data privacy regulation. FCC's nonbinding Fair Information Practices guide data privacy protections, but federal law does not require companies to have a privacy policy or notify consumers of their privacy practices. States such as California, Nevada, and Maine have data privacy laws, but only California's pertain to non-online business practices.

AVs and CVs use four types of data when operating: digital map data, data on roadside infrastructure, data on traffic and other road conditions, and data on the movements of other objects (i.e., people and vehicles). These data can be either on board (e.g., generated from a vehicle's sensors) or externally sourced. CVs and AVs also produce data as they operate or communicate with external vehicles and devices. Data generated include safety, diagnostic, road infrastructure, location, driving behavior, and traffic conditions. There is much overlap between the data CVs and AVs use and the data they generate.

CVs and AVs bring many data management challenges to both public- and private-sector agencies because of the vast amount of data that can be collected, transmitted, stored, and analyzed. And the testing phases of AVs and CVs (which are where the industries are focused now) generate more data than the operational phases. Therefore, confronting data management issues should be a priority.

CV and AV data are available and beneficial to both public and private organizations, so data sharing and data exchange among them are both wanted and needed. USDOT has launched several data-sharing initiatives, as have some state DOTs and private-sector consortia. Nearly all data sharing is done under a voluntary model—the preferred model under the current regulatory environments. For this to work, generalized data-sharing models need to focus on mutually beneficial scenarios.

The question of who owns these vehicle data has an evolving set of answers. It is informed by who has legal right to the data (e.g., vehicle owners in the case of EDRs), who has proximity to the data (e.g., OEMs), who has compiled and processed the data (e.g., data aggregators), and who operates the sensors generating the data (e.g., infrastructure owners/operators). Ownership also depends on characteristics such as the type of data, the stage of technology development, and the point in time the data are accessed and used. The issue of data ownership is an evolving challenge that still needs to be understood and resolved. It requires ongoing discussion among relevant stakeholders in the CV and AV ecosystems. It is important for groups such as the Data, Connectivity, Cybersecurity, and Privacy Subcommittee of the Texas CAV Task Force to continue working with public-private partners to deal with issues such as data sharing, data exchange, privacy, and cybersecurity protection. An exercise to inform these issues is to answer the following questions:

- Which entities are collecting, storing, and using what CV and AV data—how, for what purposes, and with what protections?
- What data gaps exist that hinder innovation and furthering the public interest?
- What data can be shared or exchanged to facilitate the safe and successful integration of AVs and CVs into the transportation ecosystem?
- What security and privacy protections need to be addressed and incorporated into AV and CV data collection and sharing?

Answering these questions will begin to clarify data ownership, data access, data use, and data-sharing issues. Particularly important are high-priority data for data sharing: information on work zones, real-time traffic and road conditions, roadway inventories, SPaT, cybersecurity, and safety performance. Addressing the ownership, technical, and policy issues surrounding these high-priority data categories will accelerate the safe deployment of AVs and CVs in Texas.

References

1. Institute of Electrical and Electronics Engineers. Connected Vehicles. https://site.ieee.org/connected-vehicles/ieee-connected-vehicles/connected-vehicles/.

2. Ipsos Business Consulting. *Connected Car: A New Ecosystem.* 2016. https://www.ipsos.com/en/connected-car-new-ecosystem.

3. McQuinn, A., and D. Castro. *A Policymaker's Guide to Connected Cars*. Information Technology and Innovation Foundation, January 16, 2018. https://itif.org/publications/2018/01/16/policymakers-guide-connected-cars.

4. RGBSI. *Driving Change: The Future of Mobility*. 2020. https://f.hubspotusercontent40.net/hubfs/2506444/Whitepapers%20and%20Downloadable%20Content/RGBSI%20Driving%20Change%20The%20Future%20of%20Mobility%20Whitepaper%202020.pdf?utm_campaign=Future%20of%20Mobility%20Whitepaper%20Download&utm_medium=email&_hsenc=p2ANqtz--z3_tZ2Ee4HlXsRiUBEU71LbgZPq-Ni2WMF8wyPvQLIlaK_WAdNUO6_K-k6O2bEmdSqO9jtVL4kOSSVLDVzuh-NC3kzQ&_hsmi=92537464&utm_content=92537464&utm_source=hs_automation&hsCtaTracking=b891f97c-9df5-486d-9cc6-9a886349b461%7C15504159-ba64-4b1d-9805-7e4b5f3acb0d.

5. Malinson, K. How C-V2X in 5G will Transform Cars and Save Lives. RCR Wireless News, February 6, 2020. https://www.rcrwireless.com/20200206/analyst-angle/c-v2x-5g-transform-cars-analyst-angle.

