0-7130, Investigate Potential Connected and Automated Vehicle (CAV) Liability Issues Within TxDOT

Research Report (R1)

Texas A&M Transportation Institute

Published: February 2024

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA/TX-24/0-7130-R1		

4. Title and Subtitle	5. Report Date
INVESTIGATE POTENTIAL CONNECTED AND AUTOMATED VEHICLE (CAV) LIABILITY ISSUES WITHIN TXDOT: RESEARCH REPORT	Published: February 2024
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Todd Hansen, Billy Hwang, Tina Geiselbrecht, Greg Rodriguez, Gretchen Stoeltje, Priyanshi Shah, Ashley Thompson	Report 0-7130-R1

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Texas A&M Transportation Institute The Texas A&M University System College Station, Texas 77843-3135	11. Contract or Grant No. Project 0-7130

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Texas Department of Transportation Research and Technology Implementation Office 125 E. 11th Street Austin, Texas 78701-2483	Technical Report: 08/2021–08/2023
	14. Sponsoring Agency Code

15. Supplementary Notes

Project performed in cooperation with the Texas Department of Transportation and the Federal Highway Administration.
Project Title: Investigate Potential Connected and Automated Vehicle (CAV) Liability Issues within TxDOT
URL: https://tti.tamu.edu/documents/0-7130-R1.pdf

16. Abstract

Connected and automated vehicles (CAV) promise momentous and positive changes to most aspects of modern life. Mobility is likely to be characterized by collaborative, communicative and driverless vehicles operating in a connected network of vehicles, infrastructure and wireless devices. One of the most uncertain and as yet undefined areas where change can be expected is legislation surrounding the licensing and operation of these technologies. Questions of liability dominate research and conversation about how to manage new mobility paradigms, including in areas of state and local government tort liability. And although governmental entities typically enjoy some level of sovereign immunity, there are areas identified in state law where they have limited liability for specific torts. This research project identifies potential tort liability for the Receiving Agency and other governmental agencies associated with CAV technologies. The Performing Agency shall provide foundational research necessary for the Receiving Agency to proactively identify, assess and address legal liabilities that may arise under current law and legal liabilities that may arise under new law as the result of CAV implementations.

17. Key Words	18. Distribution Statement
Tort, liability, automated vehicle, connected vehicle, government, technology, data protection, privacy, infrastructure, immunity, waiver, condition, defect, design.	No restrictions. This document is available to the public through NTIS: National Technical Information Service Alexandria, Virginia http://www.ntis.gov

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	170	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

Table of Contents

List of Figures

List of Tables

1. Introduction

This report supports the Texas Department of Transportation (TxDOT) research project 0-7130, Investigate Potential Connected and Automated Vehicle (CAV) Liability Issues within TxDOT. The project investigated potential tort liability for TxDOT and local governments arising from CAV technology development and implementation. Through this project and report, the Texas A&M Transportation Institute (TTI) research team is providing foundational research necessary for TxDOT to proactively identify, assess, and address legal liabilities that may arise under current law and legal liabilities under new law as the result of CAV implementations.

Background

Transportation agencies at the state and local levels are currently overseeing or authorizing testing or deployment of autonomous vehicle (AV) or connected vehicle (CV) technologies, as well as CAVs.
CV technologies allow vehicles to receive and send alerts to or from other vehicles and infrastructure, while AVs are driverless or self-driving vehicles. Figure 1 illustrates the associated levels of automation. These levels, developed by SAE International, formerly the Society of Automotive Engineers, are the accepted industry standard (Society of Automotive Engineers, 2021).

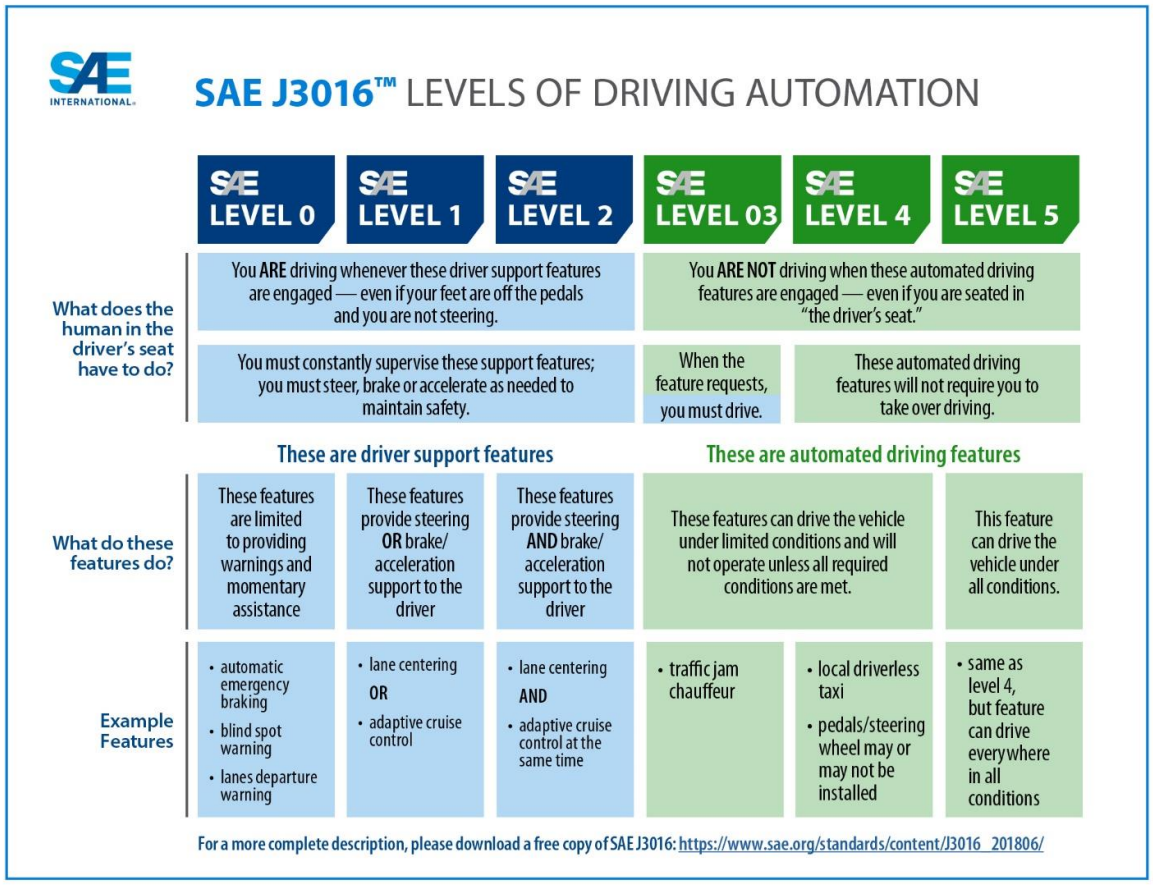

Figure 1. Levels of Automation.

CAVs leverage both CV and AV technologies by communicating with nearby vehicles and infrastructure and providing vehicle automation to make driving decisions. Governmental involvement in deployment of CAV technologies is raising questions about tort liability in the areas of vehicle operator liability, data ownership and privacy, notice, and the state's duty to cure a traffic, road, or other infrastructural condition or defect, among others. On one hand, CAVs promise momentous and positive changes to most aspects of modern life. Mobility is likely to be characterized by collaborative, communicative and driverless vehicles operating in a connected network of vehicles, infrastructure and wireless devices. On the other hand, there is a lack of certainty and consistency regarding governmental regulation of CAVs. In fact, one of the most uncertain and as yet undefined areas where change can be expected is legislation surrounding the licensing and operation of these technologies.

Questions of liability dominate research and conversation about how to manage new mobility paradigms, including in areas of state and local government tort liability. Under Texas common law, Texas state agencies (like TxDOT) and local jurisdictions are generally immune from liability. State agencies enjoy "sovereign immunity," and political subdivisions are considered to have "governmental immunity" (Evans, 2014). Although governmental entities typically enjoy some level of immunity from liability, there are areas identified in state law where such immunity is waived. Moreover, since CAVs are currently in the testing and development stage and not yet operating on a scaled basis, there are questions regarding how existing immunities for public agencies may be interpreted.

As part of TxDOT's exploration of new data sharing opportunities (e.g., receiving maintenance reports from AV trucks or digital sharing of TxDOT infrastructure data) and other opportunities (e.g., using an autonomous shuttle for TxDOT employees between campuses), this research project was initiated to delve into any legal liabilities that TxDOT and local governments with similar deployments should be aware of and proactively work to address. To this end, the research was intended to provide foundational research and a primer for TxDOT and local government use to proactively identify, assess and address legal liabilities that may arise as the result of CAV implementations.

Terminology

This report uses the term CAV to refer to the autonomous technology at issue, though there is still no single term unanimously adopted by all scholars and writers on this topic. Therefore, different terms are used throughout the review to describe the technology. Some use the term highly automated vehicle (HAV), while others refer to CAVs or C/AVs (connected and autonomous vehicles). Still others refer to connected and automated driving systems (C/ADS) hardware and software and AVTs (automated vehicle technologies). While these terms do not have identical meanings, they are broadly applied to discussions of legal and regulatory issues to the extent that they can be thought of as nearly interchangeable for purposes of this report.

However, once incorporated into statute and policy, the differences between these terms (and others they are confused with, such as advanced driver assistance systems [ADAS]) must be made clear. In technical documents, like legislation, rulemakings, or instruction manuals, they are terms of art with legal and binding meanings. Currently, efforts are underway to provide a national taxonomy for CAVs, including through the standards developed by SAE International (Society of Automotive Engineers, 2021). In the future, it is also

expected that definitions will be adopted by the National Highway Traffic Safety Administration (NHTSA) as part of a finalized federal regulatory framework for CAVs.

Project Approach

The TTI research team approached this research project with the objective to identify, assess and address legal liabilities that may arise under current law and legal liabilities that may arise under new law as the result of CAV implementations. To meet this objective, the research team performed six tasks. The following chapters of this report are structured to follow the sequence of these tasks and provide findings from the deliverables produced for each. The tasks comprised of the following:

- Literature Review—The research team conducted a comprehensive literature review to identify legal theories, statutes and case law from which tort liabilities may arise for state departments of transportation (DOTs) and local governments, and the risk mitigation techniques those entities undertook to address the liabilities. The literature review was designed to identify and define what types of tort liability CAV technologies may expose government agencies to and what emerging trends and approaches such agencies have developed or implemented to address tort liability for evolving technologies.
- Stakeholder Interviews—The research team collected feedback from subject matter experts from different organizations and stakeholder groups relevant to legal issues arising from CAVs. The interviewees represented the viewpoints of those who are regularly engaged in CAV issues and could provide perspectives from this field as it emerges, helping the TTI research team identify potential liabilities and mitigation techniques.
- State and Federal Law Analysis—The research team scanned Texas statutory codes and case law, and federal legislation and case law to identify relevant provisions and analyze them against tort liability issues identified in the literature review and stakeholder interviews.
- Use Case Legal Analyses and Recommendations—The research team performed legal analyses and provided recommendations to address liability concerns for seven use cases. The team, with input from TxDOT, developed use cases based on law and policy interests, describing the technical operation of each use case in written fact patterns and applying relevant laws and regulations to the fact patterns to perform a legal analysis of each use case.
- Peer Symposium—The research team planned and delivered a virtual Peer Symposium to understand experiences of stakeholders in the context of a moderated group discussion. This task involved virtually convening a group of practitioners involved in the testing and deployment of CAV technologies on behalf of public agencies to speak to the issues of tort liability, inviting symposium participants to share their experiences about issues that arose in their jurisdiction and what approach was taken to address those issues. The research team video-recorded and professionally edited the event and made the event available through the web-based tool developed in the next task.
- Web-Based Tool—The research team developed a web-based tool to serve as a one-stop shop for relevant statutes, policies, regulations and case law. As a web-based tool, it can easily be updated as the technology applications around CAV expand.

2. Literature Review

The purpose of the literature review was to scan available literature with a legal and tort liability focus at a high level to identify how states and other governmental units have addressed or may respond to issues of tort liability from CAV technologies. The TTI research team investigated 10 topical areas:

- Sovereign Immunity.
- Federal Preemption/Supremacy Clause.
- Design Immunity.
- Data Protection.
- Data Privacy.
- Data Ownership.
- Notice Regarding Infrastructure Conditions.
- Vehicle Safety Certification.
- Terms and Definitions.
- Insurance.

The findings of this literature review cover these categories and are structured to provide insights into each.

Methodology

The TTI research team reviewed 45 documents to identify legal theories, statutes and case law from which tort liabilities may arise for state DOTs and local governments, and the mitigation techniques those entities undertook. The reviewed documents included:

- Comprehensive research published by the Transportation Research Board (TRB) National Cooperative Highway Research Program.
- Research from research institutions and individual transportation researchers, advocacy groups, trade organizations and the U.S. Congress.
- Policy and guidance documents from state DOTs, the United States Department of Transportation (USDOT), NHTSA, and associations of regions, states, and transportation agencies.
- Articles from academic and legal journals.

The TTI research team recorded notes and key provisions from the documents into a literature review summary template. Reviewers summarized material from the literature into this document, which was reviewed and finalized with TxDOT, by the 10 topic areas listed above. The details of the TTI research team's literature review were then summarized in a master spreadsheet as the basis for this chapter.

As part of the literature review, the TTI research team conducted legal research into the question of whether a state DOT could be held liable for an incident involving CAVs. A brief summary of findings from this research is provided on the following pages.

Legal Research on DOT Liability for CAV Incidents

The legal research conducted for this project sought to answer whether a state DOT could be held liable for a collision involving an AV. The research found that case law concerning tort liability for state DOTs involving CAVs is scarce. However, case law involving other types of motor vehicle collisions indicate that it is possible for state DOTs to be held liable for negligent operation of vehicles owned by the state DOT under the motor vehicle exception to governmental immunity for tort liability. In the same way that plaintiffs have made successful claims against state DOTs for personal injury or property damage arising from negligent operation of vehicles by state DOT employees and known highway obstructions, a state DOT could risk liability if it owns and operates a fleet of AVs that are negligently operated by its agents and officers.

Dashi v. Nissan North America Inc., provides background about when common law tort claims may arise. *Dashi v. Nissan North America Inc.*, 247 Ariz. 56, 65 (Ariz. App. 2019). In that case the plaintiff crashed into a Nissan Rogue and sued Nissan alleging that the collision would not have occurred if Nissan equipped the Nissan Rogue with an automatic emergency braking system that provided forward collision warning and crash imminent braking. *Id.* The court stated that when a plaintiff's tort claims may represent an obstacle to NHTSA's achievement of a significant regulatory objective, they are preempted. *Id.* This is because if the plaintiff's negligence and design-defect claims were successful, they would impose a duty on manufacturers in Arizona for the design of automatic emergency braking systems. *Id.* The plaintiff's claim would frustrate the NHTSA's regulatory role because it would allow a jury-imposed safety standard on vehicles in Arizona. *Id.*

CAV incident litigation is still developing and there are a few cases: *Nilsson v. General Motors LLC, Hudson v. Tesla, Inc., Lommatzsch v. Tesla, Inc., Huang et al, v. Tesla, Inc.,* and two National Transportation Safety Board (NTSB) investigations including the Arizona Uber crash in 2018. None of these cases listed a state DOT as a defendant and state DOTs were largely uninvolved in the settlement or litigation of these cases. Further, the NTSB reports did not mention the role of state DOTs.

However, accidents involving non-AVs can be used as a baseline to understand if a state DOT may be held liable for incidents caused by an AV. Generally, there is a motor-vehicle exception to government immunity from tort liability. Government Tort Liability Acts have been enacted by state legislatures in 33 states, limiting the monetary amount of damages that can be recovered from the state. In addition, 29 states prohibit judgments against the state.

One exception to this general immunity is the motor vehicle exception which allow government agencies to be liable for bodily injury and property damage from the negligent operation by an officer, agent, or employee of a motor vehicle which the government agency owns. *Id.* Operation of a motor vehicle encompasses activities directly associated with driving the motor vehicle. *See Chandler v. County of Muskegon*, 467 Mich. 315, 321 (Mich. 2002). This definition is especially relevant in an AV context where driving is a dynamic term that does not entail a traditional driver in a vehicle operating the vehicle. Thus, how "operator" or "driver" is defined in a state within the context of AV operations can impact how the motor vehicle exception may be interpreted.

States without similar state tort claims acts may limit governmental immunity and establish a procedure for claims against the state. State Sovereign Immunity and Tort Liability, National Conference of State Legislatures, 2010, State Sovereign Immunity and Tort Liability (ncsl.org). Some state tort claims acts establish a special court, board, or commission to determine such claims and may limit damages or create exceptions to liability. *Id.* Connecticut, Illinois, Kentucky, North Carolina, and Ohio use this approach. *Id.*

Additionally, tort actions arising from motor vehicle accidents are subject to No-Fault Acts. *Hannay v. Dept. of Transp.*, 299 Mich. App. 261, 267 (Mich. App. 2013). A state No-Fault Act creates a no-fault auto insurance system by regulating the scope of recoverable damages in a negligence action involving a motor vehicle. *Id.* The act covers economic and noneconomic damages, and allows damages for bodily injury, work-loss benefits, and benefits for obtaining ordinary and necessary services for the injured person against governmental entities. *Id.* Currently 13 states or territories have a no-fault insurance system (Florida, Hawaii, Kansas, Kentucky, Michigan, Massachusetts, Minnesota, New Jersey, New York, North Dakota, Pennsylvania, Utah, and Puerto Rico). Further, the Court at a later stage in *Hannay* ruled that the phrase "liable for bodily injury" within the motor vehicle exception to governmental immunity means that a plaintiff who suffers bodily injury may recover for tort damages that naturally flow from the physical or corporeal injury to the body. *Hannay v. Dept. of Transp.*, 497 Mich. 45, 50 (Mich. 2014).

US DOT can be vulnerable to tort liability for personal injuries. In *Miller v. United States*, the plaintiff brought an action against the US DOT under the Federal Tort Claim Act for personal injuries resulting from a traffic accident. *Miller v. United States*, 710 F.2d 656 (0th Cir. 1983). The plaintiff alleged the agency failed to inspect construction plans to assure they complied with government regulation, and that the highway (I-10 in Garfield, County Colorado) was regulated and controlled by US DOT. *Id.* at 657-658. The Court in that case said the plaintiff's claims were within the discretionary function exception and the claims were dismissed. *Id.* at 663. In a subsequent case, a separate Court specified that though the federal government is not liable for inadequate warning, liability may attach if the government fails to issue warning of a known hazard. *See Mandel v. United States*, 793 F.2d 964, 967 (8th Cir. 1986); *see also Jurzec v. American Motors Corp.*, 856 F.2d 1116, 1119 (8th Cir. 1988). Further, a white paper for FHWA clarified that state and local entities, if not immune from a suit, will be liable if they act as manufacturers, sellers, distributors, designers, or operators of Intelligent Vehicle Highway System products. Nossaman, Guthner, Knox, Elliot, *Advanced Vehicle Control Systems Potential Tort Liability for Developers*, Prepared for Federal Highway Administration, 1993.

In *Jurzec v. American Motors Corp*, the plaintiff purchased a used Postal Service delivery truck and died when the truck rolled over while making a turn. 856 F.2d 1116, 1117. The Postal Service was selling surplus delivery trucks to the public and became aware of the rollover problem in 1980, and due to this, sale of the trucks was briefly suspended but then reinstated with a warning in the operator's manual and a label on the dashboard about the truck's potential rollover characteristic. *Id.* The deceased plaintiff brought a wrongful death suit and challenged the adequacy of the warning. *Id.* The Court ruled the warning was adequate because the warning sufficiently operated to serve the purpose of public safety. *Id.* at 1119.

Further, in *Mandel*, the Parks Service failed to warn park patrons of submerged rocks, a failure of park personnel to comply with a previously adopted policy. *Id.* Subsequent cases also looked at whether a government agent failed to follow a specific directive or to meet standards. *See McMichael v. United States*, 751 F.2d 303, 305-07 (1985); *see also Aslakson v. United States*, 790 F.2d 688 (8th Cir. 1986). In *Jurzec*, the officials did not fail to meet a requirement or directive. *Id.* at 1120.

This is relevant to the AV context because if the U.S. DOT has a specific directive, policy, or requirement for AV vehicles and includes public safety as a facet of this directive, they may be liable under the discretionary function exception to the Federal Tort Claim Act if a Court finds the agency failed to comply with the directive. Following the reasoning above, liability may also apply if adequate warning is not provided for any safety concerns during the operation of AVs through a federal program.

AV collisions have occurred and are likely to occur again. Though there have been no known cases filed against a state DOT related to an injury caused by an AV accident, a state DOT owned and operated AV could, if involved in a collision, expose a state DOT to tort liability under the state's motor vehicle exception to its Government Tort Liability Act. How such liability may or may not apply to a state that has permitted the operation of AVs on public roads without federal safety standards being implemented is not yet known.

Findings

The literature review focused on recent documents (i.e., 2016 and later) under the assumption that these would include up-to-date discussions or applications of CAV legislation or legal questions. Many of the documents provide informed and thoughtful speculation about the details of legal areas that may affect tort liability for CAVs. However, most of the literature to date focuses on the issue of tort liability as it relates to vehicle or component manufacturers, suppliers and sellers (i.e., product liability) and the ability of third parties to recover from insured drivers and manufacturers of CAVs. While few sources included discussions about the liability of state DOTs or other public regulators, analogies may be made to government liability from CAVs.

The reviewed documents share a number of common themes, namely:

- The federal government should retain oversight over vehicle safety. This may include the licensing of CAVs.
- State product liability law should continue to govern tort liability matters for defective design, manufacture and instruction.
- States should retain their authority over human driver licensing, vehicle registration, traffic laws and enforcement.
- Until NHTSA issues new Federal Motor Vehicle Safety Standards (FMVSS) for CAVs that account for their differences from conventional vehicles, the CAV technologies at issue will continue to blur the clear lines that now exist between state and federal legal authority.
- States are left to legally define and manage all new questions of law that continually arise but do not fit neatly into existing legal frameworks, including tort law and existing immunities.

While the literature review produced relevant findings on many key issues, it did not reveal many insights into the issues of proprietary data sharing and notice. Further, the literature review did not produce any examples

of active or outstanding legal matters involving tort liability for state agencies related to CAV technologies. These areas are opportunities for further research and analysis.

Specific findings from the reviewed documents are organized below in relation to the 10 topical areas referenced above.

Sovereign Immunity

For this topic, researchers identified issues such as sovereign immunity, governmental immunity, state and governmental liability, and constitutional or statutory waivers. Of the documents reviewed, four directly addressed this topic. Though most of these documents addressed the issue through anticipated CAV scenarios, *Texas Tort Claims Act Basics* provides a detailed description of sovereign immunity for the State of Texas and its political subdivisions in general:

> Governmental entities are generally immune from liability. The Tort Claims Act waives governmental and sovereign immunity of these entities and determines the liability of governmental entities related to personal injury and property damage caused by the negligence of a government employee or defect in government property (Evans, 2014).

The Texas Tort Claims Act partially waives that immunity for allegations of negligent conduct. Intentional tort actions are brought under the Federal Civil Rights Act.

Texas Civil Practice & Remedies Code §101.021 provides that immunity is waived and a governmental unit is liable for:

> …property damage, personal injury, and death proximately caused by the wrongful act or omission or the negligence of an employee acting within his scope of employment if:
>
> (A) the property damage, personal injury, or death arises from the operation or use of a motor-driven vehicle or motor-driven equipment; and
>
> (B) the employee would be personally liable to the claimant according to Texas law; and
>
> (2) personal injury and death so caused by a condition or use of tangible personal or real property if the governmental unit would, were it a private person, be liable to the claimant according to Texas law.

As currently constructed, this statute might not apply if a claim arose from a crash caused by a driverless vehicle owned by a DOT. However, if the claim arose from an incident caused by another type of employee (e.g., someone responsible for monitoring road safety systems), this statute may still apply. In a case where these elements are present, TxDOT could waive its sovereign immunity. In fact, *Texas Tort Claims Act Basics* provides an example of TxDOT's waiver of its immunity under the theory of joint enterprise when its agent, the Metropolitan Transit Authority of Harris County, built and maintained a high occupancy vehicle lane where a collision occurred that implicated the road's safety (Evans, 2014).

Sovereign immunity is detailed in two other documents. *Smart Transport for Cities and Nations: The Rise of Self-Driving & Connected Vehicles* speculates that CAVs are not expected to dramatically alter governmental liability. Rather, roadside units and other CAV infrastructure are likely to fall into existing categories of operation already contemplated by statute (Kockelman K. a., 2018). Such analysis assumes both connected and automated technologies in a vehicle.

Implications of Connected and Automated Driving Systems, Vol. 3: Legal Modification Prioritization and Harmonization Analysis provides context on the discussion in general, noting that early writing (between 1992 and 2004) on the implications of intelligent transportation systems addressed government liability issues. However, that focus shifted in the literature by 1997, with USDOT shifting its attention from automated highway systems to automated vehicles. This document also cites a U.S. Government Accountability Office report that notes both the auto industry and state DOTs might be unwilling to implement full automation unless their respective liability was limited (Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 3: Legal Modification Prioritization and Harmonization Analysis, 2018).

Federal Preemption/Supremacy Clause

In reviewing for federal preemption and the supremacy clause, researchers identified issues such as federal requirements upon which federal aid is conditioned, emerging CAV regulations that affect TxDOT liability, National Transportation Safety Board findings or rulings, and the Interstate Commerce Clause. Of the documents reviewed, 16 directly addressed federal preemption and the supremacy clause.

Most documents refer to the common assumption about federal preemption that the federal government will continue to regulate vehicle design and establish safety criteria through FMVSS. In *Preparing for the Future of Transportation: Automated Vehicles*, USDOT asserts the scope and authority of the FMVSS (U.S. Department of Transportation, 2018). As the federal standard, the FMVSS would generally preempt state and local safety standards if those state or local standards do not meet federal requirements. Likewise, the federal standards would supersede any state law that sought to impose a performance standard not consistent with the federal standard on a motor vehicle or equipment manufacturer in a state law tort claim.

Thus, states should expect to continue oversight over vehicle registration, driver licensing, traffic laws and enforcement, and motor vehicle insurance and liability regimes. However, the documents note that until a comprehensive federal framework is developed, states should address their own laws that codify federal requirements and be prepared to make modifications to them that would allow incorporation of new federal provisions (Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 3: Legal Modification Prioritization and Harmonization Analysis, 2018). As noted above, states may also need to prepare for increased federal preemption as the human driver is removed from control of the vehicle and safety verification and related licensing rules move toward NHTSA jurisdiction.

The literature review revealed a number of more specific observations about federal preemption. The first highlighted an area of uncertainty around the limits of the FMVSS' reach as to whether it preempts state common law claims. USDOT, in *Preparing for the Future of Transportation: Automated Vehicles*, notes that it may not automatically exempt a party from common law tort liability for harm caused by negligent conduct (U.S. Department of Transportation, 2018). Other authors speculate that federal law may preempt state law in certain claims, including claims of inadequate warning (Trimble T. E.-O., 2018).

A second set of observations concerns the U.S. Constitution's Commerce Clause, which locates the power to regulate interstate commerce with Congress (Glancy D. J., 2016). One author notes that the same theory that the U.S. Supreme Court used in striking down state motor vehicle regulations—that they imposed an undue burden on interstate commerce—could be applied to other areas, including intelligent vehicles that operate

across state lines (Canis, 2021). Another author notes that the federal government's ability to condition its financial support on matters of state law has the effect of overriding state authority. In this case, while not a mandate or preemption per se, the federal government supports a nationwide policy of seamless interstate commerce by incentivizing the compatibility between interstate and intrastate commercial vehicle regulation as a condition of eligibility for grant funding under the Motor Carrier Safety Assistance Program (U.S. Department of Transportation, 2018).