6. Autotalks. DSRC vs. C-V2X for Safety Applications. 2019. https://www.auto-talks.com/technology/dsrc-vs-c-v2x-2/#:~:text=DSRC%20and%20C%2DV2X%20are,distributed%20operation%20(mode%204).

7. Miller, L. *Connected Car for Dummies*. 2018. https://www.qorvo.com/design-hub/ebooks/connected-car-for-dummies.

8. SAE International. *SAE International Releases Updated Visual Chart for its "Levels of Driving Automation" Standard for Self-Driving Vehicles.* December 11, 2018. https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles/.

9. Fagella, D. The Self-Driving Car Timeline—Predictions from the Top 11 Automakers. Emerj, March 14, 2020. https://emerj.com/ai-adoption-timelines/self-driving-car-timeline-themselves-top-11-automakers/.

10. Ohnsman, A. Waymo Restarts Robotaxi Service without Human Safety Drivers. *Forbes*, October 8, 2020. https://www.forbes.com/sites/alanohnsman/2020/10/08/waymo-restarts-robotaxi-service-without-human-safety-drivers/#493ea97969d8.

11. Jones, H. Driverless Shuttles Rolling into DFW Airport. The Daily Campus, May 5, 2020. ihttps://www.smudailycampus.com/ae/driverless-shuttles-rolling-into-dfw-airport.

12. Holley, P. How Robots Are Helping One Texas Company Thrive during the Pandemic. *Texas Monthly*, August 5, 2020. https://www.texasmonthly.com/news/driverless-grocery-delivery-nuro-coronavirus-houston/.

13. Gates, G., K. Granville, J. Markoff, K. Russell, and A. Singhvi. The Race for Self-Driving Cars. *New York Times,* June 6, 2017. https://www.nytimes.com/interactive/2016/12/14/technology/how-self-driving-cars-work.html?partner=IFTTT.

14. Tangemann, C. Sensor Fusion: Technical Challenges for Level 4–5 Self-Driving Vehicles. Automotive IQ, October 21, 2019. https://www.automotive-iq.com/autonomous-drive/articles/sensor-fusion-technical-challenges-for-level-4-5-self-driving-vehicles.

15. Harrington, R., C. Senatore, J. Scanlon, and R. Yee. *The Role of Infrastructure in an Automated Vehicle Future.* National Academy of Engineering, June 15, 2018. https://www.nae.edu/183200/The-Role-of-Infrastructure-in-an-Automated-Vehicle-Future.

16. Burke, K. How Does a Self-Driving Car See? 2019. https://blogs.nvidia.com/blog/2019/04/15/how-does-a-self-driving-car-see/#:~:text=The%20three%20primary%20autonomous%20vehicle,as%20their%20three%2Ddimensional%20shape.

17. New Mobility. Hella Creates Open Fusion Platform to Simplify Development of Autonomous Driving Functions. March 26, 2019. https://newmobility.global/autonomous/hella-creates-open-fusion-platform-simplify-development-autonomous-driving-functions/.

18. Singh, A. Open Source Holds the Key to Autonomous Vehicles. Ubuntu, June 25, 2020. https://ubuntu.com/blog/open-source-economics-hold-the-key-to-autonomous-vehicles.

19. Nisenbaum, A. How Open-Source Data Can Drive Automotive Innovation. *Forbes*, March 29, 2020. https://www.forbes.com/sites/forbestechcouncil/2020/05/29/how-open-source-data-can-drive-automotive-innovation/#41027b34fd40.

20. National Academies of Sciences, Engineering, and Medicine. *A Look at the Legal Environment for Driverless Vehicles.* The National Academies Press, 2016. https://doi.org/10.17226/23453.

21. U.S. Department of Transportation. *Automated Vehicles 4.0: Ensuring American Leadership in Automated Vehicle Technologies.* January 2020. https://www.transportation.gov/sites/dot.gov/files/2020-02/EnsuringAmericanLeadershipAVTech4.pdf.

22. Federal Communications Commission. *Fact Sheet. Use of the 5.850–5.925 GHz Band. Notice of Proposed Rulemaking—ET Docket No. 19-138.* November 21, 2019. https://docs.fcc.gov/public/attachments/DOC-360940A1.pdf.

23. Federal Communications Commission. Use of the 5.850-5.925 GHz Band. *Federal Register*, February 6, 2020. https://www.federalregister.gov/documents/2020/02/06/2020-02086/use-of-the-5850-5925-ghz-band.

24. AASHTO Journal. FCC Opens Up 5.9 GHz Spectrum to Non-transportation Use. November 20, 2020. https://aashtojournal.org/2020/11/20/fcc-opens-5-9-ghz-spectrum-to-non-transportation-use/.

25. Ma, J., and S. Chiu. *Texas SPaT Challenge Update.* 2019. https://transops.s3.amazonaws.com/uploaded_files/SPaT%20Webinar%20-%20TxDOT.pdf.

26. U.S. Department of Transportation. Operational Connected Vehicle Deployments in the U.S. March 30, 2021. https://www.transportation.gov/research-and-technology/operational-connected-vehicle-deployments-us.

27. Ray, K., and B. Skorup. *Smart Cities, Dumb Infrastructure: Policy Induced Competition in Vehicle-to-Infrastructure Systems.* Mercatus Center, 2019. https://www.mercatus.org/system/files/ray-smart-cities-mercatus-working-paper-v1.pdf.

28. U.S. Department of Transportation. *Automated Driving Systems 2.0: A Vision for Safety.* 2017. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

29. U.S. Department of Transportation. *Preparing for the Future of Transportation: Automated Vehicles 3.0.* 2018. https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

30. National Highway Traffic Safety Administration. NHTSA Issues First Ever Proposal to Modernize Occupant Protection Safety Standards for Vehicles without Manual Controls. March 17, 2020. https://www.nhtsa.gov/press-releases/adapt-safety-requirements-ads-vehicles-without-manual-controls.

31. Gold, A. New Push for Autonomous Vehicles Bill. Axios, September 23, 2020. https://www.axios.com/new-push-for-autonomous-vehicles-bill-4f77892d-bcbe-4e74-a725-1b8ce9b9b46b.html.

32. Stoeltje, G. *Policy Brief: How Does Texas Law Change the Legal Landscape for Automated Vehicles?* Transportation Policy Research Center, Texas A&M Transportation Institute, November 2017. https://static.tti.tamu.edu/tti.tamu.edu/documents/PRC-2017-5.pdf.

33. Westin, A. F. *Privacy and Freedom*. Atheneum, 1967.

34. Zmud, J., M. Tooley, and M. Miller. *Data Ownership Issues in a Connected Car Environment: Implications for State and Local Agencies.* Strategic Research Program 165604-1. Texas A&M Transportation Institute, November 2016. https://tti.tamu.edu/tti-publication/data-ownership-issues-in-a-connected-car-environment-implications-for-state-and-local-agencies/.

35. Rocher, L., J. Hendrickx, and A. de Montjoye. Estimating the Success of Re-identification in Incomplete Datasets Using Generative Models. Nature Communications, July 23, 2019. https://www.nature.com/articles/s41467-019-10933-3.

36. De Montjoye, Y.-A., L. Radaelli, V. K. Singh, and A. S. Pentland. Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata. Science, January 30, 2015. 10.1126/science.1256297.

37. Zhang, S. Who Owns the Data Generated by Your Smart Car*? Harvard Journal of Law and Technology,* Vol. 32, No. 1, 2018. https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech299.pdf.

38. National Law Review. CCPA Enforcement Begins Today. July 1, 2020. https://www.natlawreview.com/article/ccpa-enforcement-begins-today.

39. Privacy4Cars. CCPA: California Consumer Privacy Act. 2020. https://privacy4cars.com/data-in-cars/ccpa/.

40. Karsten, J., and D. West. The State of Self-Driving Laws across the U.S. Brookings, May 1, 2018. https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/.

41. Huntun Andews Kurth. Texas Amends Data Breach Law; Now Requires Regulator Notification. June 26, 2019. https://www.huntonprivacyblog.com/2019/06/26/texas-amends-data-breach-law-now-requires-regulator-notification/.

42. Alliance of Automobile Manufacturers and Association of Global Automakers. *Consumer Privacy Protection Principles*. May 2018. http://autoalliance.wpengine.com/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

43. Bryans, J. The Internet of Automotive Things: Vulnerabilities, Risks and Policy Implications. *Journal of Cyber Policy*, Vol. 2, No. 2, 2017, pp. 185–194. DOI: 10.1080/23738871.2017.1360926.

44. Lemos, R. Car Hacking Hits the Streets. The Edge, January 7, 2020. https://www.darkreading.com/edge/theedge/car-hacking-hits-the-streets/b/d-id/1336730.

45. Institute of Electrical and Electronics Engineers. UN Announces New Cyber Security Regulation for Connected Vehicles. https://innovationatwork.ieee.org/un-announces-new-cyber-security-regulation-for-connected-vehicles/.

46. National Highway Traffic Safety Administration. *Cybersecurity Best Practices for Modern Vehicles.* Report No. DOT HS 812 333. 2016.