A third set of observations about federal preemption centers around Congress' recent first steps toward explicit preemption of state and local laws regarding CAVs through H.R. 3388, the Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution (SELF DRIVE) Act of 2017 (Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 5: Developing the Autonomous Vehicle Action Plan, 2018). Though not passed into law (the bill passed the U.S. House of Representatives but not the U.S. Senate), the SELF DRIVE Act would have regulated HAV safety, cybersecurity and data privacy. It would have mandated updates to FMVSS and new safety testing and certification requirements for automakers. It would have also prohibited "any state or local government from effect[ing] any law or regulation regarding the design, construction, or performance of highly automated vehicles, automated driving systems, or components of automated driving systems unless such law or regulation is identical to a standard prescribed under this chapter" (Jones Day, 2021).

Though the likelihood of Congress passing such laws in the future is uncertain without further research, should these powers eventually be granted to the federal government, they could affect TxDOT's liability if it were party to a tort claim regarding design, construction or performance of HAVs, automated driving systems (ADS) or their components where federal law preempts state law.

Design Immunity

With regard to the design immunity topic area, researchers identified issues such as the appropriateness of existing state-owned infrastructure for CAVs and unsafe conditions in the public right-of-way. Of the documents reviewed, none addressed the topic directly, but 11 raised issues related to liability due to road design. Therefore, this section includes a brief discussion about liability related to design followed by a discussion of design immunity.

Infrastructure Design for CAVs

Most of the documents refer to the needs of CAVs that are different from the needs of human drivers. Earlier research identified measures that a state DOT should take, including changes to design and access requirements necessary for safe CAV operation, noting that the more interdependent vehicles and infrastructure become, the "larger [the] aperture for negligence claims against state and local authorities (and implication of the various immunities that can apply to government decision making)" (Glancy D. J., 2016).

For example, one study notes:

> As CAVs increase in market penetration, requirements in the TxDOT Roadway Design Manual (and potentially other manuals as well) will need consistent updates to reflect the ongoing changes in vehicle technology. Certain requirements that may change include those for sight distance, curve radii, cross-sectional slopes, and other elements of geometric design. Ideally this should be completed in concurrence with changes in the AASHTO Roadway Design

> Manual. However, even if AASHTO does not make significant changes, TxDOT should still consider updating any pertinent in-house manuals to ensure that Texans can benefit from CAVs, and that it has mechanisms in place to ensure the safety of these vehicles and passengers (Kockelman K. L.-O., 2016).

A Look at the Legal Environment for Driverless Vehicles—Part 1 notes that CV infrastructure may increasingly expose local governments to defective programming claims (Glancy D. J., 2016). *Review of Automated Vehicle Technology: Policy and Implementation Implications* describes a 2017 pilot program planned for Gothenburg, Sweden, that would limit operation to certain "certified" roadways that are marked and instrumented for AVs (McGehee, 2016). In Wisconsin, an executive order mandated that a committee identify roads that could be designated special corridors for AV and CV testing and operation. Thus, limiting access to roads designed or modified for CAV operation may be another strategy for avoiding liability. Liability considerations through immunity will potentially be minimized as standards for CAVs related to safe operation are adopted and implemented.

Altogether, the research strongly suggests that infrastructure design changes may be necessary for the safe operation of CAVs. To prepare legally, state DOTs should identify what those changes may encompass and prepare their roadway design accordingly. However, states will also need to balance investment in infrastructure changes with the still evolving state of CAV technologies.

Design Immunity

Design immunity is an affirmative defense available in certain jurisdictions (e.g., California) for government entities facing claims of harm due to dangerous conditions of public properties (Judicial Council of California, 2020). This defense is used against tort claims, including those involving transportation facilities. Defendants may avoid liability if they can prove:

- A causal relationship between the plan or design and the accident.
- Discretionary approval of the plan or design prior to construction.
- Substantial evidence supporting the reasonableness of the plan or design (Roshanzamir, 2018).

If design immunity were made available to Texas governmental entities, it could potentially serve to relieve an entity of that liability if the state's general sovereign immunity proved insufficiently protective. Design immunity could be especially helpful in the transitional period when increasingly automated vehicles are traveling on roadways designed for human drivers, assuming those vehicles have different infrastructure design needs than human-controlled vehicles. Asserting a design immunity defense—showing that, at the time of design and construction, a design was safe and approved—could relieve a state DOT of liability for harm caused by a CAV traveling on a roadway not designed for it.

However, design immunity can be overcome even if a design is found reasonable if changed physical conditions have occurred to render the design now unsafe. The three elements necessary to overcome design immunity are:

> (1) The plan or design has become dangerous because of a change in physical conditions;
>
> (2) The public entity had actual or constructive notice of the dangerous condition it created; and

> (3) The public entity had a reasonable time to obtain the funds and carry out the necessary remedial work to bring the property back into conformity with a reasonable design or the public entity had not reasonably attempted to provide adequate warnings (Roshanzamir, 2018).

Handling CAV Data

CAVs are generating data about vehicles, drivers and infrastructure, which carry a high value to varying interests in the public and private sectors. The TTI research team explored three related but distinct topic areas concerning data: data protection, data privacy and data ownership. Each implicates a different legal interest, risk management strategy, defense or remedy, but all flow from the same conditions created by the unprecedented availability of and uses for data generated from CAVs and CAV-supportive infrastructure.

In the modern data-rich world, the transportation sector seeks to become more data-driven for planning, operational and other decision-making purposes (Association of Metropolitan Planning Organizations, 2019). This is especially true for anonymous and aggregated location-based data that are being collected and sold to transportation agencies.

Digital data can enhance many functions of a state DOT, including travel demand forecasting and planning, timely assessment of roadway conditions, and location-specific crash reporting and beyond. The benefits of such widespread data availability to a public service provider like a state DOT seem almost infinite, but so do the challenges.

In *National Framework for Regional Vehicle Connectivity and Automation Planning*, the Association of Metropolitan Planning Organizations notes that those challenges include proper use and management of data, institutional capacity, tension between data collection and privacy/protection concerns, and proprietary interests (Association of Metropolitan Planning Organizations, 2019). In *Review of Automated Vehicle Technology: Policy and Implementation Implications*, McGehee et al. offer a short list of data risks for state DOTs and other data handlers to consider:

> Policy questions concerning data use and legal issues abound, including how long data from [AV technologies] should be stored and maintained and by whom (Anderson et. Al, 2014). As automated vehicle technology progresses, privacy issues will be at the forefront. Who owns the data generated by AVT and does this data fall under current laws and court precedents, or will new laws and regulations be needed (Garcia, Hill, and Wagner, 2015)? (McGehee, 2016).

Data and privacy issues present another policy gap that federal and state policymakers will need to address as they regulate CAVs. The absence of federal action thus far means that states must decide whether to wait for federal action on cybersecurity and privacy or regulate at the state level (Association of Metropolitan Planning Organizations, 2019).

Below are the three specific topic areas related to data that the TTI research team identified in the literature review.

Data Protection

For this topic area, researchers identified issues such as proprietary data, cybersecurity, and data storage and transfer. As noted above, the literature review did not reveal any significant insights into the issue of

proprietary data. However, of the documents reviewed, 18 addressed the issues of cybersecurity and data storage and transfer.

Cybersecurity underlies many of the specific legal questions and new responsibilities for public entities involved with CAV technologies. As many documents note, hacking of CAVs could present consequences that "affect fundamental safety and functionality of a motor vehicle" (Channon, 2021). While vehicle, component and technology manufacturers or sellers could be liable under products' liability theories for harms resulting from such hacking, "data breaches and hacking incidents can also result in liability for agencies, [and] operators" (Kockelman K. L.-O., 2017).

The literature revealed a number of recommendations parties can consider to prepare for data management and anticipate data risks, from data audits and management plans to written cybersecurity policies. In *Implications of Connected and Automated Driving Systems, Vol. 4: Autonomous Vehicle Action Plan*, Trimble et al. recommend that states take the following actions:

- "Rigorous examination of the types of consumer data that could be collected by [C/ADS] as well as by connected infrastructure located outside vehicles."
- Assessments of "how third parties might use this collected data to compromise consumer privacy," including "whether some consumer data could be used by law enforcement or made publicly accessible through Open Records Statutes in ways that conflict with legitimate consumer privacy interests."
- In the short term, "consider statute changes to ensure public confidence and clarity on data collection and use."
- "Ensure that if privacy-sensitive data is collected on vehicles through connected infrastructure or otherwise, that data is not publicly accessible" (Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 4: Autonomous Vehicle Action Plan, 2018).

Had the SELF DRIVE Act been enacted, it would have mandated the following:

- For vehicle manufacturers to develop written cybersecurity policies that "identif[ies], assess[es], and mitigate[es] reasonably foreseeable vulnerabilities from cyber attacks or unauthorized intrusions, including false and spurious messages and malicious vehicle control commands."
- For companies to "tak[e] preventive and corrective action to mitigate against [such] vulnerabilities."
- For vehicle manufacturers to develop a written privacy plan with respect to information "collection, use, sharing, and storage," as well as practices for "data minimization, de-identification, and retention about vehicle owners or occupants" (Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 4: Autonomous Vehicle Action Plan, 2018).

This is notable because it indicates the policy direction that the federal government may take with CAV data protection—placing the primary burden on vehicle manufacturers and other private entities.

Data Privacy

For this topic area, researchers identified issues such as personally identifying information, open records requests, and actions under the Freedom of Information Act. Of the documents reviewed, 20 addressed data privacy.

In addition to hacking and safety failures, there are other risks from digital data vulnerabilities. Both proprietary corporate information and sensitive information of individuals are also at risk of loss, theft, and misuse in digital systems that store, collect, manage, convey, and otherwise distribute such data. As such, state DOTs are advised to take pains to clearly understand data use and protection rules expressed in contracts with data providers or in state or federal statute, and the types of consumer data that are collected by vehicles and infrastructure. On top of this, state DOTs are advised to make every effort at transparency regarding the management of private data (McGehee, 2016). This includes considering and mitigating risks around data sources dependent on mobile phones or related to online financial transactions.

A number of data privacy models are emerging in the United States and abroad. In *Autonomous Vehicles: Legal and Regulatory Developments in the United States*, the authors note examples from the European Union and the European Economic Area where the General Data Protection Regulation (GDPR) mandates standard data inventory, mapping of data flows, opt-out processes, and disclosure and contract requirements (Jones Day, 2021). The GDPR defines "individuals' right to privacy [which] includes a human right and property interest over their personal data" and requires private companies to "adhere to specific standards for protecting those interests." These data privacy requirements will likely influence private-sector behavior and policies in the United States since the scope of the GDPR will affect private companies worldwide and possibly any entities they contract with, including public agencies.

The authors also provide examples from the United States of domestic data privacy regulation. California's Consumer Privacy Act allows "private rights of action for data breaches. Its protections cover certain data breaches involving specific, personal information. Moreover, companies are given the opportunity to cure a violation before consumers are entitled to damages." Under the law, the State of California is authorized to "bring actions for civil penalties" (Jones Day, 2021).

Aside from this, there are differing approaches under state laws in the United States, which "create uncertainty and a lack of uniformity for HAV manufacturers and sellers" (Jones Day, 2021). Until the federal government develops nationwide regulations for CAVs, states are advised to take two steps to address legal issues related to data protection and data privacy:

- Ensure that any privacy-sensitive data collected from vehicles through connected infrastructure or otherwise are not publicly accessible (e.g., through open records statutes) in ways that could compromise the privacy of individual drivers (e.g., by being linked to specific cars).
- Consider whether this same data could be used by state enforcement officials in ways that compromise Fourth Amendment protections against unconstitutional searches and seizures (Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 5: Developing the Autonomous Vehicle Action Plan, 2018).

In order to take action on such recommendations, legislative modifications may be needed to ensure exceptions to public records laws are up to date with potential uses of data to benefit the public interest.

Data Ownership

In the realm of data ownership, researchers identified issues related to the right to convey. Of the documents reviewed, 21 addressed this topic. This topic is relevant for a state DOT that might acquire data from or

transfer data to an external or third party. Ownership will determine some of the contractual terms that define a state DOT's use of data, including compensation and indemnification. However, questions of data ownership also implicate a public entity that itself collects or gathers data directly from vehicles, other digital devices or infrastructure. Due to a special interest in TxDOT's ability to convey data it had gathered and what risks were associated with such conveyance, data ownership is examined with this question in mind.

Autonomous Vehicles: Legal and Regulatory Developments in the United States raises several legal issues arising from the value and personal nature of data:

- What data should be permissible to collect?
- Who owns the data, and who can monetize the data, under what conditions?
- How should [CAV automotive and technology] industry members store and protect data to ensure privacy—whether from monetization, hacking, or identity theft (Jones Day, 2021)?

The document goes on to identity interests that may be balanced by contractual means until a more comprehensive overarching solution is available:

> Consumers presumably will want to retain control over their personal information, and manufacturers will want, at a minimum, to access certain information for integration and optimization of their HAVs (Jones Day, 2021).

This conflict could be addressed if consumers agree to release data in exchange for certain accommodations from manufacturers, such as features or compensation. Alternately, data ownership could be divided, provided or received in vendor contracts, sales contracts, or vehicle owner's manuals and privacy notices. In the end, however, the authors conclude that "the ultimate question of who owns the data has yet to be resolved in any uniform way and will likely be contested" (Jones Day, 2021).

Notice Regarding Infrastructure Conditions

When considering infrastructure conditions, researchers identified where documents defined or explained the duty to cure defects and what constitutes notice. Of the documents reviewed, 17 addressed this topic. The literature revealed several ways that CAV technology might call for changes to the definitions and requirements for notice regarding the duty to remedy unsafe roadway conditions for TxDOT.

Actual Notice

Texas Tort Claims Act Basics discusses a number of situations, both at the municipal and state levels, when a governmental unit's duty to remedy an unsafe situation is triggered—all requiring actual notice (Evans, 2014). Regarding the removal or destruction of a traffic sign, signal, or warning device by a third person, the governmental unit (here a city) is liable only if it fails to correct the situation within a reasonable time after actual notice. Actual notice is defined by at least one Texas appellate court as "information…actually communicated to or obtained by a city employee responsible for acting on the information." As discussed further below, within the context of CAVs, further analysis is warranted about whether notice from a CAV of an infrastructure issue (e.g., pothole or inadequate striping) through data sharing between the state and vehicle would constitute notice.

In a case involving a state agency, TxDOT's failure to stop the repeated removal of traffic signs by vandals did not trigger the state's actual notice requirement, according to the Supreme Court of Texas. The state's immunity was not waived when TxDOT made discretionary decisions regarding a stop sign's susceptibility to repeated vandalism. The court found that TxDOT did not fail in its duty to correct the stop sign's "condition" simply because it was repeatedly vandalized (i.e., removed). TxDOT was not found liable on the grounds that its remedy of the situation (replacing the signs) was not designed to prevent further removals.

When the need for repair is the result of a component failure, act of God, or act of a third party, a governmental unit will be given a reasonable time to cure. However, a governmental unit could be held strictly liable for injuries and deaths if the absence or malfunction of the traffic control device was caused by one of its employees (Evans, 2014).

While digital hacking is not part of the fact pattern in these cases, nor could have been contemplated at the time they were adjudicated, the notice requirements triggering the duty to remedy an unsafe roadway condition caused by a third party's vandalism may provide guidance as to how hacking of CAVs and connected infrastructure might be treated and where liability may lie.

Digital Receipt of Roadway Information

One potential benefit of CAV technology is that it may enable a transportation agency to receive roadway condition information quickly and efficiently from CAVs, connected devices, and infrastructure. While this could create more frequent and accurate reporting on infrastructure conditions, it could also change or affect what constitutes notice and when a state DOT's duty to remedy an unsafe condition is triggered in the case of malfunctioning infrastructure.

In *Smart Transport for Cities and Nations: The Rise of Self-Driving & Connected Vehicles*, Kockelman et al. postulate that notice could actually occur when a signal from the malfunctioning infrastructure is sent or when an employee has reason to discover the defect from incoming data. The determination of notice could also be affected by whether the infrastructure is categorized as a data device rather than personal or real property. If the digital infrastructure is considered a data device, the malfunction could be exempt from liability (Kockelman K. a., 2018).

Regarding notice about general roadway conditions, Stamatiadis et al. observe in *Strategic Planning for Connected and Automated Vehicles in Massachusetts* that CAV systems "could provide asset health information" requiring the agency to "improve operational awareness and update asset management systems" (Stamatiadis, 2018). Besides state-owned or -operated infrastructure with the ability to notify a governmental unit of its condition, asset health information could come from privately owned vehicles or other connected devices, prompting other questions of notice, including:

- How and when is that information communicated and received?
- When does notice occur under these conditions?

Kockelman et al. similarly note that the increased frequency of roadway condition information could result in double the maintenance burden for TxDOT (Kockelman K. a., 2018).

Duty to Provide New or Different Infrastructure Design or Maintenance

As noted above, safe roadway design for CAVs may be different than it is for human drivers. Adding to the list of differences between human- and CAV-centric design, in *Issues in Autonomous Vehicle Testing and Deployment*, Canis notes:

> To successfully navigate roadways, an autonomous vehicle's computers, sensors and cameras will need to accomplish four tasks that a human driver undertakes instinctively: detect objects in the vehicle's path; classify those objects as to their likely makeup (e.g., plastic bag in the wind, a pedestrian, or a moving bicycle); predict the likely path of the object; and plan an appropriate response (Canis, 2021).

Such objects—whether on the roadway legitimately installed by a transportation agency or not—are among many considerations a state DOT must take into account when planning, designing, constructing and maintaining a road that should be safe for CAV operations.

Related to design and planning responsibilities of a state DOT or municipality are "special defects." In *Smart Transport for Cities and Nations: The Rise of Self-Driving & Connected Vehicles*, Kockelman et al. describe special defects as excavations and other obstructions that are implemented or placed by state DOTs. Different standards may be required of special defects to ensure that CAVs can detect them (Kockelman K. a., 2018).

These examples, together with the design discussion above, indicate that, at some point in the transition from human-driven to automated vehicles, state DOTs may be put on notice, either actual or constructive, that they must design and maintain infrastructure for CAVs rather than for humans only. Depending on federal action on the issue, this could require establishing unique, state-specific standard operating procedures and design manuals.

Actions States Could Take to Prepare

Many literature sources acknowledge that CAVs will need different roadway infrastructure conditions from human-driven vehicles. Some offer options state DOTs can consider to mitigate liability for that difference, while others caution against proceeding too quickly to accommodate CAVs.

In *A Look at the Legal Environment for Driverless Vehicles—Part 1*, Glancy et al. suggest building dedicated lanes or entirely segregated roads for driverless vehicles only. However, they also note that because of the great expense of these options, both in terms of construction and right-of-way acquisition, they will likely not be adopted (Glancy D. J., 2016). This will be especially true if, as Chatman and Moran, in *Autonomous Vehicles in the United States: Understanding Why and How Cities and Regions Are Responding*, assert, "AV deployment is slower than current projections, ultimately serving only a fraction of vehicles on the road" (Chatman, 2019). In that case, redesigning and repurposing roads for AVs may not be a helpful approach.

Others suggest a more proactive approach involving testing and communicating with automakers before CAVs are in operation. In *Adopting and Adapting: States and Automated Vehicle Policy*, Lewis et al. suggest that before committing resources to retrofitting existing infrastructure or building new facilities, states could initiate testing to understand exactly what the infrastructure needs of CAVs are (Lewis P. R., 2017). This would enable state DOTs to clearly communicate to CAV manufacturers and the public the extent to which the state's current roadway design and maintenance practices are safe for CAVs. These authors also note that "it is unrealistic to

expect states to update every roadway to have very high-quality pavement, signage, and striping." However, since "AVs need to be able to operate safely regardless of the road condition…targeting state of good repair funds to roadways with safety problems, or to high-risk areas such as work zones, can be a good place for states to start." As an example, the authors point to Virginia's Automated Corridors initiative, where AV pilot projects include "high-quality lane markings as a primary resource for its testing corridor" (Lewis P. R., 2017).

In *Fault-y Reasoning: Navigating the Liability Terrain in Intelligent Transportation Systems*, Lederman et al. highlight education for transportation professionals as a preemptive approach to protect governments from liability, citing an existing program in New York:

> The liability for municipalities regarding highway construction and conditions is complex enough to warrant the Cornell Local Roads program to offer a course for local government managers on how to protect their jurisdictions under state law (Lederman, 2016).

A way to formalize this knowledge of CAV capabilities and limits regarding road condition needs and assumption of liability is by contract. *Autonomous Vehicles: Legal and Regulatory Developments in the United States* notes that AV manufacturers can transfer the risk of liability to vehicle owners by sales contracts and in manuals that specify unsafe uses such as traveling over unpaved or unmarked roads (Jones Day, 2021). For transportation agencies, the duty to remedy unsafe roadway situations may still apply, along with the requirement of actual notice. However, this could limit the government's potential liability to paved, marked roads.

Federal Positions

Though largely advisory in nature, guidance from the federal government supports communication and collaboration. In *Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0* (U.S. Department of Transportation, 2020) and *Preparing for the Future of Transportation: Automated Vehicles* (U.S. Department of Transportation, 2018), USDOT recommends that states collaborate with CAV developers and testers to prepare infrastructure for CAVs. These documents, along with USDOT's *Automated Vehicles Comprehensive Plan*, also state USDOT's intent to update infrastructure standards to reflect CAV technologies and update the *Manual on Uniform Traffic Control Devices* (MUTCD). States are required to adopt federal MUTCD standards as their standard, adopt the national MUTCD along with a state supplement, or adopt a state traffic control device manual in substantial conformance with the national MUTCD. This means that roadway markings and signage can differ from state-to-state since MUTCD standards are not uniformly applied across all states. Thus, even if USDOT updates the MUTCD for CAVs, non-compliance (e.g., differences in markings) might present a barrier for testing and operation in some states. Additionally, minor roads are often the responsibility of local governments. Though the MUTCD applies to all public roads, including local roads, MUTCD compliance on local roads may not be effectively enforced, which presents additional challenges for CAVs (Canis, 2021).

The U.S. Congress sought to encourage the research and development of infrastructure to accommodate CAVs in a 2019 surface transportation reauthorization bill (S. 2302, America's Transportation Infrastructure Act of 2019). The bill was never voted on by the entire Senate and did not become law (Canis, 2021). However, the recently enacted P.L. 117-58, Infrastructure Investment and Jobs Act (Bipartisan Infrastructure Bill) includes several provisions authorizing research into CAVs:

- *Section 11504, Study of Impacts on Roads from Self-Driving Vehicles*—authorizes a study on the existing and future impacts of self-driving vehicles to transportation infrastructure, mobility, the environment and safety, including impacts on (a) the Interstate System, (b) urban roads, (c) rural roads, (d) corridors with heavy traffic congestion, (e) transportation systems optimization, and (f) any other areas or issues relevant to Federal Highway Administration operations.
- *Section 13005, Emerging Technology Research Pilot Program*—creates a new pilot program to conduct research and development in areas including (i) reducing the impact of automated and connected driving systems and advanced driver assistance systems on pavement and infrastructure performance and (ii) improving transportation infrastructure design in anticipation of increased usage of automated driving systems and advanced driver assistance systems.
- *Section 13006, Research and Technology Development and Deployment*—creates a Center of Excellence on New Mobility and Automated Vehicles to collect, conduct, and fund research on the impacts of new mobility and highly automated vehicles on land use, urban design, transportation, real estate, equity, and municipal budgets.
- *Section 25005, Strengthening Mobility and Revolutionizing Transportation Grant Program*—authorizes the creation of a new grant program at $100 million annually for demonstration projects focused on advanced smart city or community technologies and systems to improve transportation efficiency and safety. Grant funds may be used for intelligent, sensor-based infrastructure, systems integration, and smart technology traffic signals.

Vehicle Safety Certification

The TTI research team identified documents that defined or explained how states manage safety standards of fleets and other state-owned vehicles in the absence of federal safety standards. Of the documents reviewed, none addressed the topic of how states should manage fleet safety standards in the absence of federal regulations. Most, however, referred to NHTSA's authority in this area.

Glancy et al., in *A Look at the Legal Environment for Driverless Vehicles—Part 2*, note that "minimum safety standards for vehicles are set by NHTSA, which preempt any less exacting standards on vehicles from states" (Glancy D. P., 2016). Thus, it is unclear what authority states have in setting their own vehicle safety standards should they choose to operate fleets of CAVs.

Nevertheless, in 2021, the Texas State Legislature successfully sought to create its own motor vehicle safety standards for a subset of automated motor vehicles and automated driving systems in HB 3026. The bill amended the Texas Transportation Code to exempt "automated motor vehicles" from state motor vehicle equipment laws and regulations that support human operation of vehicles or are not relevant to automated driving systems, as well as vehicle safety inspections.

Terms and Definitions

The TTI research team discovered 30 documents in the literature review that defined or explained terminology such as ADS, decision support systems, ADAS, driver, owner, and operator.

Either by expressly advising clarity of statutory definition or by reporting the wide variety of CAV definitions adopted by different states, the literature indicates that clarity of terms and definitions is the first priority

states should address in enabling CAV operation on public roads. Volumes 4 and 5 of *Implications of Connected and Automated Driving Systems: Autonomous Vehicle Action Plan* by Trimble et al. (Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 5: Developing the Autonomous Vehicle Action Plan, 2018; Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 4: Autonomous Vehicle Action Plan, 2018) include a comment on their own research that reveals this common concern of different stakeholder groups regardless of their choice of definition:

> While there were divergent views between public agencies and industry representatives on what the right list of modifications to law should be, there was one common thread throughout all input and current actions: the need for clear and consistent definitions.

Key terms that Trimble et al. report should be defined or modified include:

- "Driver."
- "Operator."
- "Drive."
- "Operate."
- "Autonomous" or "automated" vehicle.
- "A codification of the ADS-equipped vehicle levels based on SAE J3016 definitions" (Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 3: Legal Modification Prioritization and Harmonization Analysis, 2018).

This recommendation, supported by a similar list of terms, is echoed in the other documents under review for this topic, citing at least two main reasons:

- Within any given state, terms that refer to human-driven vehicle operations such as "drive," "driver," "due care," and "operator" can appear hundreds if not thousands of times "in a single state legislative motor vehicle code and form the underpinnings of much of the code's legal applicability and jurisdictional reach" (Trimble T. W.-O., Implications of Connected and Automated Driving Systems, Vol. 5: Developing the Autonomous Vehicle Action Plan, 2018). Without some form of clarification, new CAV technologies can continue to be essentially non-existent under the law and therefore very difficult to regulate. This leaves agencies like state DOTs lacking clarity as to their jurisdiction and duty regarding those activities that are described in the terms that are in need of modification.
- Focusing on clear definitions for new technologies is important in that where those definitions differ from state to state, technology developers and manufacturers are forced to comply with 50 different state codes when designing and manufacturing their vehicles. This results in the current patchwork of state laws that keep developers hamstrung about where they may legally test or operate. Federal uniformity of law would help to streamline this issue.

On the latter point, Canis, in *Issues in Autonomous Vehicle Testing and Deployment*, notes that USDOT is seeking to redefine the terms "driver" and "operator" to reflect that humans are not always in control of the vehicle (Canis, 2021). In fact, NHTSA, in its *Standing General Order on Crash Reporting for Levels of Driving Automation 2–5*, offers a definition of "operator" that is associated with ADS, providing that "'operator' means the entity operating a motor vehicle equipped with ADS on a publicly accessible road. An operator may also be a manufacturer" (U.S. Department of Transportation, 2021).

The Texas State Legislature codified CAV-specific definitions in SB 2205 from Legislative Session 85(R), authorizing CAV operation on public roads. The bill, effective on September 1, 2017, amended the Texas Transportation Code to, among other things, place responsibility on the owner of an automated motor vehicle for compliance with traffic and motor vehicle laws, allow automated motor vehicles to operate without a human operator in the state, and prohibit automated motor vehicles from operating if they are incapable of operating in compliance with state traffic and motor vehicle laws. The bill also provides the following definitions:

- "Automated driving system" means hardware and software that, when installed on a motor vehicle and engaged, are collectively capable of performing, without any intervention or supervision by a human operator: (a) all aspects of the entire dynamic driving task for the vehicle on a sustained basis and (b) any fallback maneuvers necessary to respond to a failure of the system.
- "Automated motor vehicle" means a motor vehicle on which an automated driving system is installed.
- "Entire dynamic driving task" means the operational and tactical aspects of operating a vehicle. The term: (a) includes: (i) operational aspects, including steering, braking, accelerating, and monitoring the vehicle and the roadway; and (ii) tactical aspects, including responding to events, determining when to change lanes, turning, using signals, and other related actions; and (b) does not include strategic aspects, including determining destinations or waypoints.
- "Human operator" means a natural person in an automated motor vehicle who controls the entire dynamic driving task.
- "Owner" is "a person who: (A) holds the legal title of a vehicle; (B) has the legal right of possession of a vehicle; or (C) has the legal right of control of a vehicle."

Still, the existing law could go further to provide clear definitions, especially as certain definitions become outdated. Other states or the federal government may provide alternatives to consider for adoption in Texas to better protect TxDOT from future CAV liability.

Insurance

Of the documents examined for this literature review, none expressly addressed state agency liability with regard to CAVs in terms of workers' compensation or caps on state liability amounts. Nonetheless, 23 documents addressed this topic in general and provided useful information for consideration. Like other topics under review, insurance schemes and limits are typically beyond a state DOT's authority and control. However, TxDOT can identify models elsewhere that could potentially shield the agency from liability and recommend favorable proposals with policymakers.

Existing Texas State Liability

Texas Tort Claims Act Basics outlines existing maximum damage limits on liability for Texas governmental units, including state and local governments and municipalities, where sovereign immunity has been waived. These amounts provide a baseline for what the state has, up until now, been expected to cover.

For state government, liability is limited to money damages in a maximum amount of:

- $250,000 for each person.
- $500,000 for each single occurrence of bodily injury or death.
- $100,000 for each single occurrence of injury to or destruction of property (Evans, 2014).

State and Federal Roles in Regulating Insurance

In *A Look at the Legal Environment for Driverless Vehicles—Part 2,* Glancy et al. note that the Commerce Clause of the U.S. Constitution empowers the federal government to regulate insurance, an authority which has been delegated to the states. After Congress ceded that regulation in 1945 (through the McCarran-Ferguson Act), the few federal acts concerning insurance have involved transportation (Glancy D. P., 2016). This suggests that the federal government could reclaim its regulation of insurance should a federal insurance scheme prove to be a desirable strategy.

A number of documents from USDOT and NHTSA confirm that, at the moment, insurance is and should remain a state responsibility. In *Preparing for the Future of Transportation: Automated Vehicle*s, USDOT tasks states with developing and regulating liability and insurance policies for ADSs (U.S. Department of Transportation, 2018). Canis, writing for Congress, notes that NHTSA developed a model state policy with the American Association of Motor Vehicle Administrators, which suggested state roles and procedures with respect to CAVs, including regulation of motor vehicle liability and insurance (Canis, 2021). That model policy stipulated an insurance minimum of $5 million (Stamatiadis, 2018).

In *Beyond Speculation 2.0: An Update to Eno's Action Plan for Federal, State, and Local Policymakers*, Lewis and Grossman suggest that states could impose shared liability schemes so that all parties involved in a CAV crash—including operators, owners, passengers, manufacturers, and other entities—might be liable. They also recommend that federal regulators create a standard for human-machine interface and responsibility to ensure clarity in liability for vehicle operations (Lewis P. a., 2019).

Uncertain Futures

Removing human error from the CAV driving experience may decrease the risk of damage from impaired or distracted driving. In *Autonomous Vehicle Technology: A Guide for Policymakers*, Anderson et al. assert that in a future where CAVs reduce human-caused harm, they will reduce crash rates significantly, making auto insurance unnecessary. Health insurance could cover the costs of injuries from car crashes in the way that bicycle injuries are covered today. In fact, the authors postulate, as AV technology improves, drivers may not be liable at all, and the model of no-fault insurance may make more sense (Anderson, 2016).

Similarly, Zmud et al., in *Strategies to Advance Automated and Connected Vehicles: Briefing Document*, note that high tort liability limits could discourage and slow the adoption of CAVs. However, no-fault insurance schemes could reduce or eliminate tort liability for manufacturers, thus allowing a less fettered development of the technology (Zmud, 2017).

If CAVs reduce the number of human-caused vehicle crashes, they may also present new dangers, namely criminal hacking or system failures. Either of these scenarios could result in mass harms that are not anticipated and could not be handled by current insurance limits. A British model, described in *The Liability for Cybersecurity Breaches of Connected and Autonomous Vehicles* by Channon et al., addresses ways to manage hacking-based harms with either a purely public guarantee fund (modeled after an existing plan) or a public/private arrangement between the government and the CAV industry (Channon, 2021).

System failure is another potential risk in a connected future. TRB workshop participants at the *TRB Forum on Preparing for Automated Vehicles and Shared Mobility Mini-Workshop on the Importance and Role of Connectivity* noted that:

> There is significant fear, in both the public and the private sector, regarding the liability of a failure in connectivity. Failures might include a complete breakdown in the connectivity or the speed being too slow, resulting in injury or death. Even if the technology works perfectly, approximately one-third of all crashes involve driver impairment, and impaired drivers cannot be expected to be able to react to the alerts provided by a vehicle (Kortum, 2019).

This type of connectivity, especially if owned and operated by a public-private partnership, may require a different legislative and regulatory framework than exists today (Kortum, 2019).

State Legislative Action

In a 2018 review of state legislative action addressing CAV technology, *Automated Vehicle Legislative Issues*, Hubbard notes that, as of 2017, Texas explicitly requires that AVs carry the same insurance coverage as other vehicles. The State of Michigan has taken steps to address several aspects of insurance related to CAVs, including:

a. requir[ing] proof of insurance before conducting testing on a roadway without a human operator;

b. requir[ing] insurance for the manufacturer of the automated technology;

c. address[ing] AV liability for upfitters when third parties provide conversions;

d. [addressing liability] for mechanics and auto repair providers;

e. [addressing liability] for manufacturers when changes are made without their consent;

f. [addressing] liability for auto manufacturers who have AV fleets for ridesharing in a SAVE project (23), specifying that the manufacturer must have $10 million in liability insurance and shall be liable when the ADS is at fault (Hubbard, 2018).

Conclusion

Even as federal law or regulation concerning CAVs has yet to be codified, state DOTs cannot assume that the current legal framework between federal law and human-driven vehicles will remain relevant for CAVs. State DOTs could benefit from proactive efforts to codify definitions and liability approaches, which provide clear language and set forward the mechanisms for further action down the road without prescribing specifics on technology features that could become outdated or cause more confusion as CAV technology develops. State DOTs could also review the current processes for infrastructure design, notice of changes, and data handling to determine any current or potential gaps that may become larger issues with the arrival of CAVs. Due to the many unknowns around CAV operations, infrastructure requirements, and user adoption, continuing to collaborate with manufacturers and developers of CAVs around pilot projects appears prudent to inform data-driven decision-making.

3. Stakeholder Interviews

For the stakeholder interviews, the TTI research team collected feedback from 14 practitioners in transportation law, industry, research, planning, and engineering. The stakeholders that met with the research team reflected a diverse set of opinions and perspectives about CAVs, representing the broad scope and interests of the project to identify potential liabilities and mitigation techniques.

Methodology

To begin the task, the research team first identified broad stakeholder categories, including cities, state transportation agencies, academia, law firms, toll authorities, metropolitan planning organizations, private industry, federal government, state legislatures, and legal and professional organizations or consulting firms. Next, the team generated a list of proposed interviewees. In total, 37 individuals were identified as potential interviewees.

In consultation with TxDOT, the research team narrowed the list of interviewees to 18 individuals from 15 organizations, classified into the following categories of role or organization type:

- Attorneys (7).
  - Practicing (4).
- Legal organizations (2).
  - Law firm.
  - Professional association.
- Governmental/transportation organizations (8).
  - Municipal transportation or planning agency.
  - State transportation agency.
  - Regional metropolitan planning organization.
  - Tolling authority.
- Transportation trade associations (2).
  - Technology.
  - Shared use.
- Private-sector autonomous freight provider (1).

In preparation for the interviews, the team developed:

- A standardized interview guide, which included a common set of questions to help ensure a comparable set of outcomes and value statements from the interviews. The interview guide ensured consistency and provided an overall structure to the interviews but allowed flexibility to focus on the practical expertise and experience of the interviewees.
- A PowerPoint slide deck to guide the discussions. The document was sent to the interviewees ahead of the interviews as background to help them prepare for the conversations and in case the stakeholder wanted to provide information to the project team in advance.

For each scheduled interview, members of the TTI research team connected with interviewees via an online engagement platform and discussed the topics of the project for approximately 60 minutes. Each scheduled call was led by one team member while another team member served as a designated notetaker; for some calls, additional project team members joined to observe or participate in the discussion.

The agenda for the interviews generally followed this order:

- Introductions.
- Project background (project overview and literature review findings).
- Interview questions.
- Closing.

During the introductions, the interviewees were notified that:

- The interview would be recorded but not transcribed.
- Statements said by the interviewees would not be attributed to them personally in the technical memorandum deliverable or other project deliverables.

The interviews were conducted between March 3, 2022, and April 8, 2022.

Findings

The stakeholder interviews revealed what potential tort liabilities exist for state DOTs and other governmental units from CAV technologies, and the mitigation techniques for addressing or responding to those liabilities. Generally, the TTI research team found that:

- Existing state law in Texas provides sovereign immunity to state agencies and local governments and caps on economic damage for tort claims, which are favorable in limiting potential liabilities from CAV technologies.
- CAVs are being deployed by private companies on public roadways to operate on roadways as they are currently designed, constructed, and maintained. Private CAV manufacturers do not wish to depend on government to operationalize their vehicles and are not seeking special accommodations (e.g., dedicated lanes or other CAV-specific infrastructure) for their vehicles.
- In more permissive states like Texas, CAVs may be deployed by private companies without the state or local government's knowledge. However, some have formed partnerships with municipalities that are governed by memoranda of understanding or other types of agreements to document expectations and responsibilities between the parties.
- Public agencies are subject to open records/public information act (PIA) laws, but private companies are not. Thus, private companies are and will continue to be wary of partnering with governmental units unless they formalize mechanisms to protect certain information from disclosure.
- CAVs will potentially give rise to more data regarding infrastructure condition and defects than governmental units currently manage, so agencies will need to consider how the data will be communicated to them and how they will warn CAVs of the defect or make the condition reasonably safe.
- State DOTs and local governments should not view information about roadway conditions generated from CAV data as different from current information channels and processes, and should not require a separate

legal regime for CAV data on infrastructure condition. Instead, state DOTs and local governments should anticipate receiving more but better information about roadway conditions that will help prioritize repair work more efficiently.

- Transportation agencies that provide data or products that CAV manufacturers can obtain and use will potentially expose themselves to additional liability. To mitigate this potential liability, agencies may need to provide a user agreement or a warning that clearly states that the information may not be accurate or may be limited in other ways.
- Lawsuits involving CAVs will likely be tried under products liability theories and lead to a long evolution in case law. In most states, products liability and rules of the road are handled similarly but differ with respect to caps on economic damages. State statutes that cap damages can disincentivize lawsuits because of the limited potential return. Where caps do not exist in state statute, the opposite is true, and plaintiffs may be more inclined to bring suit.

Stakeholder Experiences with CAVs

To gather context from the interviewees prior to asking more substantive questions, the TTI research team first asked interviewees to describe their experiences with CAV technology. The level of CAV experience of the stakeholder group is deep in the realms of testing or trial deployment or transportation law, policy, and regulation, with many having long careers in government, the private sector, as lawyers, or as engineers. The TTI research team has summarized the experiences of the interviewees below.

Municipal and state transportation officials and infrastructure operators had direct involvement with pilot projects or trial operations of CAVs of various levels including:

- Passenger service.
- Personal delivery devices.
- Transit signal priority with buses and snowplows.
- Dual-mode technology (receiving and sending information).
- Truck platooning.
- Several low-speed automated vehicle pilot projects, including an ongoing series of pilots in one municipality that began with a non-auto-grade vehicle operating in a fully off-street environment. The project then moved to a second stage using retrofitted auto-grade vehicles on a low-speed circulator route and is currently piloting AVs in a mixed traffic environment though a ride-hailing platform.
- CV technologies using dedicated short-range communications (DSRC) (not involving AVs) to communicate information to onboard units in automobiles and transit vehicles from roadside units. In these limited deployments, the system transmits CV information, including wrong-way entry warning, wrong-way vehicle warning, deceleration alerts, red-light warning, and pedestrian crossing alerts. This work is credited with stopping 14 wrong-way-traveling vehicles from entering interstate ramps in an 18-month period.

State-level officials also had experience in working with their state legislatures, within their departments, or with other external partners in facilitating CAV development by:

- Setting up start-up testing labs.
- Establishing intelligent transportation system (ITS) teams for technologies like dynamic messaging and roadside information.
- Developing partnerships with original equipment manufacturers (OEMs) of CAVs.
- Organizing peer exchanges.
- Managing internal DOT programs on cooperative automated transportation with shared mobility options.
- Working as a liaison between different teams within the state DOT.
- Partnering with a state university's law school on research into AV policy regulations.
- Serving on the AV task force in the state's transportation division and multiple committees/organizations in the space.

Lawyers working in government and regulatory environments had experience practicing at USDOT, the Federal Transit Administration (FTA), and a state DOT. They are working on matters ranging from safety to technology development and disparities in transportation investments. Other positions where lawyers practiced transportation law or advised on transportation policy and regulation include overseeing CAV projects for a regional governmental unit, managing a major urban Taxi and Limousine Commission focusing on tort claims and liability structure, and presiding over an international regulatory body developing model licensing regulations. Private-sector stakeholders work in policy and possess experience at USDOT and serving on the working group for the Association for Unmanned Vehicle Systems International.

Lawyers working in special interest groups and trade associations work to promote technological and shared mobility solutions, including supporting FTA Accelerating Innovative Mobility Initiative projects in several states that focus on AVs. Others advocate for plaintiffs' attorneys at a national level.

Interviewees with tort law experience practiced for many years in private practice in four states (including Texas and California) on the plaintiff's side on automobile products liability lawsuits. These interviewees have worked on cases that raised the minimum strength standard of vehicle roofs (to enhance safety in cases of vehicle rollovers), defended a state DOT on torts related to public roadways, and handled matters of employment, contracts, construction, and intellectual property.

Private-sector technology stakeholders that were interviewed for this project are involved in the development of automated trucking solutions. The companies they work for are deploying Level 2 systems (see Figure 1) that can serve as the foundation for higher levels of vehicular automation and future collaboration between technologists and transportation agencies.

Response to Literature Review Findings

As a lead-in to the substantive interview questions, stakeholder interviewees were asked to respond to the project's literature review findings. Overall, interviewees agreed with the findings, considering them comprehensive and accurately describing the state of play at the moment. Many interviewees offered points of clarification or minor disagreement, noting that:

- The federal government should retain oversight over safety. Since 1956, the federal government has set minimum standards and should continue to do so.

- The findings on state products liability accurately describe how state products liability law should continue to govern tort liability matters for defective design, manufacture, and instruction.
- States should determine definitions for tort law and immunities.
- State DOTs may be liable for negligent operation of vehicles owned by the state DOT under the motor vehicle exception to governmental immunity for tort liability. But if the state DOT is not operating the vehicle, either in-car or remotely, the DOT should be spared from liability for the behavior of an autonomous vehicle.
- It is unclear why liability for CAVs would be any different from existing liability for traffic signals and information. The only thing changing is the driver; the question will be how states define the "driver," and who will be enforcing that definition.
- There is an assumption that the new FMVSS for CAVs from NHTSA will be comprehensive, but that is still an unknown.

CAV Technology Implementation Issues

Legal challenges and questions around CAV implementation for stakeholders clustered around several topics, including:

- False marketing and unclear messaging about levels of automation in consumer vehicles.
- Vehicle safety certification.
- How much communication takes place between a state transportation agency and an OEM.
- Data management.
- Duty of care in infrastructure design and maintenance.
- Governmental safety measures to prevent liability.

Uncertainty around Levels of Automation

A number of complex discussions centered around the current uncertainty of AV capabilities. First, several interviewees mentioned that the misleading advertising (e.g., Tesla's "Full Self-Driving Capability" technology) around consumer vehicles is cause for concern. These comments came from representatives of state DOTs and practicing transportation attorneys who noted that ADAS technologies have led to driver disengagement and overreliance on the vehicle to self-drive, causing dangerous crashes. To prevent this, vehicle levels of automation need to be well defined by OEMs and communicated to purchasers/drivers. Toward this end, NHTSA has focused new efforts to clarify automation levels with a new media campaign designed to provide updated descriptions for existing and planned levels of automation. For example, the campaign describes Levels 1 and 2 as "assistive" and attaches the phrase "You drive, you monitor" to these levels.

Effect of Vehicle Automation on Government Liability

Interviewees' opinions differed on the question of whether a CAV's capabilities change government liability. A practicing products liability attorney noted that AVs "see" what is around them on the road (e.g., markings, signage, other traffic control devices, and other vehicles) and act accordingly. AVs are not going to rely on any more additional communication from the road infrastructure than ordinary human drivers do. It follows, then, that if the AV OEM has taken over the role of the driver, an error made by the vehicle would be the OEM's responsibility (unless some other party has taken over programming the vehicle).

So far, most OEMs are not challenging this responsibility, although AV technologies have still not reached the capability of human drivers in terms of visual perception, decision-making, and reaction time. State DOT officials noted that at Level 4 automation (where humans will not be required for the vehicle to operate autonomously within identified operational domains), case law will be necessary to prove whether OEMs will take on that liability. For this reason, the state DOT interviewees stated that Level 3 automation (conditional driving automation where ADAS and artificial intelligence will make driving decisions but a human driver will still be required to control the vehicle) may be skipped. Although conceptually possible, having a human and vehicle responsible for vehicle operations at the same time muddies the issue of who or what is responsible for the driving task. This issue is further complicated by questions about whether a Level 4 vehicle will drop to Level 3 when it leaves its fully autonomous operating area. It is possible that humans and vehicles may be sharing the driving task even in Level 4 vehicles. Given that Level 5 vehicles may not deploy for a very long time, this human-vehicle collaboration is one possible reality that states may have to contend with after all.

Interviewees representing state DOTs also commented that OEMs are designing ADAS in AVs to replicate the sensory functions of humans, but that currently there are skills which human drivers are better suited for such as identifying lanes with eroded striping. A concern about this reliance on technology to be functional with the current state of infrastructure is that today's road design standards, as reflected in documents such as the *Manual on Uniform Traffic Control Device*s and American Association of State Highway and Transportation Officials (AASHTO) *Green Book*, are based on human drivers, accounting for human perception, reaction time, and predictable mistakes.

Interviewees noted that at higher levels of automation (Levels 4 and 5), there may be more potential state and local government liability, particularly if state-owned or -operated connected infrastructure that provides reliable connectivity and information is also needed for safe operations. At lower levels, liability is likely to exist more in the realm of products liability (i.e., OEM and component/software manufacturer liability). At higher automation levels, AVs may rely heavily on roadway markings (e.g., clear, wide striping) that are the jurisdiction of transportation agencies. However, in the meantime, state DOT interviewees noted that they do not intend or plan to build infrastructure to OEMs' specifications. Dedicated AV lanes would not be feasible. Instead, OEMs will need to build their systems to work with the existing infrastructure currently shared with conventional vehicles.

CVs and the Spectrum

Public entities engaged with CV programs noted the November 2020 decision by the Federal Communications Commission (FCC) to reconfigure the 5.9-gigahertz spectrum band previously allocated for ITS and DSRC vehicle safety technologies to share with unlicensed uses (e.g., Wi-Fi). FCC assigned a significant portion exclusively to cellular vehicle-to-everything (C-V2X) safety technologies, which the agency selected as the U.S. standard for vehicle safety technologies. FCC also eliminated spectrum for DSRC use altogether. Because of this, interviewees were of the opinion that there is now less of an interest in investing in CV technologies and installing onboard units in vehicles on the roadway. Without a dedicated transportation safety band in the spectrum, the risk of traffic incidents may increase as deployment of ITS and other safety-focused technologies decreases.

A private-sector interviewee noted that this may be a moot issue. The interviewee said that the lack of a CV infrastructure mandate may not be an issue for CAVs. CV infrastructure has not proven to be safer, according to this stakeholder, leading prior attempts at a mandate to fail because its benefits could not be proven in a quantifiable way. In addition, existing technologies (e.g., Waze) already do the job of a roadside unit but are often better at it. Companies are not in need of roadside units, with currently available smartphone data proving to be better anyway.

Safety Drivers in Municipal Pilots

One stakeholder from a municipality with comparatively more experience than most noted that the city has always had a human safety operator on board in every AV pilot deployment. In earlier, low-speed pilots, these operators were mostly for assurance, providing riders a level of comfort with the new technology. Operators in the current pilot are more proactive, taking over the vehicle in complex environments (e.g., unprotected turns, double-blocked cars, or pedestrian activity). Drivers currently take over for the vehicle based on their own interpretation of the environment and warnings from the system. For example, the vehicle will alert the operator when it cannot proceed. Currently, vehicles in the pilot projects are running at roughly 80 percent autonomy. The pilot projects will require a safety driver in all testing until the technology is proven. This trend is appearing in California as well; the California Public Utilities Commission recently issued permits to General Motors' Cruise and Alphabet's Waymo for "drivered deployment" ride-hailing services. The companies are authorized to collect passenger fares and offer shared rides as long as a safety driver is present in the vehicle.

Governmental Barriers to Implementation

Stakeholders also mentioned needed changes to existing governmental practices and processes to CAV implementation, including:

- Traditional procurement rules and insurance requirements are either onerous or not applicable to AVs, acting as barriers to transit agencies and government entities looking to implement AVs.
- Governmental agencies should consider simplifying their processes for adopting new technologies. One stakeholder noted that their state agency needed to focus on just a few use cases (not several) that can prove viable in order to advance CAV exploration. Traditional governmental decision-making often involves many stakeholders and requires agreement between them, which is time consuming and dampens innovation in transportation. Interviewees noted that CAVs will likely be deployed in non-democratic countries first because their representative decision-making processes are not as unwieldy as that in the United States.
- There are tremendous legal questions on CAV certifications due to the current lack of federal standards. These protocols fall outside the current expertise and responsibility of individual states, leaving them at a loss about how to regulate vehicle safety.
- State DOTs will need to shift culturally to adapt to the coming technological environment. They will have to take more risks as more is asked of them due to developments in the industry. State DOTs must also, as public servants, serve community members, which will require increased coordination and collaboration with local governments.

Potential Tort Liabilities

Texas Tort Limitations

Lawyers and municipal transportation agency representatives with knowledge of Texas law noted two relevant statutes:

- The Texas Tort Claims Act's limited immunity for state agencies and other governmental units.
- Texas law governing AVs (namely, Texas Transportation Code Ann. Chapter 545, Subchapter J Automated Motor Vehicle Operation [§§ 545.451-545.456]).

On the issue of ownership, interviewees provided that Texas state law makes the owner responsible for the vehicle. So, if a state or local government owns a vehicle, then harm caused by operation or use of the vehicle would make the government liable by waiver of its immunity.

Interviewees noted that if TxDOT owns AVs, any claims arising from their operation would work similarly to the current procedure and be decided based on questions of who owned or programmed the vehicle. Regarding notice to cure infrastructure defects, existing Texas tort claims law provides a reasonable amount of time for addressing known issues in infrastructure. The existing law applies so long as existing processes for notification and notice are in place. In addition, interviewees noted that OEMs and AV operators bear responsibility for driving prudently and at reasonable speeds on all roadways, including those in poor condition. This could relieve the state or local government from some portion of liability for poor road conditions that might arguably contribute to any harm suffered.

With regard to notice of infrastructure defects in Texas, considering the Texas Tort Claims Act's existing insurance cap and coverage of local and state governmental units under governmental and sovereign immunity, respectively, TxDOT and local or regional transportation agencies would be sufficiently protected from AV operator claims arising from harm caused by infrastructure design or device installation. (This protection would likely not apply to claims arising from harms caused by dangerous roadway conditions due to a lack of maintenance.) This is significant because, among other states, governmental or sovereign immunity is the exception and not the rule.

Interviewees from outside Texas provided that in states with joint and several liability and no sovereign immunity, government agencies have high exposure to claims. When these states are sued on a matter related to road condition, the legal inquiry involves determining whether standards exist, whether the standards were followed, and whether there were material changes to the roadway from those standards. If these requirements are satisfied, the state typically has a strong defense and some insulation from liability. Thus, AV technology OEMs could potentially sue states on the basis of defective infrastructure if the AV was following the same rules as human drivers and the infrastructure failed to meet standards designed for human driving.

In most states, products liability and rules of the road are handled similarly but differ with respect to caps on economic damages. In certain situations, caps have a chilling effect on plaintiffs' lawsuits because of the limited potential return. In others where caps do not exist in state statute, such lawsuits have the opposite effect.

In certain municipal AV ride-hailing pilot programs, liability is shifted in part to users who opt in to use an AV on the ride-hailing platform through consent granted from user agreements. AVs are available in addition to standard vehicles if their ride meets eligibility requirements.

Risk Exposure and Innovation

Transportation agencies could acquire additional responsibilities—and therefore liabilities—if the agencies provide data or other information or products to CAV manufacturers (e.g., work zone or road closure data). In doing so, transportation agencies would have to provide the data, information, or product non-negligibly along with a duty of care. This means that the agencies will need to warn the users that the data are not guaranteed to be accurate but can be used for planning purposes and not for operational purposes. The agencies will need to clearly warn the users of limitations of use of the data.

This should not deter transportation agencies from providing data, information, or other products for use by CAVs. Tort liability is important and justified as a deterrent to potentially negligent acts, preventing individual and collective harms. However, as interviewees provided, governmental units' goal should be to fix issues rather than to avoid liability. In other words, whatever the existing law, transportation agencies should consider the policies they favor and weigh them against their risk tolerance. Governmental units that have undertaken CAV pilot projects are not generally concerned about potential tort liabilities.

Interviewees noted that the discussion of tort liability of CAV technologies should be centered on community engagement; otherwise, public agencies are missing the mark on innovation. There is value in rethinking the relationship to risk in that some risk is tolerable and good for fostering innovation. Transportation agencies should guard against an "ostrich approach" and avoid innovation for fear of potential liability.

Infrastructure for CAVs

On the question of whether DOTs will be held to different design standards for CAVs, interviewees offered the following opinions:

- Though it is possible that a transportation agency may be exposed to liability on roadways that present a dangerous condition for AVs to operate, there would likely not be any excess liability for accidents involving AVs than currently with vehicles driven by humans.
- Though it has been eroded somewhat by the courts, design immunity is still important because in cases where both the transportation agency and the OEM are sued, the plaintiff will claim that the transportation agency did not design, construct, or maintain the roadway in accordance with relevant design or maintenance standards.
- The existing products liability frameworks of states could probably handle liability claims for AVs (under negligence or negligence per se) but are not optimal.
- Today's transportation agencies are not thinking differently about liability with AVs or CVs for things like potholes or pavement markings, which they will continue to maintain and repair. Those agencies that have moved to wider striping or other changes have done so because it is safer for human drivers.
- CV technologies need more space on the communications spectrum than what is currently available, which could pose liability risks.

- OEMs will not specify the infrastructure they need for fear of overregulation from the government and disclosure of information from PIA laws. In fact, AV manufacturers are working to have their AVs operate on any road as they are currently designed, constructed, operated, and maintained. OEMs want their vehicles to test and operate in the present environment without the need for additional infrastructure.

Liability of the CAV "Driver"

Currently, liability is exchanged between vehicle manufacturers and the human driver. The liability landscape is changing with regard to the vehicle driver. Interviewees provided that when the driver is no longer a human but the AV, liability should be transferred to the AV manufacturer because it has the greatest understanding of the vehicle. As long as transportation agencies are not operating the CAVs, either in-car or remotely, the agencies should be spared from liability.