47. Institute of Electrical and Electronics Engineers. California Becomes the First State to Sign IoT Cyber Security Law into Existence. https://innovationatwork.ieee.org/california-becomes-the-first-state-to-sign-iot-cyber-security-law-into-existence/.

48. Pozza, D., and T. Lee. Massachusetts Ballot Initiative Raises Privacy and Data Security Concerns for Connected Devices. November 19, 2020. https://www.jdsupra.com/legalnews/massachusetts-ballot-initiative-raises-16498/.

49. Shimada, H., A. Yamaguchi, H. Takada, and K. Sato. Implementation and Evaluation of Local Dynamic Map in Safety Driving Systems. *Journal of Transportation Technologies*, Vol. 5, 2015, pp. 102–112. https://pdfs.semanticscholar.org/2aa1/ee00129fcefc4a55f6120854fd9b53a55e1b.pdf.

50. Hong, Q., R. Wallace, and G. Krueger. *Connected v. Automated Vehicles as Generators of Useful Data.* Michigan Department of Transportation and Center for Automotive Research, September 30, 2014. http://www.cargroup.org/wp-content/uploads/2017/02/CONNECTED-V.-AUTOMATED-VEHICLES-AS-GENERATORS-OF-USEFUL-DATA.pdf.

51. Somers, A. *Connected and Automated Vehicles (CAV) Open Data Recommendations*. August 23, 2018. https://austroads.com.au/publications/connected-and-automated-vehicles/ap-r581-18.

52. Mellor, C. Data Storage Estimates for Intelligent Vehicles Vary Widely. Blocks and Files, January 17, 2020. https://blocksandfiles.com/2020/01/17/connected-car-data-storage-estimates-vary-widely/.

53. Matthews, K. Here's How Much Big Data Companies Make on the Internet. Big Data Showcase, July 24, 2018. https://bigdatashowcase.com/how-much-big-data-companies-make-on-internet/.

54. Mellor, C. Autonomous Vehicle Data Storage: We Grill Self-Driving Car Experts about Sensors, Clouds, and Robo-taxis. Blocks and Files, February 3, 2020. https://blocksandfiles.com/2020/02/03/autonomous-vehicle-data-storage-is-a-game-of-guesses/.

55. Valentine, C. The Data Platform Is Key to Connected Cars and the Internet of Automotive Things. IoT Agenda, January 29, 2018. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/The-data-platform-is-key-to-connected-cars-and-the-internet-of-automotive-things.

56. Yoshida, J. If Data Is the New Oil, Who Profits from Connected Vehicle Data? EE Times, July 15, 2020. https://www.eetimes.com/if-data-is-the-new-oil-who-profits-from-connected-vehicles/.

57. Shaw, K. What Is Edge Computing and Why It Matters. Network World, November 13, 2019. https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html.

58. Institute of Electrical and Electronics Engineers. Real-Life Use Cases for Edge Computing. 2020. https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/.

59. Joshi, B. R. Determining the Interruption of Services While Performing V2I Communication Using the SPMD Prototype. 2016. https://digitalcommons.unomaha.edu/studentwork/342/.

60. Talas, M., R. Rausch, and D. Van Duran. Connected Vehicle Challenges for the Dense Urban Environment. *ITE Journal*, December 2018. https://www.ite.org/pub/?id=C0E206F8-FB90-92E6-0A13-AFEBE16B9894.

61. MetroPlan Orlando. *MetroPlan Orlando CAV Readiness Study: Task 1 Memorandum: CAV Industry Best Practices Review.* May 30, 2019. https://metroplanorlando.org/wp-content/uploads/MetroPlan-CAV-Readiness-Study-Task-1-Memo-Final.pdf.

62. U.S. Department of Transportation. *Federal Automated Vehicle Policy: Accelerating the Next Revolution in Roadway Safety.* September 2016. https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.

63. Talburt, J. A Review of Trusted Broker Architectures for Data Sharing. *Proceedings of the Fifteenth Annual Acquisition Research Symposium*, 2018. https://dair.nps.edu/bitstream/123456789/1623/1/SYM-AM-18-106.pdf.

64. U.S. Department of Transportation. *Roundtable on Data for Automated Vehicle Safety: Summary Report.* January 23, 2018. https://www.transportation.gov/av/data/roundtable-data-automated-vehicle-safety-summary-report.

65. Krompier, J. Safety First: The Case for Mandatory Data Sharing as a Federal Safety Standard for Self-Driving Cars. *Journal of Law, Technology and Policy*, Vol. 2017, 2017. http://illinoisjltp.com/journal/wp-content/uploads/2017/12/Krompier.pdf.