In Florida and Nevada, companies are lobbying for "automated vehicle network company" definitions, which would clarify the legal identity of such companies, an identity which may not currently exist. In other states besides Texas, AVs are already treated as drivers in their current statutes, clearly stating that the vehicle system is responsible for complying with rules of the road. In other states, the driver is still assumed to be human, and there is still work to be done to correct existing laws dealing with non-human drivers of CAVs. This includes bills trying to place increased scrutiny on marketing strategies and the language of vehicle manufacturers so that consumers better understand the vehicles they purchase and their AV limitations (i.e., that they are not fully autonomous).

Interviewees noted that lawsuits involving CAVs will likely end up claiming products liability and leading to a long evolution in case law. Even where OEMs are challenged in criminal court with vehicular manslaughter charges for AVs that crash into and kill other roadway users, OEMs may be sued civilly under products liability claims. However, because most AV companies involved in lawsuits will likely settle so as not to have any information disclosed by courts, case law will not offer much guidance about what to expect in the near future. AV OEMs are already reaching settlements very quickly, so the findings from these cases have not been made public. The implication of this is that existing law will likely not be shaped or changed by these lawsuits.

Limiting Liability through CAV Permitting

AV pilots in Texas are being conducted through traditional government procedures with contract requirements determining liability for these projects. Contracts may have the public and private partners share in liability, with different partners bringing different levels of insurance depending on their roles. Or, if contracts are structured like purchase agreements, liability may be solely placed on the AV operators and have defined notification procedures and responsibilities in the event of safety incidents. Traditional government procurement, however, can hamper innovation. Still, if a state DOT or local government wishes to pursue innovation through traditional procurement, interviewees advise that the agency examine its current contracting templates and determine what needs to be included, such as insurance and data-reporting requirements, which need restructuring in most places.

In certain states, the motor vehicle agency has the authority to issue licenses to CAV OEMs. The license binds the OEMs to certain obligations, including requirements that a person be on board the vehicle, OEM reporting of disengagements by the human driver, and OEM reporting of crash data. In these states, a work-around to

permitting and licensing requirements is establishment on CAV testing grounds, where OEMs can test their vehicles on closed roadways in exchange for data.

For the most part, AVs may be deployed in Texas without the local or state government of jurisdiction knowing of the deployment. Today, government entities in Texas do not have authority to issue permits or licenses for AV testing or operation, nor are OEMs required to test or operate AVs in Texas with a permit or license. This makes matters clearer in that there is no liability to a government unit that has no knowledge of AVs operating within its jurisdiction on its roadways. Interviewees noted that contractual arrangements between a local government and an AV manufacturer would not override state law; existing state statutes on tort liability would still preempt and protect them against most lawsuits.

In other states, lawmakers have passed detailed laws allowing AVs to operate without a permit as long as the vehicle is registered and insured. In other states, the state DOT has identified existing state statutes that could be used to regulate AVs for safety purposes, such as banning vehicles deemed to be unsafe.

Private-sector interviewees provided that it seemed unlikely that states would prohibit ADAS on specific corridors to limit their liability. Most roadways have been constructed or maintained using federal funding in some form, so most roads must comply with federal rules that generally prohibit limitations on vehicle access to federally funded roadways. In any case, the state would need to prove that the roadway is not safe for AVs to justify such a prohibition.

Data

Data on Infrastructure Condition

Currently, infrastructure defects are made known to infrastructure owners through humans who call, email, or otherwise communicate to government officials. A potential problem lies in the presumption that CAV sensors will generate a lot of data regarding infrastructure conditions, defects, and damage, on top of other data related to the vehicles and operators.

Interviewees from local and state governments acknowledged that if vehicle sensor data regarding infrastructure conditions are made available to governmental owners of the infrastructure, the data could come in a form and at a volume and frequency that the agency may not be able to manage or address within a timely manner. In many jurisdictions, repairs cannot be made at the current pace with which complaints are made. If the pace intensifies with CAV data feeds to the repairing agency, the backlog of maintenance requests will only increase. In addition, more data being provided to the government mean an increased possibility of not handling the data properly.

Promisingly, however, recent AV tests in Texas have shown that the type of information being collected from AV trucks and the processing of such information by TxDOT match the kind of information that TxDOT currently receives from the greater public. Thus, TxDOT will process the data in the same way that it processes reports of roadway issues currently received through humans reporting a complaint.

A takeaway from this is that state DOTs and local governments should not view information about roadway conditions generated from CAV data as something alien to current information channels and processes and requiring a separate legal regime. Interviewees noted that they are not interested in a torrent of real-time CAV

data since they would be beyond their bandwidth and expertise to handle. Instead, CAV implementations have focused on receiving data from OEMs and service vendors in an aggregated or analyzed form for performance measurement and program monitoring purposes. Data come in the form of real-time online dashboards, maps, and monthly reports, providing insights into rider and ride characteristics and uses. In this way, transportation agencies receive more but better information (e.g., issue reports accompanied by photos) about roadway conditions that will help them more efficiently prioritize repair work and deploy maintenance crews.

Data Sharing

In states that have required OEMs to operate under a state-issued permit, the permitting agencies and regulators have run into issues from receiving a flow of data (data dumps) that they have not seen before. The information is provided for an intended purpose (e.g., for government officials to understand situations where the AV system is disconnected). However, interviewees from these states noted that the intent of the data could be misconstrued for other purposes, which may translate into a real or perceived liability.

AV pilot projects that have been funded by federal grants are often required to share data and have a data management plan. These projects, such as those funded by FTA, involve a governmental entity partnering with a private partner and the federal agency (e.g., FTA). The projects have required a tiered system for data provision where more data are provided to the federal entity than to the local or state partner or general public.

Data Release

A specific liability concern related to data is the obligation of governments to release information subject to PIA laws. Public records requests have been made and are highly sought after, which has led to caution on all sides. Thus, there has not been much discussion between governments and OEMs on data sharing for CAVs because not much information is willing to be shared by private companies, especially if they perceive the information to be proprietary.

OEMs willing to share data may only do so under a nondisclosure agreement (NDA) with a public partner. However, due to some PIA laws in certain states, many public entities are prohibited from entering into NDAs.

Because PIA laws differ from state to state, AV companies are more willing to share data with public agencies that offer some protection of their proprietary data. In certain states, the law carves out exceptions for state DOT efforts in CAV testing and implementation with respect to data. Interviewees noted that in Texas, private AV partners have gone to the Texas Attorney General and redacted certain information, claiming that it was propriety (including raw trip data from the service and financial details of the pricing structure).

Because of this and other risks, USDOT initiated the Virtual Open Innovation Collaborative Environment for Safety (VOICES) proof-of-concept project. VOICES is a distributed virtual platform that will enable virtual collaboration among participating state and local governments, private companies, and academic institutions. The virtual collaborative environment protects intellectual property while also providing for research and interoperability testing of prototype cooperative driving automation CV applications. VOICES is intended as a virtual sandbox that allows companies and entities to experiment and test together in a safe, realistic, and cost-effective environment.

Relevance of Current Legal Framework

The current legal framework between federal and state law regarding human-driven vehicles has generated ongoing uncertainty with regard to CAV technology. In light of this, interviewees provided insights regarding the current policy and funding framework for CAVs.

All interviewees agreed that safety standards will continue to be governed by NHTSA, which is typically slow to respond to changes in technology because it requires a lot of data before making a decision and is subject to the will of the political administration in office at a given time. In Texas, state law requires all vehicles to be federally compliant; until the FMVSS is revised to account for CAVs, vehicles are only allowed to operate on the state's roadways through an exemption from NHTSA. However, off-street CAV testing does not require a waiver from NHTSA.

Interviewees provided that NHTSA seems to be trending toward stricter standards for CAVs, with a vehicle incident rate of zero for AVs, which may be an unreasonable and impossible target that has not been applied to any other product. Other interviewees noted the opposite, that the FMVSS appears to be heading toward a more hands-off approach to automated trucking and commercial drivers' licenses. However, interviewees noticed a recent change in NHTSA's stance toward AV OEMs that may signal further regulatory action. Interviewees noted NHTSA's March 2022 announcement that AV startup Pony.ai would issue a recall for its vehicles following an October 2021 crash in California. NHTSA said in its statement that this was the first recall of an automated driving system and that NHTSA would "ensure that vehicle manufacturers and developers prioritize safety while they usher in the latest technologies." (Bellen, 2022)

According to some interviewees, the existing legal framework works for a CAV environment and therefore does not need changes. Nothing in the law will need to be different for CAVs since the vehicles still need to be consistent with state laws and standards. If an AV is in a crash because it did not perform as it was supposed to, the fault would go to the OEM as it currently does under products liability. NHTSA would issue a recall for any recurring issues with certain types of AVs the same as it would today for any other type of automobile safety issue.

Interviewees provided that state DOTs will likely continue to wait for federal CAV standards rather than creating their own. In the absence of federal CAV standards, states may decide to work in unison voluntarily. A committee approach with the industry may be helpful, but distrust of private industry may undermine its efforts. Technical assistance systems, such as trainings, professional development, pipeline education, and/or a national guidebook equally accessible to all states and local governments will need to be developed until the federal government provides a new regulatory framework for CAVs. Otherwise, CAVs will be tested and deployed inequitably, with states that have spent their own dollars and are most engaged in CAVs (e.g., Michigan, Maryland, Minnesota, Florida, Maryland, and Virginia) benefiting from advances and investments in vehicle technology more than other states.

Collaboration

Interviewees were asked to share their thoughts on the value of collaboration between governments and OEMs of CAVs in the current legal and regulatory environment, as well as between governmental units. Overall, there

is a need for parties to understand one another and for roles to be clarified, but actual collaboration may not be necessary.

Interviewees advised that state DOTs and local governments collaborate with elected officials and OEMs or suffer the economic and social consequences of being left behind with regard to emerging transportation technologies. Collaboration can take the form of pilot projects, state or local committees on CAV data, informational hearings, stakeholder meetings with legislators, and demonstration projects.

Many interviewees noted that ongoing collaboration between governments and the AV community is unlikely. For the most part, private AV OEMs do not want government bureaucracies involved in the driving task, and government agencies are reluctant to enter into contracts with OEMs. Any collaboration between governments and OEMs is likely to be done through formal rulemaking processes at the federal level. Indeed, lawmaking is viewed by interviewees as the best way to establish clarity of expectations of public and private responsibilities.

Because there is a lot of suspicion in the marketplace between CAV manufacturers and technology companies with respect to data, technology companies are positioning themselves to plug into mobility-as-a-service (MaaS) platforms. MaaS refers to the integration of various forms of transportation services into a single mobility service that is accessible on demand. MaaS can potentially add value to users through a single mobile application that provides access to many mobility options, including CAVs (whether they take the form of transit or ride-hailing vehicles) with a single payment channel instead of multiple ticketing and payment operations. This fragmentation of the private sector related to CAVs presents potential collaboration issues for government agencies looking to support the CAV ecosystem or reacting to private vendors that may be representing manufacturers but not technology companies or vice versa.

Interviewees recommended that with regard to governments providing data in the form of an applicable program interface for use by CAVs, governments should start small and take an incremental approach. Because of the enormous amounts of data that can be gathered and generated by CAVs, state and local government partners may not know what kind of data they should share with OEMs to support CAV deployments. Therefore, state and local agencies should focus first on sharing available data, such as work zone data, and then build from there. Private companies could reciprocate with work zone data from CAV sensors in a form and format that the government agencies could best use. Starting in a narrow, limited way would provide a foundation for building new capacities such as inspection capabilities. CAVs have the potential to support enhanced pre-trip inspections where trucks could be inspected prior to the start of a trip and transmit weight, size, dimension, and other data to law enforcement and inspection stations instead of stopping at weigh stations and other facilities. These trucks could also provide information back to operators about road conditions and interact with first responders.

Interviewees noted that while collaboration may not always be required, there is nevertheless communication between the public and private sectors. Currently, government bodies respond to vendor questions but are generally not engaged with private CAV companies. Ultimately, the vendors are responsible for figuring out where they can safely operate. However, governments are worried about potential inadvertent liability if they do not perform due diligence on an AV OEM that deploys in their state and the company's AV is in a collision. Thus, state DOTs are cautiously monitoring AV deployments in other states as opposed to taking proactive steps to collaborate.

According to interviewees, an important motivation for a company to test and deploy its CAVs in a state is that the state government supports scaling of the business enterprise to become profitable. There must be a legitimate business opportunity to bring people to the table. A committee approach with the industry is helpful for some engagement, but it is possible that not all members of the committee will be versed enough to know whether industry claims are true.

One approach that governments can take is to pursue potential use cases together. A collection of states can pursue use cases through a similar approach (i.e., addressing, codifying, or settling the issue of liability). An example is AASHTO's community of practice with state DOT staff comprised of those who self-identify as having applicable jobs in the industry.

Potential Mitigation Techniques

The stakeholder interviewees shared their thoughts on best practices regarding potential mitigation techniques state and local governments could undertake to prepare for CAV technology deployment.

Vehicles

Interviewees advised that state agencies consider the following measures with regard to CAVs:

- Avoid vehicle certification, licensing of vehicles, or any kind of external or remote control of CAVs. State DOTs may want to be vigilant, however, and take collaborative action with NHTSA or other federal authorities in cases where a vehicle or its software has malfunctioned and collided with an object or otherwise been determined unsafe.
- State DOTs should focus investments on infrastructure improvements that will benefit the human driver. If the investments happen to help CAV systems as well, that is a secondary benefit. In the same way, state DOTs should not make judgments on whether certain roadways are technology safe for CAVs but rather defer to the federal government, which will need to determine which vehicles are safe for ADS and ADAS.
- Because manufacturers are designing CAVs to operate on any existing road, state DOTs should not focus efforts on modifying infrastructure designs for CAVs but rather on broadband, smart work zones, system preservation, and other current needs that will support CAVs whether they are deployed today or years from now.
- State DOTs should make information they already provide (e.g., work zone data, road weather information, and truck parking information) available for CAV use.

Statewide Policy Position

Interviewees provided that statewide policy goals shared among agencies and local jurisdictions are important for success in innovation. Thus, states should proactively determine where they are comfortable in relation to inviting CAVs on their roadways. In this way, states will have to consider where the government should intervene or take a hands-off approach to CAV testing and deployment. Questions to consider when developing a statewide policy position with regard to CAVs include:

- Will the state DOT provide data to OEMs under a franchise model, providing information to certain companies, or instead provide "open data" to anyone who wants to use it?
- Will the state and/or local government provide incentives for ride sharing and equitable access of CAVs?

- Which agency (e.g., the state DOT, motor vehicle agency, public service/utility commission, or law enforcement) will lead with regard to CAVs and serve as the government's public relations messenger that can provide effective messaging to the private sector and public?
- Which project partners or community champions can work well with state and local agencies to communicate with state legislatures?
- Will the state and local agencies be more proactive or more reactive in their approach to CAVs?
- Which business model does the state want to support in the CAV marketplace—free for all, complete control, or a middle ground (e.g., MaaS)?

Risk Mitigation

Interviewees advised state agencies to consider the following measures to mitigate risk of potential tort liabilities from CAV deployments:

- Government agencies will eventually need regulatory authority over CAVs, with their responsibilities written down through state laws and regulations that, among other things, grant access to CAVs and deployment information.
- Governmental insurance policies may need to be adjusted at the legislative level. Insurance wrappers or pools could mitigate potential losses to states caught up in products liability cases. States could also set up claims funds to help protect the public in claims from CAV crashes that might occur.
- States should investigate use cases that consider factors such as liability, economic benefit, business case, testing requirements, and weather, and apply findings to test states' comfort level for risk tolerance. Community engagement can help determine which use cases are the most helpful for states to pursue, as well as the corridors or locations most in need of testing.

Data Handling

Interviewees provided models for state transportation agencies to consider replicating in securely handling CAV data, including:

- *Tolling*—These systems have been generating, using, and managing data associated with vehicle tracking and toll transactions, and using contracts with vendors to handle the data.
- *Snowplows*—In northern states of the United States, these vehicles are exchanging data back and forth with roadside units with CV applications.

Interviewees also advised on the types of data that state DOTs and local governments should or should not handle, including:

- Transportation agencies should provide information using data that can assist the human driver but should avoid providing data directly to CAVs. In this scenario, the drivers themselves are still in control of the cars and are liable for incidents that might occur from acting on that information.
- In-vehicle information such as forward collision warning is better left managed by OEMs.

Mitigating Liability through Clearer Statutory and Contract Language

State DOTs can address potential liabilities from CAV technologies by providing clear language in statutes, policies, contracts, agreements, and procurement documents. In doing so, DOTs should also take measures to prevent being overly prescriptive on CAV technology that could become outdated.

Interviewees noted that state statutes on liability ought to be revamped, including laws related to:

- Insurance, which ought to account for crashes and other injuries involving CAV deployments. This would take the guesswork out of the court system and help with government and industry planning. Interviewees varied in their opinions of who would be liable in a highly automated CAV world, with some asserting that the owner of the vehicle would likely be liable, while others noted that if the OEM has taken over the role of the driver, an error made by the vehicle would be the OEM's responsibility. A determination either way would provide predictability with regard to insurance premiums.
- Authorization of CAV activities consistent with governors' executive orders so that both the state code and executive order are consistent with each other in how terms, such as *driver*, *design immunity*, and *commercial deployment*, are defined, as well as requirements for deployment, including requiring safety drivers.

Contracts and other binding instruments were another area where stakeholders called for increased clarity. In particular, interviewees suggested that state and local governments enter into contracts and agreements where:

- Liability is assigned to the CAV operator to mitigate potential liability from infrastructure defects.
- The governmental party is indemnified by AV companies.
- In CAV pilot partnerships, the private partner is responsible for adding additional terms and conditions to its user agreements to cover the CAV element.
- Memoranda of understanding (or agreements) are used to communicate expectations and responsibilities but not bind the parties in a significant way.

Mitigating Liability through Clearer Bid Document Language

Language in procurement documents should also be examined to mitigate potential liabilities from CAV technologies. Specifically, interviewees recommended that state and local governments take the following actions to foster innovation in a cautious manner:

- Update data security specifications, which should be clearly identified in requests for proposals and other bid documents to protect data and information.
- Use samples and templates for improved procurement document language or processes as well as other resources from trade associations and alliances (e.g., ITS America and the Mobility on Demand Alliance).
- Examine current procurement document templates and determine what needs to be included. To foster innovation, bid documents could potentially follow a simplified template that allows bids to be evaluated and vendors selected within two to three months. This may involve using a prequalified information form and methodology for innovative technologies to meet agency goals.

Notice of Roadway Defects

As provided previously, the potential flood of data from CAVs about roadway defects may strain transportation agencies that do not have the capacity to address them within defined notice periods and may open them up to potential tort liability. To address this, state DOTs can begin by investing in their information technology capabilities and increasing staff capacity and ability to access, analyze, and manage data. Staff could also test and develop protocols for making agency data available to OEMs for CAV applications. Work zone data are an example of a resource that OEMs can access to notify CAVs and their operators of changes in real time.

Interviewees also advised that state DOTs become familiar with CAV sensor data while the industry is nascent. In this way, DOTs can establish processes and standards that can evolve over time.

As interviewees noted, agencies that have already established processes for addressing complaints about roadway defects are sufficiently prepared for the complaint resolution process when CAVs report roadway issues. However, these agencies will need to consider how the data will be provided to the agency. It may be most advantageous for the data to be communicated from the vehicle to the OEM (rather than directly to the agency) in the form of reports scheduled at a regular interval. A regular reporting plan from the manufacturer to the agency will allow the manufacturer to decide what conditions to report, mimicking the current process where the public selectively reports roadway conditions. Then, agencies can add the service requests into their current systems and make decisions on how to grade and prioritize the requests for maintenance.

Mitigating Potential Liability from Release of Information

Stakeholders advised that state and local government agencies change practices regarding data storage and release to account for CAV data. As data are made available from CAVs, agencies should be aware of notice requirements and privacy protections, examining whether agencies should impose a different regime to deal with protecting private or proprietary information from PIA requests. For example, CAVs and the roadside infrastructure supporting them could potentially use video for sensing or detecting their environment. Video images may violate privacy protections if they are not stored or used correctly. Thus, agencies may not want to keep any video they use for vehicle mobility purposes in storage.

Certain actions could be useful for state DOTs to maintain privacy in data. DOTs could replicate practices used by private technology companies where false attributes are inserted into data in order to anonymize them. State DOTs could also acquire third-party data management services.

Data and privacy protections could also include:

- Requesting download certificates to confirm data-handling and privacy procedures and limitations.
- Using a content management system or security management system for data to ensure account information protections for any vehicle connected to CV infrastructure.
- If providing a product that vehicles can use (e.g., a digitized map of roadway assets), doing so non-negligibly and with a duty of care by warning users that the data are not guaranteed to be accurate and clearly stating the data's known limitations.

Conclusion

While federal law and regulations concerning CAVs have yet to be proposed and codified, state DOTs and local governments should assume that the current legal framework between federal law and human-driven vehicles will remain relevant for CAVs. State DOTs and local governments could benefit from proactive efforts to codify definitions and liability approaches, as well as reviews of the current processes for infrastructure design, notice of changes, and data handling to determine any current or potential gaps that may become larger issues with the arrival of CAVs. However, agencies in Texas could take no action and still be relatively well protected from potential tort liabilities from CAV technologies. State agencies and local governments in Texas are protected by existing law that provides sovereign immunity and caps on economic damage for tort claims. These are favorable in limiting potential liabilities from CAV technologies.

Due to the many unknowns around CAV operations, infrastructure requirements, and user adoption, continuing to collaborate with manufacturers and developers of CAVs around pilot projects appears prudent to inform data-driven decision-making. However, in states like Texas, CAVs may be deployed by private companies without a state or local government agency's knowledge. Even so, some OEMs have formed partnerships with municipalities that are governed by memoranda of understanding or other types of agreements to document expectations and responsibilities between the parties. Governments may also have an interest in collaborating with OEMs to provide data or products that manufacturers will want to use to safely guide CAVs through work zones, severe weather events, or other potentially hazardous conditions. To mitigate for any potential liability, agencies may need to provide a user agreement or a warning that clearly states that the information may not be accurate or may be limited in other ways.

The stakeholder interviews revealed that CAVs are being deployed by private companies on public roadways to operate on roadways as they are currently designed, constructed, and maintained. Private CAV manufacturers do not wish to depend on government to operationalize their vehicles and are not seeking dedicated lanes or other CAV-specific infrastructure or accommodations for their vehicles. In addition, because public agencies are subject to PIA laws, private companies are and will continue to be wary of partnering with governments, unless they formalize mechanisms to protect proprietary information from disclosure.

The stakeholder interviews also affirmed that CAVs will potentially give rise to more data regarding infrastructure conditions and defects than governmental units currently manage. Thus, agencies will need to consider how the data will be communicated to them and how they will provide notice to CAVs of infrastructure defects or make conditions reasonably safe. On the other hand, state DOTs and local governments should not view information about roadway conditions generated from CAV data as different from current information channels and processes, and should not require a separate legal regime for CAV data on infrastructure condition. Instead, state DOTs should anticipate receiving more but better information about roadway conditions that will help prioritize repair work more efficiently.

4. State and Federal Law Analysis

For the state and federal legal review, the TTI research team sought to determine whether Texas state law or federal law has addressed the liability issues identified in the literature review and stakeholder interviews or if the law still contains gaps and silences. The review of these laws was also intended to provide issue-spotting, as well as legal and technical mitigation suggestions, and determine whether other states' mitigation choices identified in the literature review and stakeholder interviews may be appropriate for Texas.

Three research questions were addressed through the state and federal legal analysis:

1. How does Texas tort limitation affect TxDOT's efforts in deployments of CAV technologies?
2. How do TxDOT and local government entities position themselves to address increased liability concerns?
3. What can be learned from existing law (i.e., case law and statute) that might indicate what liability TxDOT and local jurisdictions might have?

The legal analyses build upon analyses that were performed for the literature review and stakeholder interviews regarding the following topical areas:

- Sovereign immunity.
- Design immunity.
- Data use, protection, and privacy.
- Federal preemption and vehicle safety certification.
- Insurance.

Methodology

The TTI research team completed their state and federal law analyses by searching Texas statutory codes and case law, as well as federal legislation and case law using databases (e.g., Casetext, the Transportation Research International Documentation and the Transportation Research Information Services, Lexis Nexis, Westlaw, and the EBSCO database). The Texas law analysis identified relevant statutory and case law, including:

- The Texas Tort Claims Act.
- The Texas Transportation Code provisions related to TxDOT powers and authorities and CAV operations.
- The Texas Public Information Act.
- Texas cybersecurity laws.
- Texas negligence laws.
- Texas data dissemination laws.
- Texas privacy laws.
- Texas products liability laws.

The federal law analysis identified relevant statutory and case law regarding:

- The Work Zone Data Exchange.
- Automated Driving System demonstration grant programs.
- H.R. 3388, the SELF DRIVE Act of 2017.

- S. 1885, the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act.
- P.L. 117-58, Infrastructure Investment and Jobs Act (IIJA, or the Bipartisan Infrastructure Bill).
- American Data Privacy and Protection Act (ADPPA).

Having identified relevant statutory and case law, the TTI research team analyzed the topic areas identified in the literature review and stakeholder interviews against these relevant Texas and federal laws. The research team recorded notes and key provisions from the statutes, cases, and regulations (proposed and enacted) into summary tables, included at the beginning of each topical section.

As part of this task, the research team also coordinated with TxDOT's Legislative Affairs staff to prepare for the upcoming 88th legislative session. Communication with TxDOT's Legislative Affairs staff was intended to provide TxDOT early notice of any issues that could be addressed during the legislative session in order to determine the best strategy for addressing issues with legislative members.

State Law Analysis

The TTI research team scanned existing state statutes and case law related to the issues identified in the literature review and stakeholder interviews to determine whether Texas state law has addressed those issues or if it still contains gaps and silences. The review revealed a large body of case law related to sovereign immunity for state agencies and other governmental units from tort liability, provided by the Texas Tort Claims Act (TTCA). Because sovereign immunity is a defense that a state agency may raise, it is a threshold question that may determine liability at the outset of the case, regardless of other areas of law the claim may encompass. The essential issue at the heart of this research project is tort liability. Thus, the TTCA is the prevailing statute providing for sovereign immunity that shields state agencies from liability and exceptions where such liability is waived. Accordingly, the findings on sovereign immunity are more extensively discussed in this chapter than those for the other legal areas. These findings will be applied by the research team to specific use cases in the next chapter, providing the basis from which liability may be determined for TxDOT under the scenarios.

Sovereign Immunity

Table 1 summarizes the law related to sovereign immunity generally.

Table 1. Laws Related to Sovereign Immunity.

Statute/Case	Rule	Citation
Texas Civil Practice and Remedies Code (Tex. Civ. Prac. & Rem. Code)	Generally, no liability to TxDOT for the act, omission, or negligence of a TxDOT employee who, acting within their scope of employment, causes property damage, personal injury, or death.	Tex. Civ. Prac. & Rem. Code §101.025

Generally, there is no risk of liability to TxDOT for the act, omission, or negligence of a TxDOT employee who, acting within their scope of employment, causes property damage, personal injury, or death. This is because state agencies benefit from sovereign immunity, just as political subdivisions are protected by governmental immunity, under the TTCA (*Reata Const. Corp. v. City of Dallas*, 197 S.W.3d 371 [Tex., 2006]). Codified as Title 5, Chapter 101 of the Tex. Civ. Prac. & Rem. Code, the TTCA protects "governmental units" from tort claim suits "unless the immunity has been waived by the constitution or state law" (*University of Texas Southwestern Medical Center v. Rhoades*, 605 S.W.3d 853 [Tex. 2020]). "Governmental units" include municipalities and state agencies (Tex. Civ. Prac. & Rem. Code § 101.001), which must affirmatively plead and prove sovereign or governmental immunity in order to deprive a trial court of subject-matter jurisdiction (*Jefferson County, Texas v. Ellarene Farris, Individually and as Personal Representative of the Heirs and Estate of James Farris Appeal from 11th District Court of Harris County* [Tex. App. 2018]).

Waiver of Immunity

Table 2 summarizes the law related to waivers of immunity generally.

Table 2. Laws Related to Immunity.

Statute/Case	Rule	Citation
Tex. Civ. Prac. & Rem. Code	Immunity may be waived if (1) injury arises from the operation of vehicle or vehicle equipment and the employee would be personally liable and (2) injury was caused by condition or use of tangible personal or real property and TxDOT, were it a person, would be liable.	Tex. Civ. Prac. & Rem. Code §101.021

Failure to plead immunity as a defense waives the immunity, and it cannot be raised for the first time on appeal (*Davis v. City of San Antonio*, 752 S.W.2d 518 [Tex. 1988]). Sovereign or governmental immunity is also waived by municipalities and state agencies where the Texas State Legislature has, through the TTCA, waived immunity in "clear and unambiguous language" (*Sampson v. Univ. of Tex. at Aus.*, 500 S.W.3d 380 [Tex. 2016]; Tex. Gov't. Code § 311.034). The TTCA provides such a waiver, enumerating the instances and conditions of and limitations on a governmental unit's tort liability for property damage, personal injury, and death. Specifically, under the TTCA, damages may be recovered from governmental units in Texas for:

> (1) property damage, personal injury, and death proximately caused by the wrongful act or omission or the negligence of an employee acting within his scope of employment if:
>
> (A) the property damage, personal injury, or death arises from the operation or use of a motor-driven vehicle or motor-driven equipment; and
>
> (B) the employee would be personally liable to the claimant according to Texas law; and
>
> (2) personal injury and death so caused by a condition or use of tangible personal or real property if the governmental unit would, were it a private person, be liable to the claimant according to Texas law. (Tex. Civ. Prac. & Rem. Code §101.021).

Thus, the TTCA expressly waives immunity for certain negligent acts by governmental employees in three areas when statutory requirements are met: (a) use of publicly-owned automobiles, (b) injuries arising out of a condition or use of tangible personal property, and (c) premises defects (Sampson, 500 S.W.3d at 380).

Use of Motorized Vehicles and Equipment

Table 3 summarizes case law related to the exception to sovereign immunity for the use of motorized vehicles and equipment. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 3. Laws Related to Exceptions to Sovereign Immunity.

Statute/Case	Rule	Citation
Tex. Civ. Prac. & Rem. Code	The TTCA waives sovereign immunity for property damage, personal injury, or deaths that are proximately caused by "the wrongful act or omission or the negligence" of government employees involved in the "operation or use of a motor-driven vehicle" while they are "acting within [their] scope of employment."	Tex. Civ. Prac. & Rem. Code §101.021(1)
Mount Pleasant Indep. Sch. Dist. v. Estate of Linburg	Plaintiffs must prove a "direct nexus" between the injury negligently caused by a governmental employee and the operation or use of the motor-driven vehicle. This nexus requires more than "mere involvement or proximity of a vehicle."	766 S.W.2d 208, 211 (Tex. 1989)
Dallas Area Rapid Transit v. Whitley	Use of the vehicle must have actually caused the injury and not just furnish a condition that makes the injury possible. No waiver of liability exists for a claim based on the failure to provide protection.	104 S.W.3d 540 (Tex. 2003)
City of El Paso v. Hernandez	Damages must arise from *actual* operation or use of the vehicle or equipment in performing governmental functions. No waiver of liability exists for a claim based on the non-use of publicly owned vehicles or equipment.	16 S.W.3d 409 (Tex. App.—El Paso 2000)
Leleaux v. Hamshire-Fannett Indep. Sch. Dist.	Damages must arise from the *government employee's* operation or use of the vehicle or equipment—not the injured person's or some third party's operation or use of it.	835 S.W.2d 49 (Tex. 1992)

Statute/Case	Rule	Citation
VIA Metropolitan Transit v. Meck	Governmental units providing transit services waive their immunity under the motorized vehicle and equipment exception to the TTCA. Thus, they are subject to negligence under the duty of care that a common carrier holds.	835 S.W.2d 49 (Tex. 1992)

The TTCA waives sovereign immunity for property damage, personal injury, or deaths that are proximately caused by "the wrongful act or omission or the negligence" of government employees involved in the "operation or use of a motor-driven vehicle" while they are "acting within [their] scope of employment" (Tex. Civ. Prac. & Rem. Code §101.021[1]). Sovereign immunity would be waived when someone is struck and killed by a vehicle that is operated by a government employee acting "within his scope of employment" but is under the influence, demonstrating their "wrongful act" or negligence.

The Texas Supreme Court has also determined that "operation" is "a doing or performing of practical work," and "use" means "put[ting] or bring[ing] into action or service" or "employ[ing] for or apply[ing] to a given purpose" (*Mount Pleasant Indep. Sch. Dist. v. Estate of Linburg*, 766 S.W.2d 208 [Tex. 1989]). Plaintiffs must prove a "direct nexus" between the injury negligently caused by a governmental employee and the operation or use of the motor-driven vehicle. This nexus requires more than "mere involvement or proximity of a vehicle." For liability to attach to the injury, damage, or death, the use of the vehicle "must have actually caused the injury." In other words, "the operation or use of a motor vehicle does not cause injury if it does no more than furnish a condition that makes the injury possible." Thus, damages must arise from *actual* operation or use of the vehicle or equipment in performing governmental functions. No waiver of liability exists for a claim based on the failure to provide protection or the non-use of publicly owned vehicles or equipment (*Dallas Area Rapid Transit v. Whitley*, 104 S.W.3d 540 [Tex. 2003]; *City of El Paso v. Hernandez*, 16 S.W.3d 409 [Tex. App.—El Paso 2000, no pet.]). So, sovereign immunity is not waived when someone is struck and killed by a vehicle that is properly operated by a government employee but manufactured with faulty equipment. Nor is immunity waived when injury or death is proximately caused by a vehicle operated by someone other than the government employee. Damages must arise from the *government employee's* operation or use of the vehicle or equipment—not the injured person's or some third party's operation or use of it (*Leleaux v. Hamshire-Fannett Indep. Sch. Dist.*, 835 S.W.2d 49 [Tex. 1992]).

Governmental units providing transit services waive their immunity under the motorized vehicle and equipment exception to the TTCA. Thus, they are subject to negligence under the duty of care that a common carrier holds. Such units can be found liable for "slight negligence," which under the common law imposes a duty to exercise a high degree of care on transit providers (*VIA Metropolitan Transit v. Meck*, 620 S.W.3d 356 [Tex. 2020]).

While the law has not yet been applied to cases where a state employee's wrongful act, omission, or negligence involved the operation or use of CAVs, an agency's reliance on sovereign immunity could be limited in such cases. CAVs owned by governmental units carrying out governmental activities can purportedly be operated or used independent of an employee, but the employee may be engaged in overseeing the operation of the CAV. Any property damage, personal injury, or deaths that are proximately caused by CAVs could

potentially involve a "wrongful act or omission or the negligence of an employee" in the "operation or use of a motor-driven vehicle," in the words of the TTCA. The operation or use of a publicly owned CAV, while a motor-driven vehicle, could be deemed under current law to cause injury if an employee activates or oversees operations of a CAV that is not fully autonomous. If a fully autonomous CAV operates independent of government employees, it could be considered to do "no more than furnish a condition that makes the injury possible" (*Dallas Area Rapid Transit*, 104 S.W.3d at 540).

This conclusion is, of course, subject to interpretation by the courts and legislature. One may interpret government agencies' liability for property damage, personal injury, or death that "arises from the operation or use of a motor-driven vehicle or motor-driven equipment," as the courts currently do, as a waiver of immunity for damage, injury, or death arising from the employee's operation or use of a motorized vehicle. The waiver could also include government-owned or -operated CAVs. Thus, if TxDOT wishes to be proactive, a course of action may be to propose legislation that revises Tex. Civ. Prac. & Rem. Code §101.021(1)(a) to provide that damages may be recovered from governmental units for property damage, personal injury, or death that "arises from the EMPLOYEE'S operation or use of a motor-driven vehicle or motor-driven equipment" (revision in underlined all caps). This would conform to the court's current interpretation of the law and preserve sovereign immunity if fully autonomous CAVs are operated by the ADS (i.e., without a human operator).

If a state agency were to offer transit services using CAVs, it would be considered a common carrier and held to a higher duty of care. This duty would not make the agency strictly liable as insurers or require them to employ the highest degree of care, but the agency would owe a duty to its passengers to act as "a very cautious and prudent person" would act under the same or similar circumstances (*VIA Metropolitan Transit*, 620 S.W.3d at 356). Presently, TxDOT does not directly offer any transit services.

Conditions or Use of Tangible Personal Property

Table 4 summarizes case law relevant to the exception to sovereign immunity for conditions or use of tangible personal property. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 4. Case Law Relevant to Sovereign Immunity Exceptions.

Statute/Case	Rule	Citation
Tex. Civ. Prac. & Rem. Code	Immunity may be waived if the injury is caused by a condition or use of tangible personal or real property, and TxDOT, were it a person, would be liable.	Tex. Civ. Prac. & Rem. Code §101.021(2)
TxDOT v. Jones	Governmental liability only extends to personal injuries or death and not to property damage.	8 S.W.3d 636 (Tex. 1999)
Harris County v. Shook	A contemporaneous "action or service" (use) or "state of being" (condition) of tangible personal property may be determined to cause injury and a claim for damages.	634 S.W.3d 942 (Tex. 2021)

Statute/Case	Rule	Citation
University of Texas Southwestern Medical Center v. Rhoades	The use of the personal property must have actually caused the injury. Non-use, furnishing a condition, or mere involvement are not sufficient.	605 S.W.3d 853 (Tex. 2020)

The TTCA waives sovereign immunity for personal injury or death caused by a condition or use of tangible personal or real property (Tex. Civ. Prac. & Rem. Code §101.021[2]). This includes a "condition or use" of: (a) tangible personal property and (b) tangible real property, also known as "premises defects" (covered in the next sub-section of this memorandum). With regard to a condition or use of tangible personal property, governmental liability only extends to personal injuries or death and not to property damage. Thus, damages for mental anguish or some other type of personal injury are recoverable if they can be proven (*Texas Dept. of Transp. v. Jones*, 8 S.W.3d 636 [Tex. 1999]).

The Texas Supreme Court defines "condition" as "either an intentional or an inadvertent state of being" and "use" as "put[ting] or bring[ing] into action or service" or "employ[ing] for or apply[ing] to a given purpose." In doing so it has held that a contemporaneous "action or service" (use) or "state of being" (condition) of tangible personal property may be determined to cause injury and a claim for damages (*Harris County v. Shook*, 634 S.W.3d 942 [Tex. 2021]).

Similar to its holdings with regard to operation or use of motor-driven vehicles and equipment, the Texas Supreme Court has held that government agencies waive sovereign immunity when personal property is put or brought into action or service, or employed or applied to a given purpose, holding that:

> [M]ere involvement of the [personal] property is not enough. Likewise, a use that merely furnishes the condition that makes the injury possible is not sufficient to waive immunity. A claim of non-use is also insufficient to waive immunity; actual use is required. And the use of the [personal] property must have actually caused the injury (Harris County v. Shook, 634 S.W.3d 942 [Tex. 2021]).

Current statutes and the common law are silent on whether an agency's electronic data can be regarded as tangible personal property, as well as whether the condition or use of government-owned, -produced, or -shared data waive an agency's sovereign immunity if they cause personal injury or death. However, one may draw parallels with what the Texas Supreme Court has held to be negligent use of tangible personal property. While the Court has held an electrocardiogram to be tangible personal property and misinterpretation of an electrocardiogram graph to be negligence, it has also determined that immunity is not waived for negligence involving the use, misuse, or non-use of information found in medical records (*Salcedo v. El Paso Hosp. Dist.*, 659 S.W.2d 30 [Tex. 1983]; *University of Texas Med. Branch at Galveston v. York*, 871 S.W.2d 175 [Tex. 1994]). Thus, by extension, a hard drive or server containing electronic data may be "tangible personal property." However, the condition, use, misuse, or non-use of the information contained within data may not waive liability in the same way that use, misuse, or non-use of information found in medical records does not waive liability.

At this point, this conclusion is conjecture and subject to interpretation by the courts and legislature. Therefore, if TxDOT wishes to be proactive, a course of action may be to propose legislation that expressly defines "tangible personal property" to exclude electronic data that are owned, produced, or shared by governmental units. This would conform to the court's prior decisions regarding information contained within tangible medical records while leaving government agencies open to waivers of immunity for conditions or use of other forms of tangible personal property.

Premises Defects

Table 5 summarizes state case law and statutes regarding the premises defects exception to sovereign immunity. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 5. Case Law Regarding Premises Defects Exceptions to Sovereign Immunity.

Statute/Case	Rule	Citation
Harris County v. Shook	If a condition of real property, which can be created by tangible personal property, causes injury, it gives rise to a premises defect claim.	634 S.W.3d 942 (Tex. 2021)
Texas Transportation Code	TxDOT has "exclusive and direct control of all improvement of the state highway system."	Texas Transp. Code § 224.031
Gunn v. Harris Methodist Affiliated Hosp.	Premises defects include potholes on a roadway. TxDOT can mitigate this risk by providing adequate notice under its legal duty of care.	887 S.W.2d 248, 250 (Tex. App.—Fort Worth 1994)
Eldridge v. Brazoria County	A premises defect does not have to be caused by a governmental employee.	No. 01-13- 00314-CV, 2014 WL 1267055 (Tex. App.—Houston [1st Dist.], 2014)
DeWitt v. Harris County	When injury is caused by real property, liability is not determined by the action of a government employee, but upon the property itself being unsafe.	904 S.W.2d 650, 653 (Tex. 1995)
Tex. Civ. Prac. & Rem. Code	If a claim arises from a premises defect, the governmental unit owes to the plaintiff only the duty a private person owes to a licensee on private property, unless the claimant pays for use of the premises.	Tex. Civ. Prac. & Rem. Code § 101.022(a)

Statute/Case	Rule	Citation
Tex. Civ. Prac. & Rem. Code	Invitees who pay for use of real property (e.g., users of a tolled road) are owed by the government a higher standard of care than claims based on "a condition or use of tangible personal property."	Tex. Civ. Prac. & Rem. Code § 101.022(c)
Sampson v. University of Texas at Austin	The level of awareness required of governmental units under the standard of care for premises defects is "actual knowledge" of the condition that has created "an unreasonable risk of harm to the licensee."	500 S.W.3d 380, 385 (Tex. 2016)

As provided in the previous sub-section, a premises defect claim can arise if a condition of real property causes an injury (*Harris County*, 634 S.W.3d at 942). The TTCA waives sovereign immunity for "personal injury and death so caused by a condition or use of tangible personal or real property" (Tex. Civ. Prac. & Rem. Code §101.021[2]). A claim cannot be both a premises defect claim and a claim relating to a condition or use of tangible property. The two claim types can be distinguished by assessing whether the actual use or condition of the tangible personal property itself caused the injury, or whether a condition of real property, which can be created by tangible personal property, caused the injury, giving rise to a premises defect claim (*Harris County*, 634 S.W.3d at 942).

The Texas Transportation Commission and TxDOT are particularly sensitive to premises defects claims due to their statutory authority to "plan and make policies for the location, construction, and maintenance of a comprehensive system of state highways and public roads" and have "exclusive and direct control of all improvement of the state highway system" (Texas Transportation Code §§ 201.103, 224.031). As real property, the state highways and public roads in Texas may be in a condition that creates potential personal injury or death, which presents risk of premises defect claims. For example, premises defects include potholes on a roadway. TxDOT can mitigate this risk by providing adequate notice under its legal duty of care (*Gunn v. Harris Methodist Affiliated Hosp*., 887 S.W.2d 248, 250 [Tex. App.—Fort Worth 1994, writ denied]).

Under the TTCA, a premises defect does not have to be caused by a governmental employee (*Eldridge v. Brazoria Cnty*., No. 01-13- 00314-CV, 2014 WL 1267055 [Tex. App.—Houston, 1st Dist., Mar. 27, 2014]). When injury is caused by real property, liability is not determined by the action of a governmental employee but upon the property itself being unsafe (*DeWitt v. Harris Cnty*., 904 S.W.2d 650, 653 [Tex. 1995]). However, the TTCA provides that "if a claim arises from a premise defect, the governmental unit owes to the plaintiff only the duty a private person owes to a licensee on private property, unless the claimant pays for use of the premises" (Tex. Civ. Prac. & Rem. Code § 101.022[a]). This is a different standard of care than claims based on "a condition or use of tangible personal property" and specifically applies when "a claim arises from a premise defect on a toll highway, road, or street" (Tex. Civ. Prac. & Rem. Code § 101.022[c]). Even though one could argue that users of tolled highways are owed a higher standard of care because they are invitees who make

payment for use of the roadway, the same duty applies as if the person were a licensee. Similarly, Texas courts have held that payment of vehicle registration and licensing fees do not constitute payment for the use of the state's highways (*State Dept. of Highways and Public Transp. v. Kitchen*, 867 S.W.2d 784 [Tex. 1993]).

The duty that a private person owes to a licensee on private property requires that they "not injure a licensee by willful, wanton, or grossly negligent conduct" and "use ordinary care either to warn a licensee of, or to make reasonably safe, a dangerous condition of which the owner is aware and the licensee is not." The Texas Supreme Court has established that plaintiffs must prove five elements to establish breach of this duty:

> (1) a condition of the premises created an unreasonable risk of harm to the licensee; (2) the owner actually knew of the condition; (3) the licensee did not actually know of the condition; (4) the owner failed to exercise ordinary care to protect the licensee from danger; (5) the owner's failure was a proximate cause of injury to the licensee.

The level of awareness required of governmental units under the standard of care for premises defects is "actual knowledge" of the condition that has created "an unreasonable risk of harm to the licensee." Though the common law does not provide a test for determining actual knowledge, Texas courts "generally consider whether the premises owner has received reports of prior injuries or reports of the potential danger presented by the condition." To be subject to liability, government agencies are required to have knowledge of "the dangerous condition at the time of the accident, not merely of the possibility that a dangerous condition can develop over time" nor "[a]wareness of a potential problem" (*Sampson v. Univ. of Tex. at Aus*., 500 S.W.3d 380, 385 [Tex. 2016]).

Once governmental units have actual knowledge of a premises defect, they have a duty to "exercise ordinary care to protect the licensee from danger." Thus, they have the duty to either warn the licensee of, or make reasonably safe, the unreasonably dangerous condition.

Applying the law on premises defects to CAV technology deployment, TxDOT will likely owe the same standard of care it owes to persons in non-CAV vehicles on its roadways since the duty applies to drivers and passengers. In a world where CAVs are as ubiquitous as non-CAVs are today, a dangerous roadway condition will still potentially create unreasonable risk of harm to passengers in the CAVs. Therefore, TxDOT will still need to have actual knowledge of the premises defect through reports of prior injuries or potential danger arising from the condition. If CAV sensors generate large volumes of data at high frequencies regarding infrastructure condition and defects, they will only serve to add to the backlog of maintenance requests that will need to be handled to make roadways safe. However, as noted in the previous chapter, recent CAV tests in Texas have shown that the type of information being collected from CAVs and the processing of such information by TxDOT match the kind of information that TxDOT currently receives from the greater public. Thus, as it does with reports of roadway issues currently received though humans calling in a complaint, TxDOT will process CAV data in a timely fashion.

Legislation on this issue may not be necessary to prepare for a scenario where the volume and frequency of data regarding roadway condition increases to a level that exceeds TxDOT's ability to process the information and handle service requests since roadway conditions where CAVs operate are likely to remain the same as today. However, TxDOT may choose to consider implementing operational measures that will provide CAVs and their passengers actual knowledge of premises defects. These measures could include alerts on the vehicle's

display or passenger's communication device as well as data provided to ADS warning of the dangerous condition and advising how to avoid it.

Special Defects

Table 6 summarizes state statutes and case law regarding the special defects exception to sovereign immunity. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 6. Statutes and Case Law Regarding Special Defects Exceptions to Sovereign Immunity.

Statute/Case	Rule	Citation
Texas Civ. Prac. & Rem. Code	Under the TTCA, the government owes a higher duty of care for (1) special defects and (2) the absence, condition, or malfunction of traffic signs, signals, or warning devices.	Tex. Civ. Prac. & Rem. Code § 101.022(b)
Denton County v. Beynon	Special defects are excavations or obstructions on a roadway that pose a threat to ordinary users in the manner that an excavation or obstruction blocking the road does. Special defects do not include an unsecured floodgate arm in a resting position three feet off a roadway pointed toward oncoming traffic.	283 S.W.3d 329 (Tex. 2009)
State v. Burris	Special defects do not include a fully operational motor vehicle making an illegal movement or momentarily stopped on a highway.	877 S.W.2d 298 (Tex. 1994)
City of Houston v. Rushing	Special defects do not include a stopped pickup truck blocking a lane of traffic.	7 S.W.3d 909, 909
City of Grapevine v. Roberts	Special defects do not include a sidewalk and its steps to the street.	946 S.W.2d 841 (Tex. 1997)
State Dept. of Highways and Public Transp. v. Payne	Special defects do not include culverts.	838 S.W.2d 235 (Tex. 1992)
Reyes v. Laredo	Special defects do not include flooded low water crossings.	335 S.W.3d 605 (Tex. 2010)

Statute/Case	Rule	Citation
Brumfield v. TxDOT	Special defects do not include a 2-inch difference in grade on a highway.	2014 WL 2462699, No. 02- 13-00175-CV (Tex. App.—Fort Worth, 2104)
City of Houston v. Cogburn	Special defects do not include tree roots.	No. 01- 11000318-CV, 2014 WL 1778279 (Tex. App.—Houston [1st Dist.], 2014)
TxDOT v. York	Under the more lenient invitee standard, plaintiffs only need to prove that the governmental unit "should have known of a condition that created an unreasonable risk of harm."	284 S.W.3d 844 (Tex. 2009)
State Dept. of Highways and Public Transp. v. Payne	Special defects are roadway excavations or obstructions that pose a threat to the ordinary users of a particular roadway. The statutory test for proving a special defect is whether the condition is of the same class as an excavation or obstruction. With special defects, the governmental unit owes the same duty to warn of dangerous conditions that a private landowner owes to an invitee. Proving that a government agency failed this duty requires establishing that the agency is or reasonably should be aware of the dangerous condition. Special defects do not include loose gravel on a roadway.	838 S.W.2d 235 (Tex. 1992)

The government's duty to exercise ordinary care under Tex. Civ. Prac. & Rem. Code § 101.022(a) "does not apply to the duty to warn of two types of conditions: (1) 'special defects'; and (2) the absence, condition, or malfunction of traffic signs, signals, or warning devices." In these cases, the government's duty is not limited, and therefore, the government owes a higher duty of care.

By statute, special defects include "excavations or obstructions on highways, roads, or streets" that "pose a threat to the ordinary users of a particular roadway." The statutory test for proving a special defect is "simply whether the condition is of the same class as an excavation or obstruction" (*State Dept. of Highways and Public Transp. v. Payne*, 838 S.W.2d 235 [Tex. 1992]). The Texas Supreme Court has narrowly defined special defects as excavations or obstructions on a roadway that pose a threat to ordinary users in the manner that an excavation or obstruction blocking the road does (*Denton County v. Beynon*, S.W.3d 329 [Tex. 2009]). Under common law, Texas courts have determined that special defects do not include:

- A fully operational motor vehicle making an illegal movement or momentarily stopped on a highway (State v. Burris, 877 S.W.2d 298 [Tex. 1994]).
- A stopped pickup truck blocking a lane of traffic (City of Houston v. Rushing, 7 S.W.3d 909).
- A sidewalk and its steps to the street (City of Grapevine v. Roberts, 946 S.W.2d 841 [Tex. 1997]).
- Culverts (State Dept. of Highways and Public Transp., 838 S.W.2d at 235).
- Flooded low water crossings (Reyes v. Laredo, 335 S.W.3d 605 [Tex. 2010]).
- A 2-inch difference in grade on a highway (Brumfield v. Tex. Dept. of Transp., 2014 WL 2462699, No. 02-13-00175-CV [Tex. App.—Fort Worth May 29, 2104]).
- Tree roots (City of Houston v. Cogburn, No. 01- 11000318-CV, 2014 WL 1778279 [Tex. App.—Houston, 1st Dist., May 1, 2014]).
- An unsecured floodgate arm in a resting position three feet off a roadway pointed toward oncoming traffic (Denton County v. Beynon, S.W.3d 329 [Tex. 2009]).
- Loose gravel on a roadway (Tex. Dept. of Transp. v. York, 284 S.W.3d 844 [Tex. 2009]).

With special defects, the governmental unit owes the roadway user the duty to warn of dangerous conditions that a private landowner owes to an invitee (as opposed to premises defects, for which a licensee standard applies). Under the more lenient invitee standard, plaintiffs only need to prove that the governmental unit "should have known of a condition that created an unreasonable risk of harm" (*Tex. Dept. of Transp.*, 284 S.W.3d at 844). Thus, proving that a government agency failed this duty requires establishing that the agency is or reasonably should be aware of the dangerous condition (*State Dept. of Highways and Public Transp.*, 838 S.W.2d at 235).

With regard to special defects, TxDOT will likely owe the same duty of care it owes to persons in non-CAV vehicles on its roadways since the duty applies to drivers and passengers. Once CAVs have been deployed, an excavation or obstruction on a highway, road, or street can still present a potential threat to ordinary roadway users in CAVs. Therefore, TxDOT will need to be more vigilant about special defects than with premises defects since the agency will not have to wait until they have actual knowledge of the special defect. Rather, TxDOT will be expected to act to notify CAVs or otherwise mitigate the special defect when it should have known of it. As with premises defects, legislation may not be necessary to prepare for CAV deployments since roadway conditions where CAVs operate are likely to remain the same as today. However, TxDOT may choose to consider implementing operational measures that will quickly alert maintenance and operations personnel of excavations or obstructions on a roadway and provide CAVs and their passengers notice of the special defect through such forms as alerts and data warning of the special defect.

Traffic Signs, Signals, and Warning Devices

Table 7 summarizes the statutes and case law related to the traffic signs, signals, and warning devices exception to sovereign immunity. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 7. Case Law and Statutes Related to Traffic Signs, Signals, and Warning Devices Exceptions to Sovereign Immunity.

Statute/Case	Rule	Citation
Texas Civ. Prac. & Rem. Code	TxDOT owes a higher duty of care for the absence, condition, or malfunction of traffic signs, signals, or warning devices.	Tex. Civ. Prac. & Rem. Code § 101.022(b)
Texas Civ. Prac. & Rem. Code	TxDOT may be found liable when (1) the absence, condition, or malfunction is not corrected within a reasonable time after notice of the missing or malfunctioning sign or signal; or (2) a traffic or road sign, signal, or warning device is removed or destroyed by a third party and the governmental unit fails to correct the removal or destruction within a reasonable time after actual notice.	Tex. Civ. Prac. & Rem. Code § 101.060
TxDOT v. Olivares	Deteriorated pavement markings that insufficiently perform their traffic control function fall within this exception, so they must be corrected by the responsible governmental unit within a reasonable time after receiving actual or constructive notice.	316 S.W.3d 89 (Tex. App. 2010)
City of Austin v. Lamas	The duty to warn of the absence, condition, or malfunction of traffic signals, signs, or warnings does not require actual notice. Notice can be either actual or constructive.	160 S.W.3d 97 (Tex. App. 2005)
City of Dallas v. Donovan	The duty to warn of the removal or destruction of traffic signals, signs, or warnings requires actual notice.	768 S.W.2d 905 (Tex. App.— Dallas 1989)
State ex rel. State Dept. of Highways and Public Transp. v. Gonzalez	Under subsection (a)(1), which makes governmental units liable for failure to initially place a traffic or road sign, signal, or warning device as a result of a discretionary decision, the state retains immunity for discretionary sign-placement decisions. The "failure to make certain discretionary decisions affecting a stop sign's susceptibility to repeated vandalism was not a failure to correct the sign's 'condition.'"	82 S.W.3d 322 (Tex. 2002)
TxDOT v. Ramming	A governmental unit could be held liable for injuries and deaths for missing or malfunctioning traffic control devices caused by its employees. The governmental unit will be given a reasonable time to replace a missing traffic control device or repair a malfunctioning one, but only if the malfunction or absence was the result of a component failure, act of God, or act of a third party.	861 S.W.2d 460, 465 (Tex. App.— Houston [14th Dist.] 1993)

The TTCA's limitation on governmental units' duty to exercise ordinary care also extends to "the absence, condition, or malfunction of traffic signs, signals, or warning devices" (Tex. Civ. Prac. & Rem. Code § 101.022[b]). Texas courts have determined that the condition of pavement markings falls under this traffic safety device exception to sovereign immunity (*Tex. Dept. of Transp. v. Olivare*s, 316 W.W.3d 89 [Tex. App. 2010]). Thus, failure to correct the condition of a traffic sign, signal, warning device, or lane marking that raises safety issues within a reasonable time after notice renders a governmental unit susceptible to a waiver of sovereign immunity and subject to a higher duty of care than under Tex. Civ. Prac. & Rem. Code § 101.022(a).

Because the initial decision to erect a traffic sign, signal, or warning device is discretionary, it is protected by sovereign immunity. However, this immunity can be waived by governmental units if a traffic control device is in fact erected and its absence, condition, or malfunction is not corrected within a reasonable time after notice. If the government agency does not provide a warning and had notice of the defect, it could be held liable for personal injuries or death caused by the defect.

TxDOT has statutory authority to place and maintain traffic control signs, signals, and warning devices under Title 6, Subtitle A, Chapter 201 and Title 7, Subtitle C, Chapter 544 of the Texas Transportation Code. Tex. Civ. Prac. & Rem. Code § 101.060(a)(1)'s waiver of immunity for failure to initially place a traffic sign, signal, or warning device as a result of a discretionary decision does not apply to TxDOT's discretionary sign-placement decisions. TxDOT, however, has a duty to warn of the absence, condition, or malfunction of traffic signals, signs, or warnings and may be found liable if:

- The absence, condition, or malfunction is not corrected within a reasonable time after notice of the missing or malfunctioning sign or signal (Tex. Civ. Prac. & Rem. Code § 101.022[b]).
- A traffic or road sign, signal, or warning device is removed or destroyed by a third party and the governmental unit fails to correct the removal or destruction within a reasonable time after actual notice (Tex. Civ. Prac. & Rem. Code § 101.060).

The duty to warn of the absence, condition, or malfunction of traffic signals, signs, or warnings does not require actual notice. Notice can be either actual or constructive (*City of Austin v. Lamas*, 160 S.W.3d 97 [Tex. App. 2005]). However, the duty to warn of the removal or destruction of traffic signals, signs, or warnings by a third party requires actual notice, which the court defined as "information…actually communicated to or obtained by a city employee responsible for acting on the information" (*City of Dallas v. Donovan*, 768 S.W.2d 905 [Tex. App.—Dallas 1989]).

The Texas Supreme Court held that failure to stop the repeated removal of traffic signs by vandals does not waive sovereign immunity. While the TTCA creates a duty for TxDOT and other government agencies to correct a traffic sign's removal or destruction by a third person upon receiving notice, the "failure to make certain discretionary decisions affecting a stop sign's susceptibility to repeated vandalism was not a failure to correct the sign's 'condition'" (*State ex rel. State Dept. of Highways and Public Transp. v. Gonzalez*, 82 S.W.3d 322 [Tex. 2002]).

The Texas Supreme Court has also held that a governmental unit could be held liable for injuries and deaths for missing or malfunctioning traffic control devices caused by its employees. The governmental unit will be

given a reasonable time to replace a missing traffic control device or repair a malfunctioning one, but only if the malfunction or absence was the result of a component failure, act of God, or act of a third party (*Texas Dept. of Transp. v. Ramming*, 861 S.W.2d 460, 465 [Tex. App.—Houston, 14th Dist., 1993]).

CAVs will likely rely on traffic signs, signals, warning devices, and lane markings in the same way that human drivers need them for safe traffic operations. Thus, TxDOT will likely owe the same duty of care it owes to persons in non-CAV vehicles on its roadways since the duty applies to drivers and passengers. Once CAVs have been deployed, the absence, condition, or malfunction of traffic signs, signals, warning devices, or lane markings can still present a danger to roadway users in CAVs. TxDOT will need to have either constructive or actual notice of these traffic control devices. TxDOT will need actual notice of traffic control devices that have been destroyed or removed by a third party. Thus, as with premises defects and special defects, legislation may not be necessary to prepare for CAV deployments. However, this will not relieve TxDOT of the need to consider implementing operational measures that will warn CAVs and their passengers of absent, defective, or malfunctioning traffic control devices.

In the future, it is possible that the digitization of data about TxDOT's traffic control devices could give rise to legal issues from the dissemination of those data to other governmental units (e.g., municipalities, metropolitan planning organizations) and road users. Such data may come in the form of location data, photographic data, or vehicle telematics, which may be collected and distributed to CAVs. TxDOT could acquire, store, maintain, update, and disseminate such data, applying the statutory duty of care to warn of the absence, condition, or malfunction of traffic signals, signs, or warnings upon notice. To fulfill this duty, TxDOT could adopt a policy of warning users of missing, destroyed, or malfunctioning traffic control devices, including lane markings, upon receiving actual or construed communication of the missing, destroyed, or malfunctioning traffic control device. These warnings could come in the form of alerts and data showing the absence, defect, or malfunction.

If such data were to be compromised through hacking rendering the traffic control device inoperable or otherwise damaged, TxDOT will be given a reasonable time after actual notice to repair the traffic control device because the malfunction was the result of the act of a third party. However, it could still be prudent for TxDOT to adopt a policy of warning users of defective or inoperable traffic control devices, as well as hacking of traffic control device data, if it cannot make the devices and data reasonably safe within a reasonable time once it has knowledge of the defect or threat.

Joint Enterprise and Independent Contractors

Table 8 summarizes the statutory and case law related to the application of sovereign immunity to joint enterprises and independent contractors. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 8. Case Law and Statutes Related to Sovereign Immunity and Joint Enterprises and Independent Contractors.

Statute/Case	Rule	Citation
Shoemaker v. Estate of Whistler	A joint enterprise must involve a governmental unit engaging in: (1) an express or implied agreement with other parties in a group, (2) a common purpose that will be carried out by the group, (3) a "community of pecuniary interest in that purpose" amongst the group's members, and (4) an "equal right to a voice in the direction of the enterprise," giving an equal right to control of the joint enterprise.	514 S.W. 2d 10 (1974)
TxDOT v. Able; St. Joseph Hosp. v. Wolff	TxDOT waived its sovereign immunity because it entered into a joint enterprise with the Metropolitan Transit Authority of Harris County (Houston METRO) to build and maintain a high-occupancy vehicle (HOV) lane where an accident raised questions about its safety.	35 S.W.3d 608 (Tex. 2000); 94 S.W.3d 513 (Tex. 2002)
Tex. Civ. Prac. & Rem. Code	Governmental units cannot plead sovereign immunity for damage, injury, or death proximately caused by wrongful acts, omissions, or negligence of their independent contractors.	Tex. Civ. Prac. & Rem. Code § 101.001(2)
City of Houston v. Williams	Sovereign immunity is waived by state agencies when they contract with a private party for engineering, architectural, or construction services and have been found to be in breach of the contract.	353 S.W.3d 128 (2011)

The Supreme Court of Texas has considered whether governmental units waive their sovereign immunity as members of a joint enterprise. The court has determined four elements for determining whether a joint enterprise exists. A joint enterprise must involve a governmental unit engaging in: (1) an express or implied agreement with other parties in a group, (2) a common purpose that will be carried out by the group, (3) a "community of pecuniary interest in that purpose" amongst the group's members, and (4) an "equal right to a voice in the direction of the enterprise," giving an equal right to control of the joint enterprise (*Shoemaker v Estate of Whistler*, 514 S.W. 2d 10, 14 [1974]). The court has held that, hypothetically speaking, if Agency A, which would otherwise be immune from liability, is engaged in a joint enterprise with Agency B, and Agency B acts as an agent for Agency A, Agency A can be found liable for Agency B's negligence as if it were a private person.

The Texas Supreme Court has already found that TxDOT engaged in a joint enterprise and therefore waived sovereign immunity for a claim against them under the TTCA. In 2002, the court held that TxDOT waived its sovereign immunity because it entered into a joint enterprise with the Houston METRO to build and maintain a HOV lane where a crash raised questions about its safety. Houston METRO was liable as a private person for its negligence in the construction and maintenance of the HOV lane. TxDOT, as a member of the joint enterprise with Houston METRO (where Houston METRO acted as TxDOT's agent), also waived its immunity and

was subject to the same liability (*Texas Dept. of Transp. v. Able*, 35 S.W.3d 608 [Tex. 2000]; *St. Joseph Hosp. v. Wolff*, 94 S.W.3d 513 [Tex. 2002]).

Texas statutes do not extend sovereign immunity to independent contractors. The TTCA defines an "employee" as "a person, including an officer or agent, who is in the paid service of a governmental unit by competent authority" but excludes "an independent contractor, an agent or employee of an independent contractor, or a person who performs tasks the details of which the governmental unit does not have the legal right to control" (Tex. Civ. Prac. & Rem. Code § 101.001[2]). As such, governmental units cannot plead sovereign immunity for damage, injury, or death proximately caused by wrongful acts, omissions, or negligence of their independent contractors.

Sovereign immunity is also waived by state agencies when they contract with a private party for engineering, architectural, or construction services and have been found to be in breach of the contract (Tex. Civ. Prac. & Rem. Code § 114.003). The Texas Supreme Court has affirmed this principle, holding that "according to its plain terms, the [TTCA] by clear and unambiguous language waives a governmental entity's immunity from suit for breach of written contract" (*City of Houston v. Williams*, 353 S.W.3d 128 [2011]).

CAV deployment in Texas may involve joint enterprises with other governmental units (i.e., local, regional, and state), as well as contracts with private engineering, architectural, or construction firms. These arrangements may be needed to collect, store, maintain, share, and distribute infrastructure data to be used by CAVs or design and construct CAV infrastructure (e.g., sensors, roadside units, dedicated CAV lanes). In doing so, TxDOT may be exposed to potential liabilities from waivers of sovereign immunity resulting from the acts of its third-party public- and private-sector agents. Therefore, TxDOT may consider protecting itself from this potential liability through legislative and contractual means.

The simplest legislative means of limiting TxDOT's liability for joint enterprises for CAV deployment would be to amend Tex. Civ. Prac. & Rem. Code § 101.0211, which makes two exceptions to the extension of liability to all parties of a joint enterprise (i.e., vicarious liability). The amendment would add another exception to include state agencies involved with other state agencies, municipalities, and regional agencies or authorities in a joint enterprise to deploy CAV infrastructure.

Similarly, the simplest legislative means of limiting TxDOT's liability for its independent contractors involved in CAV deployment would be to amend Tex. Civ. Prac. & Rem. Code § 101.001(2), which defines an "employee" for purposes of the TTCA. The amendment would strike the phrase "but does not include an independent contractor, an agent or employee of an independent contractor, or a person who performs tasks the details of which the governmental unit does not have the legal right to control." This, however, may be too broad and counter to public policy since it renders TxDOT immune from liability resulting from acts of all of its contractors. Alternatively, Tex. Civ. Prac. & Rem. Code § 101.055 could be amended to add another governmental function that is excluded from any waiver of immunity. It could provide that the TTCA does not apply to claims arising from the actions of a governmental employee or an independent contractor in connection with planning, designing, constructing, and maintaining infrastructure and data collection and distribution that support the operation of CAVs on state highways. This exception could be modeled on the one that exists for traffic and road signs, signals, and warning devices in Tex. Civ. Prac. & Rem. Code § 101.060 to limit liability for potential

hazards connected to use of roadways by CAVs and preserve the duty of care and notice and mitigation requirements under the TTCA.

TxDOT could also limit its liability from joint enterprises and its independent contractors through contractual means by including indemnification clauses in its contractual agreements with third parties. Indemnification is a means of shifting loss between or among parties targeted by plaintiffs injured by an act or omission of a party; it is a legal agreement by one party to hold the other harmless to liability for potential loss or damages arising from a contractual arrangement. Through indemnification, contractors can hold state agencies blameless in the event of possible loss or damage such that the contractors are wholly liable for the plaintiff's claims related to the services rendered by the contractor.

Caps on Damages and Proportionate Responsibility

Table 9 summarizes the statutes covering caps on damages and proportionate responsibility.

Table 9. Case Law and Statutes Related to Caps on Damages and Proportionate Responsibility.

Statute/Case	Rule	Citation
Tex. Civ. Prac. & Rem. Code	Where sovereign immunity has been waived, caps on liability are applied to the total of monetary damages and prejudgment interest with limits for: • The state government (i.e., $250,000 per person, $500,000 per occurrence of bodily injury or death, and $100,000 per injury or destruction of property). • Units of local government (i.e., $100,000 per person, $300,000 per bodily injury or death, and $100,000 per injury or destruction of property). • Municipalities (i.e., $250,000 per person, $500,000 per bodily injury or death, and $100,000 per injury to or destruction of property).	Tex. Civ. Prac. & Rem. Code § 101.023
Tex. Civ. Prac. & Rem. Code	Proportionate responsibility bars a plaintiff's recovery of damages if their "percentage of responsibility is greater than 50 percent."	Tex. Civ. Prac. & Rem. Code § 33.001
Tex. Civ. Prac. & Rem. Code	If the plaintiff's percentage of responsibility is not greater than 50 percent, the court must reduce the amount of damages by a percentage equal to the claimant's percentage of responsibility. This reduction must also account for other parties involved.	Tex. Civ. Prac. & Rem. Code § 33.012

Even if sovereign immunity is waived by TxDOT for tort claims related to CAV deployment, it is advantaged by caps on damages provided by the TTCA. State statute sets maximum damage limits on liability for actions brought under the TTCA against a governmental unit involving governmental functions where sovereign immunity has been waived. The caps are applied to the total of monetary damages and prejudgment interest with limits on liability for:

- The state government, which is only liable for money damages up to $250,000 for each person, $500,000 for each single occurrence of bodily injury or death, and $100,000 for each single occurrence of injury to or destruction of property.
- Units of local government, which are liable for money damages up to $100,000 for each person, $300,000 for each single occurrence of bodily injury or death, and $100,000 for each single occurrence of injury to or destruction of property.
- Municipalities, which are only liable for money damages up to $250,000 for each person, $500,000 for each single occurrence of bodily injury or death, and $100,000 for each single occurrence of injury to or destruction of property (Tex. Civ. Prac. & Rem. Code § 101.023).

Another protection against tort liability is Texas law establishing it as a "proportionate responsibility" state. Similar to comparative negligence, which allows a reduction in a plaintiff's recovery if the plaintiff was partially to blame for their injury, proportionate responsibility bars a plaintiff's recovery of damages if their "percentage of responsibility is greater than 50 percent" (Tex. Civ. Prac. & Rem. Code § 33.001).

Under state statute, it is the trier of fact's responsibility to determine the percentage of responsibility among the parties, as follows:

> Stated in whole numbers, for the following persons with respect to each person's causing or contributing to cause in any way the harm for which recovery of damages is sought, whether by negligent act or omission, by any defective or unreasonably dangerous product, by other conduct or activity that violates an applicable legal standard, or by any combination of these:
>
> (1) each claimant;
>
> (2) each defendant;
>
> (3) each settling person; and
>
> (4) each responsible third party…(Tex. Civ. Prac. & Rem. Code § 33.003).

If the plaintiff's percentage of responsibility is not greater than 50 percent, the court must reduce the amount of damages "by a percentage equal to the claimant's percentage of responsibility." This amount is further reduced to the extent that other parties are involved in the cause of action (Tex. Civ. Prac. & Rem. Code § 33.012).

Design Immunity

Table 10 summarizes the statutes and case law regarding design immunity. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 10. Case Law and Statutes Related to Design Immunity.

Statute/Case	Rule	Citation
Carrasco v. City of El Paso	Governmental units who engage in design of roadways may not be sued for claims of harm due to dangerous conditions of public properties designed through engineering-based decisions.	625 S.W.3d 189 (Tex. App. 2021)
Texas Transp. Code	State statute provides design criteria for transportation projects but is silent on design appropriateness for future modes or vehicles (e.g., CAVs).	Tex. Transp. Code §201.615

Texas design immunity principles protect TxDOT from a claim that a roadway, where injury or death involving a CAV occurs, was not designed for CAVs. Two components of state statute support this assertion.

First, the TTCA provides an exception for discretionary functions, applying sovereign immunity to claims based on:

> (1) the failure of a governmental unit to perform an act that the unit is not required by law to perform; or
>
> (2) a governmental unit's decision not to perform an act or on its failure to make a decision on the performance or nonperformance of an act if the law leaves the performance or nonperformance of the act to the discretion of the governmental unit (Tex. Civ. Prac. & Rem. Code § 101.056).

The Texas Supreme Court has held that design of any public work, including roadways, is a discretionary function protected by this statute to which governmental or sovereign immunity applies. Thus, governmental units who engage in design of roadways may not be sued for claims of harm due to dangerous conditions of public properties designed through engineering-based decisions (*Carrasco v. City of El Paso*, 625 S.W.3d 189 [Tex. App. 2021]).

Second, the Texas Transportation Code provides design criteria for transportation projects (excluding maintenance resurfacing projects) that include aspects of safety and durability, the cost of maintenance, the effects on the environment and surrounding communities, and access to other transportation modes, thus supplying a statutory standard for design. This section does not require that TxDOT contemplate the question of design appropriateness for future modes or vehicles (e.g., CAVs) (Tex. Transp. Code §201.615). Thus, it is possible that TxDOT is not required to take CAVs into consideration under its statutory authority.

Federal Preemption and Vehicle Safety Certification

Table 11 summarizes the statutes and federal order governing federal preemption of vehicle safety certification. In the discussion below, these provisions are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 11. Statutes and Federal Orders Regarding Preemption of Federal Vehicle Safety Certification.

Statute/Case	Rule	Citation
Texas Transp. Code	An "automated driving system" is defined as hardware and software installed in a vehicle that can collectively perform "all aspects of the entire dynamic driving task for the vehicle on a sustained basis" as well as "any fallback maneuvers necessary to respond to a failure of the system" without human intervention or supervision. An "automated motor vehicle" is defined as a vehicle with an automated driving system installed in it.	Tex. Transp. Code § 545.451
Texas Transp. Code	Owners of automated motor vehicles are responsible for compliance with traffic and motor vehicle laws. Automated motor vehicles are allowed to operate without a human operator in the state of Texas.	Tex. Transp. Code § 545.453
Texas Transp. Code	Automated motor vehicles are prohibited from operating if they are incapable of operating in compliance with state traffic and motor vehicle laws, are not equipped with manufacturer-installed recording devices and federally compliant automated driving systems, not registered and titled in the state, or not insured.	Tex. Transp. Code § 545.454
Texas Transp. Code	Automated motor vehicles are required to comply with existing state law regarding accidents and reporting of accidents.	Tex. Transp. Code § 545.455
Texas Transp. Code	Automated vehicle owners may identify them as such to the state.	Tex. Transp. Code § 545.456
Texas Transp. Code	"Automated motor vehicles" are exempt from: • State motor vehicle equipment laws and regulations that support human operation of vehicles or are not relevant to automated driving systems. • Required vehicle safety inspections with respect to any equipment.	Tex. Transp. Code § 547.618
Texas Transp. Code	Political subdivisions and state agencies are prohibited from "impos[ing] a franchise or other regulation related to the operation of an automated motor vehicle or automated driving system.	Tex. Transp. Code § 545.452

Statute/Case	Rule	Citation
Texas Transp. Code	Automated vehicles are assumed to have passed state safety inspections, as long as they are not a trailer, semitrailer, pole trailer, or mobile home and are equipped with ADS designed to be operated exclusively by the ADS for all trips.	Texas. Transp. Code § 547.618
Texas Transp. Code	State statute requires that protocols around crashes involving automated motor vehicles must conform with existing required procedures under Chapter 550 of the Texas Transportation Code.	Tex. Transp. Code § 545.455
NHTSA Standing Order	Federal requirement creates a three-year reporting obligation for named manufacturers, developers, and operators of Level 2 ADAS and Levels 3 through 5 ADS in which covered crashes must be reported within 10 days of the incident.	NHTSA, *Summary Report: Standing General Order on Crash Reporting for Level 2 Advanced Driver Assistance Systems*, 2021

As the literature review revealed, the federal government is expected to continue to regulate vehicle design and establish safety criteria through NHTSA's FMVSS. This federal standard for automobile safety-related components, systems, and design features generally preempts state and local safety standards if those state or local standards do not meet federal requirements. Likewise, FMVSS supersede any state law that imposes a performance standard not consistent with the federal standard on motor vehicle and component manufacturers in a state law tort claim.

In lieu of federal standards for CAVs, Texas has adopted its own regulatory framework for CAVs. In 2017, during the 85th Legislative Session, the Texas Legislature passed Senate Bill (S.B.) 2205. The bill amended the Texas Transportation Code to:

- Define an "automated driving system" as hardware and software installed in a vehicle that can collectively perform "all aspects of the entire dynamic driving task for the vehicle on a sustained basis" as well as "any fallback maneuvers necessary to respond to a failure of the system" without human intervention or supervision.
- Define an "automated motor vehicle" as a vehicle with an automated driving system installed in it (Tex. Transp. Code § 545.451).
- Place responsibility with the owner of an automated motor vehicle for compliance with traffic and motor vehicle laws.
- Allow automated motor vehicles to operate without a human operator in the state (Tex. Transp. Code § 545.453).

- Prohibit automated motor vehicles from operating if they are incapable of operating in compliance with state traffic and motor vehicle laws, are not equipped with manufacturer-installed recording devices and federally compliant automated driving systems, not registered and titled in the state, or insured (Tex. Transp. Code § 545.454).
- Require automated motor vehicles to comply with existing state law regarding accidents and reporting of accidents (Tex. Transp. Code § 545.455).
- Permit automated vehicle owners to identify them as such to the state (Tex. Transp. Code § 545.456).

The bill also expressly prohibited political subdivisions and state agencies from "impos[ing] a franchise or other regulation related to the operation of an automated motor vehicle or automated driving system" (Tex. Transp. Code § 545.452).

In 2021, during the 87th Legislative Session, the Texas Legislature passed House Bill (H.B.) 3026. The bill amended the Texas Transportation Code to exempt "automated motor vehicles" from:

- State motor vehicle equipment laws and regulations that support human operation of vehicles or are not relevant to automated driving systems.
- Required vehicle safety inspections with respect to any equipment (Tex. Transp. Code § 547.618).

In 2021, the legislature also passed H.B. 1791, which permitted "platooning" of connected vehicles on Texas roadways. Platooning, under the new statute, occurs when "an operator of a vehicle equipped with a connected braking system that is following another vehicle equipped with that system may be assisted by the system to maintain an assured clear distance or sufficient space" (Tex. Transp. Code § 545.062[d]).

Whether these provisions conflict with or support federal CAV authority has not yet been adjudicated. Thus far, federal ADS safety standards have not been promulgated, so under Texas Transportation Code § 545.454, automated motor vehicles are allowed to operate in Texas so long as they are capable of operating in compliance with state traffic and motor vehicle laws, equipped with manufacturer-installed recording devices, registered and titled in the state, and insured.

In addition, under Texas Transportation Code § 547.618, automated vehicles are assumed to have passed state safety inspections, as long as they are not a trailer, semitrailer, pole trailer, or mobile home, and equipped with ADS designed to be operated exclusively by the ADS for all trips. This may come in conflict with federal regulations in the future, so it is an issue that TxDOT may consider staying apprised of and comment on when federal regulations are proposed.

Another issue that warrants monitoring is the procedure for reporting crashes. Under Texas law, protocols around crashes involving automated motor vehicles must conform with existing required procedures under Chapter 550 of the Texas Transportation Code. Tex. Transp. Code § 545.455. However, NHTSA's Standing General Order Update, issued in June 2021 and amended in August 2021, creates a three-year reporting obligation for named manufacturers, developers, and operators of Level 2 ADAS and Levels 3 through 5 ADS in which covered crashes must be reported within 10 days of the incident (National Highway Traffic Safety Administration, 2022).

Thus, owners of automated motor vehicles in Texas must comply with two parallel requirements for accident reporting. This is another issue that TxDOT may consider commenting on should proposed federal regulations impinge on state safety requirements.

Data Use, Protection, and Privacy

The potential collection, storing, sharing, selling, disclosure, and maintenance of data by government agencies to support CAV technology deployments and government operations raises legal questions about a state agency's liability surrounding data protection and privacy, specifically as it relates to proprietary data and trade secrets, products liability, and privacy and PIA laws. Specific legal questions vary depending on the type of data at issue (e.g., location data, photographic data, and vehicle telematics), how the data are stored and processed, and how an agency plans to share the data with others (e.g., by sharing, selling, or incorporating the data into a free, open, publicly available database for use by road users or other third parties).

Products Liability

Table 12 summarizes state statutes regarding products liability. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 12. State Statutes Related to Product Liability.

Statute/Case	Rule	Citation
Tex. Civ. Prac. & Rem. Code	For liability to attach, products liability law requires proof "by a preponderance of the evidence that: (1) there was a safer alternative design; and (2) the defect was a producing cause of the personal injury, property damage, or death for which the claimant seeks recovery."	Tex. Civ. Prac. & Rem. Code § 82.002(a)
Tex. Civ. Prac. & Rem. Code	"Safer alternative design" is a product design that "in reasonable probability" meets two criteria: (1) it "would have prevented or significantly reduced the risk of the claimant's personal injury, property damage, or death without substantially impairing the product's utility;" (2) the unused design must have been "economically and technologically feasible at the time the product left the control of the manufacturer or seller by the application of existing or reasonably achievable scientific knowledge."	Tex. Civ. Prac. & Rem. Code § 82.005

Statute/Case	Rule	Citation
Tex. Civ. Prac. & Rem. Code	Texas law provides for a "rebuttable presumption" that manufacturers and sellers are not liable for any injury caused by "some aspect of the formulation, labeling, or design of a product" so long as they can prove: (1) compliance with federal standards such that the formula, labeling, or design complied with "mandatory federal safety standards or regulations that were adopted and promulgated at the time of production;" or (2) the product was granted licensing or approval by a federal authority.	Tex. Civ. Prac. & Rem. Code § 82.008
Tex. Civ. Prac. & Rem. Code	Manufacturers are required to indemnify sellers against losses arising out of product liability actions, except for any loss caused by the seller's negligence, intentional misconduct, or other act or omission for which the seller is independently liable.	Tex. Civ. Prac. & Rem. Code § 82.002(b)
Tex. Civ. Prac. & Rem. Code	Sellers are not liable for harm a product causes unless they participated in the design, altered the product, installed the product, had substantial control of the product, made an express factual representation about the product, or knew the product had a defect.	Tex. Civ. Prac. & Rem. Code § 82.003

New legal issues of products liability could arise from several hypothetical situations TxDOT may encounter through CAV deployments. TxDOT may use data, either directly collected or acquired from a third party, to produce and sell a product (e.g., a digital map) for use by CAVs. Liability could attach if that product is not updated to notify vehicles of premises defects, special defects, roadway design changes, work zones, or closed roadways. TxDOT could also be the owner of a CAV that relies on potentially defective data products and is involved in an injury or death.

Texas's products liability law, codified in Title 4 of the Tex. Civ. Prac. & Rem. Code, is relatively friendly to manufacturers and sellers, encouraging the placing of products and component parts thereof into the stream of commerce. The law burdens plaintiffs by requiring proof "by a preponderance of the evidence that: (1) there was a safer alternative design; and (2) the defect was a producing cause of the personal injury, property damage, or death for which the claimant seeks recovery" (Tex. Civ. Prac. & Rem. Code § 82.002[a]). The law defines "safer alternative design" as a product design that "in reasonable probability" meets two criteria. First, it "would have prevented or significantly reduced the risk of the claimant's personal injury, property damage, or death without substantially impairing the product's utility." Second, the unused design must have been "economically and technologically feasible at the time the product left the control of the manufacturer or seller by the application of existing or reasonably achievable scientific knowledge" (Tex. Civ. Prac. & Rem. Code § 82.005).

Another advantage provided by Texas' products liability law to manufacturers and sellers is a "rebuttable presumption" that they are not liable for any injury caused by "some aspect of the formulation, labeling, or

design of a product" so long as they can prove: (1) compliance with federal standards such that the formula, labeling, or design complied with "mandatory federal safety standards or regulations that were adopted and promulgated at the time of production;" or (2) the product was granted licensing or approval by a federal authority (Tex. Civ. Prac. & Rem. Code § 82.008).

Sellers of defective products or components are also protected through two provisions of the state products liability law. First, manufacturers are required to indemnify sellers against losses arising out of product liability actions, except for any loss caused by the seller's negligence, intentional misconduct, or other act or omission for which the seller is independently liable (Tex. Civ. Prac. & Rem. Code § 82.002[b]). Second, sellers are not liable for harm a product causes unless they participated in the design, altered the product, installed the product, had substantial control of the product, made an express factual representation about the product, or knew the product had a defect (Tex. Civ. Prac. & Rem. Code § 82.003).

If TxDOT produces a data product (e.g., a digital map) for use in a CAV, it may effectively make the agency a manufacturer of a product and expose the agency to tort liability for product-related injuries. Similarly, legal issues may arise from data product updates. If TxDOT implements updates to the products it produces, implementing the updates remotely using automatic update notifications, it may be responsible for ensuring that it (or a third party) pushing out those notifications use secure networks for file upload and download. If the data product updates fail to reach a particular CAV or the updates are not consistent with current roadway conditions, TxDOT could potentially be exposed to liability if a crash occurs because the data were inconsistent with actual conditions that the CAV encountered. This liability may be similar to those involved with traffic signal data, which some state DOTs provide to third-party automobile manufacturers for a variety of applications. Signal timing is periodically updated, and the signal data, if not properly conveyed to users without appropriate warnings and notifications, leave these agencies legally exposed.

Working to TxDOT's advantage, however, is Texas' products liability law, which provides relatively more legal protections to manufacturers and sellers than the products liability laws of other states. Plaintiffs would have the burden of proving the product's design is defective by asserting a safer alternative design and direct causation between the product and the claimed injury, death, or property damage. Plaintiffs would also be challenged by the rebuttable presumption that TxDOT, as a manufacturer and/or seller, complied with federal standards or was granted federal approval. If TxDOT does not produce but rather sells a data or digital product for use in CAVs, it would benefit from the manufacturer's indemnification and the presumption that it is not liable for harm caused by products for which it was not involved in the manufacturing or knew was defective.

If TxDOT is an owner of a CAV (or fleet of CAVs) that utilizes defective data products and causes injury or death, the agency would be in the opposite disadvantaged position, having to pursue the manufacturer for liability and damages. If the seller took part in the manufacturing of the vehicle or knew of the defect, they could be pursued for liability too.

Proprietary Data and Trade Secrets

Table 13 summarizes the case law and statutes regarding proprietary data and trade secrets. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 13. Case Law and Statutes Related to Proprietary Data and Trade Secrets.

Statute/Case	Rule	Citation
Texas Government Code (Tex. Gov't. Code)	Each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees.	Tex. Gov't. Code § 552.001
Tex. Gov't. Code	A Texas agency is required, upon a request for public information, to promptly produce the information for inspection, duplication, or both. "Public information" is defined as any information that, "under a law or ordinance or in connection with the transaction of official business" is "written, produced, collected, assembled, or maintained" by or for a governmental unit where the governmental body owns the information or has a right of access to it.	Tex. Gov't. Code § 552.002(a)
Tex. Gov't. Code	"Public information" pertains to "electronic communication created, transmitted, received, or maintained on any device if the communication is in connection with the transaction of official business."	Tex. Gov't. Code § 552.002(a-2)
Tex. Gov't. Code	Whether electronic or not, public information can take the form of a book, paper, letter, document, e-mail, Internet posting, text message, instant message, other electronic communication, printout, photograph, film, tape, microfiche, microfilm, photostat, sound recording, map, and drawing and a voice, data, or video representation held in computer memory.	Tex. Gov't. Code § 552.002(c)
Tex. Gov't. Code	Public information subject to disclosure includes: • Completed reports, audits, evaluations, or investigations made of, for, or by a governmental body. • Account, voucher, or contract information related to the receipt or expenditure of funds by a government body. • Working papers, research material, and information used to estimate the need for or expenditure of public funds or taxes by a governmental body. • Policy statements that have been adopted or issued by an agency. • Information deemed open to the public under an agency's policies.	Tex. Gov't. Code § 552.022

Statute/Case	Rule	Citation
Tex. Gov't. Code	Contracting information is deemed public under the law and is subject to disclosure with many contract terms not protected by the PIA's general protections of certain information.	Tex. Gov't. Code § 552.0222
Tex. Gov't. Code	Trade secrets are exempt from disclosure and include: business, scientific, technical, economic, or engineering information and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or however stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing. Trade secrets are those that possess "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."	Tex. Gov't. Code § 552.110
Tex. Gov't. Code	Proprietary information is exempt from disclosure and is information that vendors and contractors submit to governmental bodies in bids, proposals, or qualifications that meet two criteria: (1) they "reveal an individual approach to: (A) work; (B) organizational structure; (C) staffing; (D) internal operations; (E) processes; or (F)…pricing information that will be used in future solicitation or bid documents;" and (2) advantage a competitor.	Tex. Gov't. Code § 552.1101
Tex. Gov't. Code	Information deemed confidential by law is exempt from disclosure.	Tex. Gov't. Code § 552.101
In re the City of Georgetown	Information made confidential under the Texas Rules of Civil Procedure and Rules of Evidence is exempt from disclosure.	53 S.W.3d 328 (Tex. 2001)
Tex. Gov't. Code	Motor vehicle inspection records are exempt from disclosure.	Tex. Gov't. Code § 552.129
Tex. Gov't. Code	Motor vehicle records such as driver's licenses or permits, motor vehicle titles or registrations, and personal identification documents issued by any state or local agency are exempt from disclosure.	Tex. Gov't. Code § 552.130

Statute/Case	Rule	Citation
Tex. Gov't. Code	Government information related to computer network security, including vulnerability reports and assessments, is exempt from disclosure.	Tex. Gov't. Code § 552.139
Texas Department of Public Safety v. Cox Texas Newspapers, L.P	Information that, if disclosed, would create a substantial threat of physical harm is exempt from disclosure.	343 S.W.3d 112 (Tex. 2011)
City of Garland v. Dallas Morning News	Agency communications or parts of agency communications that are deliberative relating to agency policymaking are exempt from disclosure.	22 S.W.3d 351 (Tex. 2000)

A state agency's intended and unintended use of data from a vendor will be governed in part by torts law as well as contract law and the state's PIA. Laws governing tort liability will be triggered if the agency discloses CAV data containing trade secrets where the agency could be held liable for the tort of appropriation if they use the information for the value associated with it, the information could be identified from the disclosure, and the disclosing party benefits from or was advantaged by the disclosure (*Matthews v. Wozencraft*, 15 F.3d 432 [5th Cir. 1994]; *Henley v. Dillard Dept. Stores*, 46 F.Supp.2d 587 [N.D. Tex. 1999]).

The sharing and distribution of CAV data could also be affected by contract law and the rights that may be enumerated in agreements with data providers that transfer rights or provide a license to use the data. Agencies interested in sharing such data from third parties with other external stakeholders, regardless of any fee or charge, must refer to use provisions outlined in purchase or licensing agreements (Canton, 2021).

A third way to determine the level of protection for third parties' proprietary information and trade secrets can also be determined by a state's PIA, which under Texas law exempts such information from disclosure. Codified in Chapter 552 of the Texas Government Code, the Texas PIA obligates the government to make public information reasonably available to those who request it but allows for exceptions and confidentiality under certain circumstances. Agencies like TxDOT are subject to this law, which is constructed liberally based on the express policy that "each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees" (Tex. Gov't. Code § 552.001).

State agencies in Texas are required, upon a request for public information, to promptly produce the information for inspection, duplication, or both, where "public information" is defined as any information that "under a law or ordinance or in connection with the transaction of official business" is "written, produced, collected, assembled, or maintained" by or for a governmental unit where the governmental body owns the information or has a right of access to it (Tex. Gov't. Code § 552.002[a]). The legal definition of "public

information" pertains to "electronic communication created, transmitted, received, or maintained on any device if the communication is in connection with the transaction of official business" (Tex. Gov't. Code § 552.002[a-2]). Whether electronic or not, public information can take the form of the following:

> [A] book, paper, letter, document, e-mail, Internet posting, text message, instant message, other electronic communication, printout, photograph, film, tape, microfiche, microfilm, photostat, sound recording, map, and drawing and a voice, data, or video representation held in computer memory (Tex. Gov't. Code § 552.002[c]).

The PIA specifies types of public information that are subject to disclosure, including:

- Completed reports, audits, evaluations, or investigations made of, for, or by a governmental body.
- Account, voucher, or contract information related to the receipt or expenditure of funds by a government body.
- Working papers, research material, and information used to estimate the need for or expenditure of public funds or taxes by a governmental body.
- Policy statements that have been adopted or issued by an agency.
- Information deemed open to the public under an agency's policies (Tex. Gov't. Code § 552.022).

Contracting information is deemed public under the law and is subject to disclosure with many contract terms not protected by the PIA's general protections of certain information (Tex. Gov't. Code § 552.0222). These protections provided by the PIA generally exempt what are considered "trade secrets" and "proprietary information" from disclosure. "Trade secrets" include:

> [B]usiness, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or however stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing. (Tex. Gov't. Code § 552.110).

Information that qualifies as "trade secrets" are those that possess "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information" (Tex. Gov't. Code § 552.110).

"Proprietary information" is information that vendors and contractors submit to governmental bodies in bids, proposals, or qualifications that meet two criteria: (1) they "reveal an individual approach to: (A) work; (B) organizational structure; (C) staffing; (D) internal operations; (E) processes; or (F)…pricing information that will be used in future solicitation or bid documents;" and (2) advantage a competitor (Tex. Gov't. Code § 552.1101).

Other exceptions to the Texas PIA that protect information from disclosure include:

- Information deemed confidential by law, including those made confidential under the Texas Rules of Civil Procedure and Rules of Evidence (Tex. Gov't. Code § 552.101; *In re the City of Georgetown*, 53 S.W.3d 328 [Tex. 2001]).
- Motor vehicle inspection records (Tex. Gov't. Code § 552.129).

- Motor vehicle records such as driver's licenses or permits, motor vehicle titles or registrations, and personal identification documents issued by any state or local agency (Tex. Gov't. Code § 552.130).
- Government information related to computer network security, including vulnerability reports and assessments (Tex. Gov't. Code § 552.139).
- Information that, if disclosed, would create a substantial threat of physical harm (*Texas Department of Public Safety v. Cox Texas Newspapers, L.P.*, 343 S.W.3d 112 [Tex. 2011]).
- Agency communications or parts of agency communications that are deliberative relating to agency policymaking (*City of Garland v. Dallas Morning News*, 22 S.W.3d 351 [Tex. 2000]).

Taking these provisions of the PIA into account, TxDOT may consider evaluating the nature and purpose of the data it acquires, stores, and uses to protect certain information from disclosure. Under the PIA, electronic data are considered public information and, therefore, subject to disclosure when they take the form of electronic communications, maps, and data representation held in computer memory. However, the data may be exempt from disclosure if they can qualify as "trade secrets" or include information that are already exempted under the PIA. Thus, TxDOT may consider evaluating data it possesses or wishes to acquire and also consider preventing such data from disclosure based on whether the data have "independent economic value, actual or potential" from being unknown and unascertainable or can fall under existing exceptions.

The PIA is unclear, however, as to whether data stored in the cloud and other types of data and datasets that may potentially be used by CAVs will be subject to disclosure. For example, photographic data might contain images of a person's face and could, if not properly scrubbed or protected, be deemed public information under the PIA, disclosed, and result in an invasion of that person's individual privacy. Location data and vehicle data, even if anonymized, could be layered with other datasets, resulting in the re-identification of someone's personal data (which does not fall within existing exceptions under the PIA). Therefore, to limit these risks, TxDOT could discuss with the legislature the idea of amending the PIA to protect third party and TxDOT data stored in the cloud and/or data revealing personally identifiable information (PII).

Regardless of whether data are collected directly by transportation departments or purchased from third-party data owners, the processes for acquiring and processing those data would benefit from review and development of a framework and set of protocols for managing and protecting data (Jones Day, 2021). These actions would minimize liability for the transportation agency, protect the privacy interests of those whose PII may be captured in the aggregated data, and protect the proprietary interests of those whose technology and business systems were used to manufacture and generate the data.

Data Management

Table 14 summarizes the statutes governing data management in Texas. In the discussion below, these laws are also applied hypothetically to the legal topic issues identified as the focus of this project.

Table 14. Statutes Governing Data Management in Texas.

Statute/Case	Rule	Citation
Tex. Transp. Code	Government agencies may only disclose personal information to those who are the subject of the information or with their consent, or for specific uses.	Tex. Transp. Code §§ 730.006, 730.007
Tex. Transp. Code	Government agencies may not sell personal information to anyone not authorized to receive it, exposing sellers of personal information to an unauthorized recipient to civil liability.	Tex. Transp. Code §§ 730.0122, 730.0123
Tex. Transp. Code	Government agencies must include in contracts with authorized third parties for personal information provisions covering cybersecurity, compliance, and reporting requirements.	Tex. Transp. Code § 730.014
Tex. Gov't. Code	Government agencies must designate a data management officer to establish an agency data governance program and post on the Texas Open Data Portal at least three high-value data sets.	Tex. Gov't. Code § 2054.137
Tex. Gov't. Code	Government agencies must include in contracts with vendors authorized to access, transmit, use, or store data for the agency a provision requiring the vendor to meet the agency's security controls and provide evidence that they meet the security controls.	Tex. Gov't. Code § 2054.138
Tex. Gov't. Code	Government agencies must require vendors to provide cloud computing services for the agency, demonstrate compliance with program requirements, and maintain program compliance and certification throughout the term of the contract.	Tex. Gov't. Code § 2062.002
Tex. Gov't. Code	Government agencies are prohibited from acquiring, retaining, and disseminating "information that alone or in conjunction with other information identifies an individual or the individual's location" without the individual's written or electronic consent, unless required or permitted by federal or state law (other than the PIA) or for law enforcement purposes.	Tex. Gov't. Code § 2062.002

Texas state law codifies data management and disclosure limitations to protect private information that TxDOT, as well as its data vendors, must follow. In 2021, the Texas State Legislature enacted SB 15/HB 3471, also known as the Texas Consumer Privacy Act Phase I, which amends the Texas Transportation Code to "restrict disclosure of personal information to essential government agencies, and forbids personal information from redisclosure or resale to private entities such as marketing and technology companies" (Texas State Legislature, 2021). Specifically, the law provides that government agencies:

- Only disclose personal information (i.e., information identifying a person, including photos, social security number, date of birth, driver identification number, name, address, email address, and medical or disability information) to those who are the subject of the information or with their consent, or for specific uses (Tex. Transp. Code §§ 730.006, 730.007).
- Never sell personal information to anyone not authorized to receive it, exposing sellers of personal information to an unauthorized recipient to civil liability (Tex. Transp. Code §§ 730.0122, 730.0123).
- Include in contracts with authorized third parties for personal information provisions covering cybersecurity, compliance, and reporting requirements (Tex. Transp. Code § 730.014).

In 2021, the Texas State Legislature also enacted SB 475 to establish state agency data management requirements and procedures. The bill requires agencies, including TxDOT, to:

- Designate a data management officer to, among other things, establish an agency data governance program and post on the Texas Open Data Portal at least three high-value data sets (Tex. Gov't. Code § 2054.137).
- Include in contracts with vendors authorized to access, transmit, use, or store data for the agency a provision requiring the vendor to meet the agency's security controls and provide evidence that they meet the security controls (Tex. Gov't. Code § 2054.138).
- Require vendors to provide cloud computing services for the agency to comply with the requirements of the state risk and authorization management program, demonstrate compliance with program requirements, and maintain program compliance and certification throughout the term of the contract.
- Prohibit acquiring, retaining, and disseminating "information that alone or in conjunction with other information identifies an individual or the individual's location" without the individual's written or electronic consent, unless required or permitted by federal or state law (other than the PIA) or for law enforcement purposes (Tex. Gov't. Code § 2062.002).

With these new requirements and prohibitions related to personal information and data security, TxDOT will need to include additional provisions in its contracts and develop policies and procedures to mitigate disclosure and capture individual authorizations and consent. The new section of the Texas Government Code requiring state agencies to obtain the written or electronic consent of an individual before acquiring, retaining, or disseminating information that identifies the individual or their location through the use of global positioning system technology, individual contact tracing, or technology designed to obtain biometric identifiers (i.e., a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry) should be noted since it is the agency's obligation, and not the agency's vendor, collaborator, or other third party, to obtain the consent from individuals before collecting the data. If a vendor will be collecting location data on behalf of TxDOT, TxDOT may need to make the vendor aware of this obligation so that they can put in place a mechanism to acquire consent. For example, the vendor's platform can be set up to obtain and store the consent from individuals on behalf of TxDOT, which should also develop a standard consent form for the collection of this data.

Insurance

Table 15 summarizes the statutes and case law regarding insurance. In the discussion below, these laws are applied hypothetically to the legal topic issues identified as the focus of this project.

Table 15. Case Law and Statutes Related to Insurance.

Statute/Case	Rule	Citation
Tex. Transp. Code	CAVs are not permitted to operate on the state's highways unless they are "covered by motor vehicle liability coverage or self-insurance in an amount equal to the amount of coverage that is required under the laws of this state."	Tex. Transp. Code §545.454(b)(5)
Tex. Civ. Prac. & Rem. Code	Governmental units are allowed to purchase insurance policies protecting the unit and employees against torts claims and relinquish to the insurer the right to investigate, defend, compromise, and settle any claim.	Tex. Civ. Prac. & Rem. Code § 101.027
Tex. Civ. Prac. & Rem. Code	Neither the existence, nor the amount of insurance held by a governmental unit is admissible in trial in a suit against the governmental unit.	Tex. Civ. Prac. & Rem. Code § 101.104
In re Sabine Valley Ctr.	State statutes prohibit discovery of insurance covering claims against a governmental unit and against its employees for which it can be directly or vicariously liable under the TTCA.	986 S.W.2d 612 (Tex. 1999)
Jefferson County, Texas v. Ellarene Farris	A governmental unit that provides workers' compensation is immune from liability and likewise immune from suit.	569 S.W.3d 814 (Tex. App. 2018)

If TxDOT were to operate CAVs, it would be required to obtain insurance to cover its liability. Automated motor vehicles are already required to carry insurance under state law. CAVs are not permitted to operate on the state's highways unless they are "covered by motor vehicle liability coverage or self-insurance in an amount equal to the amount of coverage that is required under the laws of this state" (Tex. Transp. Code § 545.454[b][5]). Under the TTCA, governmental units are allowed to purchase insurance policies protecting the unit and employees against torts claims and relinquish to the insurer the right to investigate, defend, compromise, and settle any claim (Tex. Civ. Prac. & Rem. Code § 101.027). Neither the existence, nor the amount of insurance held by a governmental unit is admissible in trial in a suit against the governmental unit (Tex. Civ. Prac. & Rem. Code § 101.104). The Texas Supreme Court has also held that state statutes prohibit discovery of insurance covering claims against a governmental unit and against its employees for which it can be directly or vicariously liable under the TTCA (*In re Sabine Valley Ctr.*, 986 S.W.2d 612 [Tex. 1999]).

With regard to workers compensation, the Texas Supreme Court has held that a governmental unit that is immune from liability by having provided workers' compensation is likewise immune from suit. The TTCA expressly applies privileges and immunities granted by workers' compensation laws to governmental units (*Jefferson County, Texas v. Ellarene Farris*, 569 S.W.3d 814 [Tex. App. 2018]). Thus, TxDOT would be immune

from liability under a workers compensation claim if an employee were injured or died as a result of their operation of a CAV in the course of employment.

Federal Law Analysis

The year 2016 marked the start of the U.S. federal government's increased focus on the development and integration of CAVs into the nation's transportation system. USDOT began issuing iterative policy guidance applicable to all CAV use cases and regulatory agencies including NHTSA, FMCSA, and FHWA and seeking input on policies associated with the deployment of CAVs.

The U.S. Congress also saw legislative action on this topic. In 2017, the Senate introduced S. 1885, the AV START Act, and the House introduced H.R. 3388, the SELF DRIVE Act. Neither bill, however, became law. The House bill has been re-introduced, but to date there has been no further action.

Recently, there seems to be renewed interest and momentum on federal CAV legislation from both chambers of Congress, including hearings that have included the themes of safety, workforce, and local coordination. However, to date, there has been no meaningful, enacted legislative action. In the absence of Congressional action, USDOT has taken a role in promulgating federal regulatory action across its agencies. However, without enabling federal legislation, such regulations face legal scrutiny. Also, federal regulations may lead to preemption questions for existing state statutes if statutes are determined to conflict with existing and accepted federal jurisdiction over vehicle safety standards.

The following tables provide a summary of activity from agencies within USDOT focused on CAVs, along with a succinct federal legislative snapshot. Such agency actions provide an important opportunity for tracking potential federal regulations, concerns from industry, and topics of interest from other state DOTs. Table 16 provides a summary of federal rulemaking, while Table 17 summarizes non-rulemaking actions.

Table 16. Federal Rulemaking Overview.

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
Vehicle Size and Weight	FHWA	Anticipated Notice of Proposed Rulemaking (ANPRM)— July 2022	This rulemaking would amend FHWA's regulations in 23 CFR 657 and 658.	This is important to track because ADS sensors extend beyond the maximum allowable width limit and may impact state DOT infrastructure planning and decision making.	Spring 2022 Unified Agenda
Work Zones	FHWA	ANPRM—August 2022	This rulemaking would amend the regulations in 23 CFR part 630, subparts J (Work Zone Safety and Mobility) and K (Temporary Traffic Control Devices).	This is important to track because this rulemaking will be how ADS developers certify safe vehicular interactions with work zones.	Spring 2022 Unified Agenda
Manual on Uniform Traffic Control Devices (MUTCD)	FHWA	Required Final Rule May 2023	This rulemaking would update the MUTCD. The new edition will update the technical provisions of the 2009 edition to reflect	This is important to track in consideration of roadway design and markings and best practices compliance	Spring 2022 Unified Agenda

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
			advances in technologies and operational practices that are not currently allowed in the MUTCD.	in consideration of potential liability.	
Human Factors Considerations in Commercial Motor Vehicle Automated Driving Systems and Advanced Driver Assistance Systems	FMCSA	ANRPM—June 2023	FMCSA announced its plan to submit an Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and approval. The notice invited comments on a proposed information collection titled "Human Factors Considerations in Commercial Motor Vehicle Automated Driving Systems and Advanced Driver Assistance Systems", a driving simulator study with a series of	Approximately 100 CMV drivers will participate in the study, which will examine the effect of non-driving secondary task engagement, transfer of control, and training on driver behavior in CMVs equipped with ADAS and ADS.	Published in Federal Register on June 23, 2023

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
			questionnaires that will evaluate how commercial motor vehicle drivers engage in trucks equipped with SAE International Level 2 ADAS and Level 3 ADS.		
Safety Impacts of Human-Automated Driving System (ADS) Team Driving Applications	FMCSA	ANRPM—June 2023	FMCSA announced its plan to submit the Information Collection Request (ICR) to the Office of Management and Budget (OMB) for its review and approval and invites public comment. This notice invited comments on a proposed information collection titled “Safety Impacts of Human-Automated Driving System (ADS) Team Driving Applications," a driving simulator study	The study will focus on team driving applications with an SAE Level 4 vehicle. Approximately 80 drivers will participate in the study to assess the safety benefits and disbenefits of human-ADS team driving applications and support the analysis of potential requests for relief from FMCSA's hours-of-service (HOS) regulations.	Published in Federal Register on June 8, 2023

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
			with a series of questionnaires, which will quantify the safety implications of team driving applications between humans and ADS-equipped commercial motor vehicles.		
Safe Integration of ADS-Equipped Commercial Motor Vehicles	FMCSA	Supplemental ANPRM—February 2023 (Comments due March 2023)	FMCSA proposes to amend certain Federal Motor Carrier Safety Regulations (FMCSRs) to ensure the safe introduction of ADS-equipped commercial motor vehicles onto the nation's roadways. FMCSA originally published an ANPRM in May 2019, seeking comments on FMCSRs that may need to be amended, revised, or eliminated to facilitate	This is critically important to track since it would be the agency's most comprehensive—and preemptive—action on ADS-equipped commercial motor vehicles to date. With the supplemental ANPRM, FMCSA continued to consider amendments to the FMCSRs to ensure the safe integration of ADS-equipped CMVs	Published in Federal Register on February 1, 2023.

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
			the safe introduction of ADS-equipped CMVs onto the Nation's roadways.	into interstate motor carriers' operations and request additional information.	
Electronic Logging Device (ELD) Revisions	FMCSA	ANPRM—August 2022	FMCSA is seeking information to determine what changes to ELD regulations would be warranted.	This is important for state DOTs to track given current ELD enforcement duties maintained by state highway patrol officers.	Spring 2022 Unified Agenda
Unique Electronic Identification of CMVs	FMCSA	ANPRM—Nov 2022	FMCSA requests public comment on potential amendments to the FMCSR to require every CMV operating in interstate commerce to be equipped with an electronic device capable of communicating a unique identification number when queried by a roadside system.	This is important to track because this could also serve to identify Level 4 CMVs operating on the roads.	Spring 2022 Unified Agenda

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
Standing General Order 2021-01 | Incident Reporting for Automated Driving Systems and Level 2 Advanced Driver Assistance Systems	NHTSA	Issued in June 2021	NHTSA's General Order requires manufacturers and operators to report crashes involving vehicles equipped with ADS or SAE Level 2 ADAS. With these data, NHTSA can respond to crashes that raise safety concerns about ADS and Level 2 ADAS technologies through further investigation and enforcement. If NHTSA finds a safety defect, it will take action to ensure that unsafe vehicles are taken off public roads or remedied. Entities named in the General Order must report a crash if ADS was in use at any time within 30 seconds of the crash	NHTSA issued the General Order in June 2021 to evaluate whether the manufacturers of ADS and Level 2 ADAS systems and the vehicles equipped with them, are meeting their statutory obligations to ensure that their vehicles and equipment are free of defects that pose unreasonable risks to motor vehicle safety. Prior to the implementation of the General Order, NHTSA's sources of timely crash notifications were limited and generally inconsistent across manufacturers.	Amended in April 2023

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
			and the crash resulted in property damage or injury, or if Level 2 ADAS was in use at any time within 30 seconds of the crash and the crash involved a vulnerable road user or resulted in a fatality, a vehicle tow-away, an air bag deployment, or any individual being transported to a hospital for medical treatment.		
Occupant Protection for Vehicles with ADS	NHTSA	Final	This final rule makes clear that, despite their innovative designs, vehicles with ADS technology must continue to provide the same high levels of occupant protection that current passenger vehicles provide. This	This is important because it is an update to the FMVSS specifically for ADS-equipped passenger vehicles and is one of the first final federal rules related to CAVs.	Published March 30, 2022

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
			final rule is limited to the crashworthiness standards to provide a unified set of regulatory text applicable to vehicles with and without ADS functionality.		
Facilitating New ADS Vehicle Designs for Crash Avoidance Testing	NHTSA	ANPRM—May 2019 (comments due August 2019)	This notice sought comment on crash avoidance test procedures to facilitate the safe introduction and certification of new vehicle designs equipped with ADS.	This is important given its potential impact on FMVSS and those requirements for ADS vehicles.	Spring 2022 Unified Agenda
Alternative Options for Rearview Mirrors	NHTSA	ANPRM—October 2019 (comments due December 2019)	This notice sought public comment on the safety standard for rear visibility to facilitate new designs regarding the introduction and certification of	This is important to track to see what determinations are made around whether cameras are sufficient replacements or augmenting tools for traditional mirrors.	Spring 2022 Unified Agenda

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
			cameras replacing rearview mirrors.		
Framework for ADS Safety	NHTSA	ANPRM—December 2020 (comments due April 2021)	This ANPRM requested comments on the development of a framework for ADS safety.	This is extremely relevant to state DOTs depending on scale and sophistication of eventual rulemaking.	Spring 2022 Unified Agenda
Updating Event Data Recorders (EDR) Standard	NHTSA	ANPRM--June 2022	In accordance with the 2015 FAST Act, this rulemaking proposes to amend 49 CFR part 563, to update the current pre-crash recording duration for motor vehicles equipped with EDRs. For motor vehicles equipped with an EDR, the current regulation requires a 5 second pre-crash recording period at a frequency rate of 2 cycles/second (Hz).	This is extremely relevant for all ADS vehicles and enforcement personnel, given the implication on insurance/liability.	Spring 2022 Unified Agenda

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
Passenger-Less Delivery Vehicles Equipped With ADS	NHTSA	2018 ANPRM, "deleted at agency request" in 2021	The agency published a Federal Register notice on January 18, 2018, requesting comment on existing regulatory barriers that may block the introduction and certification of ADS-equipped vehicles, particularly those without human controls and purpose-built for goods movement.	While action on this rulemaking has been halted for the time being, this is an important issue for state DOTs to track since such vehicles do not fit neatly into existing motor vehicle laws.	Fall 2019 Unified Agenda
Pilot Program for Collaborative Research on Motor Vehicles With High or Full Driving Automation	NHTSA	2018 ANPRM, agency withdrew in 2021	NHTSA withdrew this rulemaking. Based on further agency analysis, the proposals discussed in the ANPRM may be considered in a NHTSA rulemaking titled "Expansion of Temporary Exemption	This is important for state DOTs to note so as to indicate changing federal agency priorities related to CAVs. Additionally, appropriate terminology for ADS vehicles has evolved, and regulatory actions	Spring 2022 Unified Agenda

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
			Program to Domestic Manufacturers for Research, Demonstrations, and Other Purposes."	would no longer use the phrase "high or full automation." It is critical that future government action on CAVs use accurate language.	
Expansion of Temporary Exemption Program to Domestic Manufacturers for Research, Demonstrations, and Other Purposes	NHTSA	ANPRM--Oct 2022	In 2020, NHTSA announced its plan to publish an Interim Final Rule (IFR) to set a new regulation allowing entities to request exemptions to operate nonconforming vehicles, on public roads for purposes of research, investigations, demonstrations, training, competitive racing events, show, or display, but not sale or lease. NHTSA is now	This is important for state DOTs to track given the potential of novel vehicle types operating on public roadways, including potential liability and safety considerations.	Spring 2022 Unified Agenda

Name	Issuing Agency	Rule Status	Description	Why It Matters	Last Updated
			developing a NPRM instead of the IFR.		

Table 17. Non-rulemaking Federal Regulatory Actions.

Title	Description	Why it matters	Date(s) of interest
Exemption Application From Waymo LLC, and Aurora Operations, Inc.	FMCSA published a notice announcing an application from Waymo LLC and Aurora Operations, Inc. for a 5-year exemption from the required placement of warning devices around stopped commercial motor vehicles; the requirement that lamps for warning devices be steady-burning; and to allow use of a warning device for stopped vehicles not currently allowed by Agency rules.	This application was filed by Waymo and Aurora on behalf of a class of motor carriers operating ADS equipped CMVs (i.e., it is not limited to Waymo or Aurora).	Posted to the Federal Register on March 9, 2023. Comments due April 2023.
General Motors (GM)-Receipt of Petition for Temporary Exemption From Various Requirements of the FMVSS for an ADS-Equipped Vehicle	On February 17, 2022, GM submitted a petition for exemption for its Origin vehicle, which GM states is a multipurpose passenger vehicle equipped with a "Level 4 ADS." This document notifies the public that NHTSA has received from GM a petition for a temporary exemption from portions of six FMVSS. GM requests a two-year exemption, during which it seeks to be allowed to manufacture not more than 2,500	This is important for state DOTs to track given the potential of novel GM vehicles operating on public roadways and the impact of those vehicles on enforcement personnel. Additionally, the agency response to this petition will be important to analyze for signs of interest, engagement, and knowledge on behalf of federal regulators and what that might mean for future action, including updates to FMVSS.	Posted to the Federal Register in July 2021. Comments due August 2022.

Title	Description	Why it matters	Date(s) of interest
	exempted vehicles for each 12-month period covered by the exemption.		
Ford Motor Company-Receipt of Petition for Temporary Exemption From Various Requirements of the FMVSS for an ADS-Equipped Vehicle	In July 2021, Ford submitted an exemption petition under 49 CFR part 555 for a vehicle equipped with an SAE International Level 4 ADS that can be operated in either a human-driven mode (Manual Mode), or in an ADS-driven mode (AV Mode). Ford states that it is seeking an exemption from portions of seven FMVSS to allow for the controlled deployment and usage of the vehicle "on tested, proven roadways during appropriate weather conditions." Ford also states that no more than 2,500 exempted vehicles will be produced and introduced into interstate commerce within a 12-month period during the 2-year exemption.	This is important for state DOTs to track given the potential of novel Ford vehicles operating on public roadways and the impact of those vehicles on enforcement personnel. Additionally, the agency response to this petition will be important to analyze for signs of interest, engagement, and knowledge on behalf of federal regulators and what that might mean for future action, including updates to FMVSS.	Posted to the Federal Register in July 2021. Comments due August 2022.
NHTSA Standing General Order on Crash Reporting	NHTSA issued a Standing General Order (the General Order) requiring identified manufacturers and operators to report to the agency	This information is important for state DOTs to be aware of and potentially leverage in evaluating the safety of allowing ADS systems	Published in July 2021, first data dump in June 2022, expected data dump every

Title	Description	Why it matters	Date(s) of interest
	certain crashes involving vehicles equipped with ADS or SAE Level 2 advanced driver assistance systems.	on public roads. It is public safety data classified by reporting entity, and though important context is omitted from the data collection, it is still the most CAV safety information that has ever been collected and made available publicly. It will be important for state DOTs to track how this information is shared and how it may be used for safety enforcement by NHSTA.	month, all data will be publicly available on the NHTSA site.
Nuro, Inc.; Grant of Temporary Exemption for a Low-Speed Vehicle with an ADS	On Feb 6, 2020, NHTSA announced the first-ever temporary exemption from specific FMVSS for a driverless vehicle; the exemption was awarded to Nuro so the company could operate its purpose-built delivery vehicle on public roads.	How NHTSA responds to the GM and Ford petitions listed above will further indicate USDOT's willingness to move forward on federal CAV regulations and grant exemptions for CAVs with passengers instead of just goods.	Announced in February 2020, open question if the exemption is still valid.
Einride Exemption	Einride received approval from NHTSA to test its autonomous, electric truck prototypes on public roads. The Pod will still be monitored by a remote operator, who can assume control if	State DOTs should understand from this exemption that the electric vehicle aspect was likely a motivating factor. Additionally, Einride has a unique perspective	Announced on June 23, 2022.

Title	Description	Why it matters	Date(s) of interest
	needed, but it will otherwise be operating in an automated manner on public roads.	on workforce where a remote operator is inherent to operations, and that data point likely served as yet another greenlight for federal exemption approval.	

Work Zone Data Exchange

A robust and active task force specifically focused on how CAVs will and should interact with work zones has arisen within the FHWA, aptly named the Work Zone Data Exchange (WZDx). The WZDx specification "enables infrastructure owners and operators to make harmonized work zone data available for third party use… Specifically, the project aims to get data on work zones into vehicles to help ADS and human drivers navigate more safely."

The Work Zone Data Working Group released version 4.2 of the WZDx specification in February 2023. Version 4.2 is the final version of the WZDx specification to be released by the Work Zone Data Working Group. The WZDx specification is transitioning into a formal standard by the FHWA under ITE and SAE stewardship.

The WZDx specification currently lists data feeds from 16 jurisdictions, including TxDOT. The long-term goal is for all 50 state DOTs to adopt identical data ingestion and reporting mechanisms so industry can most easily adopt these new safety data into their vehicles.

This is an important issue for state DOTs to be involved in since it affects data sharing and accompanying standards development. Up-to-date information about dynamic roadway and traffic conditions in work zones can help ADS and human drivers navigate safely. While states collect work zone data, they lack a common data standard and convening mechanism, which makes it difficult and costly for third parties (e.g., OEMs) to access and use these data across jurisdictions. CAVs will collect a huge amount of information, and potential liabilities associated with the collection and sharing of such data will necessarily affect state DOTs.

Automated Driving System Demonstration Grants

Under the 2018 Consolidated Appropriations Act (P.L. 115-141), $60 million was appropriated to USDOT for the purpose of facilitating the competitive ADS Demonstration Grant Program (U.S. Department of Transportation, 2021). The program's goals were threefold: to test the safe integration of ADS onto the nation's roads, ensure data gathering and sharing, and work with state and local governments and private partners.

Of the 73 total applicants, the following 8 were selected:

- Texas A&M Engineering Experiment Station—"AVA: Automated Vehicles for All."
- University of Iowa—"ADS for Rural America."
- Virginia Tech Transportation Institute—"Safely Operating ADS in Challenging Dynamic Scenarios: An Optimized Automated Driving Corridor Demonstration."
- Virginia Tech Transportation Institute—"Trucking Fleet CONOPS for Managing Mixed Fleets."
- Ohio Department of Transportation—"D.A.T.A. in Ohio: Deploying Automated Technology Anywhere."
- Pennsylvania Department of Transportation—"Safe Integration of Automated Vehicles (AV) in Work Zones."
- City of Detroit, MI—"Michigan Mobility Collaborative—ADS Demonstration."
- Contra Costa Transportation Authority—"Contra Costa Transportation Authority's ADS Demonstration Program."

As these projects are completed, best practices will be generated with a focus on the specific issues upon which the grant funding was awarded.

Infrastructure Investment and Jobs Act

In 2021, the U.S. Congress enacted P.L. 117-58, the IIJA, which includes several provisions authorizing CAV research and grant programs, including:

- *Section 11504, Study of Impacts on Roads from Self-Driving Vehicles*—authorizes a study on the existing and future impacts of self-driving vehicles to transportation infrastructure, mobility, the environment, and safety, including impacts on (a) the Interstate System, (b) urban roads, (c) rural roads, (d) corridors with heavy traffic congestion, (e) transportation systems optimization, and (f) any other areas or issues relevant to FHWA operations.
- *Section 13005, Emerging Technology Research Pilot Program*—creates a new pilot program to conduct research and development in areas including reducing the impact of CAV driving systems and ADS on pavement and infrastructure performance and in improving transportation infrastructure design in anticipation of increased usage of ADS and ADAS.
- *Section 13006, Research and Technology Development and Deployment*—creates a Center of Excellence on New Mobility and Automated Vehicles to collect, conduct, and fund research on the impacts of new mobility and highly automated vehicles (HAVs) on land use, urban design, transportation, real estate, equity, and municipal budgets.
- *Section 25005, Strengthening Mobility and Revolutionizing Transportation Grant Program*—authorizes the creation of a new grant program at $100 million annually for demonstration projects focused on advanced smart city or community technologies and systems to improve transportation efficiency and safety. Grant funds may be used for intelligent, sensor-based infrastructure, systems integration, and smart technology traffic signals.

Federal Legislative Overview

The two seminal pieces of federal CAV legislation are H.R. 3388 and S. 1885, the SELF DRIVE Act and the AV START Act, respectively. Both bills were introduced in 2017, and the House version passed out of the Energy and Commerce Committees. However, the Senate bill died before receiving a committee vote. The SELF DRIVE Act has been re-introduced in subsequent Congresses, but the legislation is not expected to move any further.

Summaries of each bill are below. However, the most important aspect of both pieces of legislation is that they did not and, in the case of the SELF DRIVE Act, do not include automated vehicles over 10,000 pounds (i.e., medium and heavy-duty trucks). However, it is anticipated that future federal CAV legislation will include vehicles over 10,000 pounds.

AV START and SELF DRIVE

These two pieces of federal legislation have been the only CAV-specific legislation introduced in the U.S. Congress to date. Both bills cover similar topics and, in many cases, use identical text.

Critical topics in both bills include:

- The establishment of federal preemption over "standard[s] regulating the design, construction, or performance of highly automated vehicles," which the legislation defined as vehicles under 10,000 pounds operating with Level 3–5 automation systems.
- Requirements to streamline and define the federal exemption process for CAVs.
- Relevance of human drivers to various existing federal safety and vehicle design standards, including passenger safety requirements should the internal configurations for passengers in vehicles be modified.
- Parameters for a federal HAV public, on-road testing program. The bill defines HAVs as those equipped with Level 3–5 ADS.
- Federal adoption of the SAE J3016 Levels of Automation taxonomy.
- HAV safety evaluation reports submitted by vehicle manufacturers, inclusive of cybersecurity practices.
- Creation of a motor vehicle privacy database that will describe information from individuals collected as part of the operation of CAVs and privacy policies associated with the use and operation of CAVs.
- The establishment of an advisory committee and working groups:
    - A HAV technical committee comprised of industry stakeholders to inform future agency actions.
    - A consumer education working group with a specified focus of helping consumers delineate between ADAS and ADS vehicles.
    - A data access advisory committee for the purpose of convening stakeholders to advise Congress on data management practices.
- Research initiatives into the potential effects on traffic wrought by the integration of ADS-equipped vehicles.

Other Federal Legislative Action

Interestingly, in early 2022, House lawmakers launched a new Congressional Autonomous Vehicle Caucus, indicating what could be a promising outlook for future federal legislative action. Representatives Debbie Dingell (D-MI-12) and Bob Latta (R-OH-05), known industry stalwarts, are the caucus co-leads. Given the amount of work both their offices have put into House legislation previously, it is expected that the caucus will gain momentum moving forward. In fact, Rep. Latta re-introduced the SELF DRIVE Act in 2021, setting the stage for what could be legislative action in the next congressional session.

Lending credence to the hypothesis that there will be increased federal legislative action on CAVs is the fact that in February 2022, the House held its first dedicated hearing on automated vehicles in over two years. Witnesses included organized labor, AV industry representatives, and state and local leaders, among others.

Large barriers to future federal legislative action, however, still exist, including:

- *Organized labor*—Labor unions such as the AFL-CIO and the International Brotherhood of Teamsters have not coalesced on what they want to see in federal CAV legislation. As a result, their primary congressional allies have held up movement on such legislation.
- *Lack of stability in the AV industry*—The AV industry has suffered from market and public perception failures that have slowed the pace of testing and deployment. In 2022, Argo AI, which had been backed by

Ford and Volkswagen, ceased operations (Korosec, 2022). In 2023, two AV trucking companies, Embark Trucks and Locomation, wound down its work forces and are rumored to be shutting down (Adler, March 2023; Adler, February 2023). Since their deployment in San Francisco in 2022, Cruise "robotaxi" vehicles have been documented blocking traffic for hours (Bellan, 2022). If they continue at this pace, these changes in market forces and public sentiment may undermine the credibility of the AV industry and provide political cover for federal inaction.

American Data Privacy and Protection Act

In July 2022, the House introduced a first-of-its-kind data privacy bill. The text of the bill focused on data minimization, which means companies and any data collectors would only be able to use consumer data for specific purposes spelled out in the legislation.

There are carveouts within the text, but with regard to AV developers and service providers, this bill is anticipated to affect data ingestion. ADS-equipped vehicles rely on external sensors to understand the world and make decisions, but if company data collection practices are curtailed, the CAV industry would need to pivot from a "gather everything possible" approach to one with much more limitations. If that change were to happen, that might affect how quickly this technology can approach commercial viability.

The ADPPA received a markup in the House committee of jurisdiction; however, it did not move any further throughout the legislative process nor is there a Senate companion bill. As such, the ADPPA is a long way from becoming law. Given the number of industries and markets it would affect, its likelihood of passage in current form—even next legislative session—is slim. However, it does indicate that Congress is taking seriously consumer data privacy concerns, perhaps pushed along by more aggressive action on behalf of states and other countries. As noted above, exactly how this impacts the operation of CAVs is still unknown but will be an important topic to track, and industry can be expected to voice concerns around any privacy requirements that may curtail operations.

Conclusion

Regarding state law, the TTCA narrowly limits liability for governmental agencies like TxDOT to claims where, unless waived, an intentional or negligent act of an employee arising from the operation of a motor vehicle or motor vehicle equipment proximately caused damage to property or human injury or fatality. In other words, whether the facts comprising the claim also involved data, automated or connected vehicles, roadway or traffic signal defects, or the acts of third parties, these threshold elements must be present for liability to attach to a state agency. If they are not, that agency is likely protected by sovereign immunity.

The areas where the law has not been tested or is silent are in three general areas: (a) electronic data, (b) whether FMVSS requirements and recent Texas state law may be in conflict, and (c) whether product-related injuries may expose the agency to tort liability. With regard to electronic data, it is currently unclear whether sovereign immunity can be waived from an agency's condition or use of electronic data. Current statutes and the common law are silent on whether an agency's electronic data can be regarded as tangible personal property, as well as whether the condition or use of government-owned, -produced, or -shared data waives an agency's sovereign immunity if it causes personal injury or death.

The law is clearer with regard to premises defects, special defects, and traffic signs, signals, warning devices, and other traffic control devices (including lane markings). Liability for these issues is likely similar in an environment with CAVs in operation as it is in the current environment without CAVs. Dangerous roadway conditions will still potentially create unreasonable risk of harm to passengers in CAVs as they do in human-operated vehicles. Risks for these liabilities can be mitigated by providing adequate notice or repairing the defect in a reasonable time once the agency knows or should have known of the dangerous condition.

With regard to the question of whether FMVSS requirements and recent Texas state law may be in conflict, the FMVSS preempts any state or local standard that does not meet federal requirements and supersedes any inconsistent state standards. It has not yet been adjudicated whether state provisions on CAVs in the Texas Transportation Code conflict with or support federal CAV authority.

With regard to the question of whether product-related injuries may expose the agency to tort liability, data products produced by a state agency for CAVs may expose the agency to tort liability for product-related injuries. However, Texas product liability law would still provide protections for the agency through burden of evidence requirements.

With regard to federal law, for a variety of reasons, it has been difficult for Congress to act on CAVs. This has led to some delay and a lack of focused action by USDOT and applicable regulatory agencies, including NHTSA and FMCSA. However, there continue to be rulemakings and requests for comments around CAVs. The information being gathered by USDOT through such rulemakings will hopefully lead to informed regulatory action that considers the flexibility needed as CAV technologies continue to mature and use cases evolve. While there are few specific references to CAVs in federal legislation at this point in time, notwithstanding the AV START and SELF DRIVE Acts discussed above, there are several bills that address issues touching CAVs. This includes legislation focused on privacy, smart cities, grant programs, and infrastructure focused on intelligent transportation solutions.

With the information gathered through this research project, TxDOT can remain informed and engaged on federal regulatory actions related to CAVs. For example, tracking potential actions on the exemptions that have been submitted by traditional auto manufacturers and how additional exemptions are granted or renewed around ADS focused on goods movement will provide important insights.

Texas is an unequivocal leader in CAV, and the knowledge the state has collected is invaluable to numerous stakeholders, not least of which is USDOT. Understanding that eventually there may be federal legislation that may preempt some aspects of state laws, Texas can focus on continuing to build a robust and safe deployment environment for all CAV use cases.

5. Use Case Legal Analysis

The TTI research team performed legal analyses for seven use cases involving CAV deployment. The use cases were developed based on law and policy interests from which the technical operation of each were described in written fact patterns and relevant laws and regulations were applied to perform the legal analyses.

Methodology

Based on experience with the testing and deployment of CAV technologies in the United States, as well as a review of ongoing practices in this area, the TTI research team collaborated with the TxDOT project monitoring committee (PMC) to develop use cases and written fact patterns. Attorneys and legal experts from the research team then applied the relevant state and federal laws and regulations identified in the state and federal law analysis (see Chapter 4) to the fact patterns to provide a legal analysis of each use case.

The use cases collaboratively developed between the TxDOT PMC and the TTI research team started from five use cases that TxDOT provided at the outset of the project:

- The operation of a CAV shuttle between two TxDOT campuses by TxDOT.
- A scenario in which CAVs operating on Texas roads cause damage to TxDOT assets and TxDOT seeks to recover damages.
- Digital sharing of TxDOT infrastructure information to CAVs.
- Receiving data about maintenance issues from private entities.
- A public shuttle for general use.

The TTI research team and the TxDOT PMC reconsidered these use cases in light of others proposed by the research team:

- A third-party vendor installing CAV equipment on TxDOT assets (e.g., lights, signals, signs) or other infrastructure located in the right-of-way.
- A TxDOT contractor utilizing CAVs for TxDOT construction/maintenance projects.
- Use of CAVs by TxDOT for maintenance/construction with larger safety risks (e.g., material loading/unloading within median, truck-mounted attenuators [TMAs]).
- TxDOT being party to Terms of Use agreements for subscription services to on-demand (rideshare) CAVs.
- CAVs used by TxDOT to monitor traffic and provide freeway safety patrol/incident management services that help drivers in distress.
- Privately owned CAVs receive and rely on corrupted data from TxDOT.
- TxDOT receives a PIA request for CAV data.
- TxDOT enters into an agreement with a metropolitan planning organization or a transit authority to construct and maintain a CAV corridor (for transit or freight purposes).
- Use of non-surface transportation AVs for TxDOT purposes (e.g., bridge inspections).

From these, the TTI research team and TxDOT PMC settled on seven use cases stemming from the following brief issue statements:

1. A scenario in which CAVs operating on Texas roads cause damage to TxDOT assets and TxDOT seeks to recover damages.
2. Digital sharing of TxDOT infrastructure information to CAVs.
3. TxDOT receives data about maintenance issues from private entities.
4. TxDOT use of CAVs for maintenance and construction activities.
5. A third-party vendor/contractor's use of CAVs.
6. TxDOT receives a PIA request for CAV data.
7. A transit operator's operation of a public CAV bus for general use.

Having selected the seven use cases, the TTI research team described the technical operation of each scenario in written fact patterns. Then, having already identified relevant statutory and case law (see Chapter 4), the TTI research team applied these principles to each use case to perform a legal analysis of the tort liabilities for the use cases. In each case, the team provided an analysis of the fact pattern that could reasonably arise in the near-term and that would be subject to current law.

Use Case Legal Analyses

This section provides a summary of the fact patterns and legal analyses performed for each of the seven use cases. The TTI research team tailored each fact pattern to narrow down the issues from each use case and provide a clearer holding based on the issues. Each use case legal analysis follows the Issue-Rule-Analysis-Conclusion format, identifying the issues, relevant law for each use case, application of the law to the fact patterns, and legal conclusion based on the analysis. Each analysis also includes a discussion of potential mitigation strategies for consideration that may be appropriate for Texas.

Use Case #1—CAV Operating on Texas Roads Causes Damage to TxDOT Assets and TxDOT Seeks to Recover Damages

Facts

- TxDOT posts a temporary "rollup" traffic control zone sign warning drivers of "Guardrail Damage Ahead," similar to the sign shown in Figure 2.
- The temporary sign is damaged in a hailstorm and is hard to read at night. Though readable to humans, it is not to a CAV.
- A freight CAV transporting machinery strikes the damaged guardrail and falls off the roadway (assume vehicle would not have fallen if guardrail was not damaged). The vehicle and machinery are irreparably damaged (no passengers are injured or killed).
- The insurance company for the freight carrier refuses to pay out the claim, claiming TxDOT's insufficient warning caused the crash.
- TxDOT sues the CAV owner for damage to the roadway and additional damage to the guardrail.
- The CAV owner also sues TxDOT for damage to the vehicle and freight.

Source: venturing4th

Figure 2. Temporary Rollup Sign.

Issue

- Whether the CAV owner can recover damages from TxDOT for insufficient warning of damaged guardrail.
- Whether TxDOT can recover damages from a CAV operator when a sign that would have sufficiently warned a human driver was not detected by the CAV's ADS and the CAV damaged the road's shoulder and further damaged the guardrail on a Texas road.

Rule

Sovereign Immunity: Condition or Use of Tangible Property:

- Tex. Civ. Prac. & Rem. Code §101.021.
- *Harris County v. Shook*, 634 S.W.3d 942 (Tex. 2021).
- *University of Texas Southwestern Medical Center v. Rhoades*, 605 S.W.3d 853 (Tex. 2020).

Sovereign Immunity: Premises Defects:

- Tex. Civ. Prac. & Rem. Code § 101.022(a).
- *Sampson v. Univ. of Tex. at Aus*., 500 S.W.3d 380 (Tex. 2016).
- *Harris County v. Shook*, 634 S.W.3d 942 (Tex. 2021).
- *Jefferson County, Texas v. Ellarene Farris, Individually and as Personal Representative of the Heirs and Estate of James Farris*, Appeal from 11th District Court of Harris County (Tex. App. 2018).

Sovereign Immunity: Traffic Signs, Signals, and Warning Devices:

- Tex. Civ. Prac. & Rem. Code §§ 101.022(b) and 101.060.
- *Denton County v. Beynon*, S.W.3d 329 (Tex. 2009).
- *City of Austin v. Lamas*, 160 S.W.3d 97 (Tex. App. 2005).
- *Texas Dept. of Transp. v. Ramming*, 861 S.W.2d 460 (Tex. App.— Houston [14th Dist.] 1993).

Sovereign Immunity: Discretionary Functions:

- Tex. Transp. Code § 201.615.
- *Carrasco v. City of El Paso*, 625 S.W.3d 189 (Tex. App. 2021).
- Tex. Civ. Prac. & Rem. Code § 101.056.

Caps on Damages and Proportionate Responsibility:

- Tex. Civ. Prac. & Rem. Code § 101.023.
- Tex. Civ. Prac. & Rem. Code §§ 33.001 and 33.012.

Federal Preemption and Vehicle Safety Certification

- Tex. Transp. Code §§ 545.453, 545.454, and 547.618.

Analysis

- *Sovereign Immunity: Premises Defects*—The damaged guardrail constituted a premises defect because it was tangible personal property that created a dangerous real property condition. The condition or use of the guardrail itself did not cause the injury. Likewise, because the damaged guardrail was not similar to an excavation or obstruction on the roadway, it did not constitute a special defect.
    - The damaged guardrail created a condition that presented an unreasonable risk of harm to drivers and passengers on the roadway.
    - TxDOT had a duty to exercise ordinary care and warn of the condition or make it reasonably safe after receiving actual notice of the condition.
    - TxDOT met this duty by erecting the temporary traffic control sign that warned of the damaged guardrail ahead.
- *Sovereign Immunity: Traffic Signs, Signals, and Warning Devices*—The temporary sign that read "Guardrail Damage Ahead" that was damaged in the hailstorm presented a condition for a traffic sign, signal, or warning device that waived sovereign immunity.
    - Under the TTCA, TxDOT had a duty to warn of the condition of the damaged sign after receiving either actual or constructive notice of the potential danger presented by the sign to CAVs.
    - TxDOT had not received reports or otherwise known of the potential danger presented by the sign to CAVs, so it did not have actual notice of the damaged sign. Likewise, TxDOT did not have constructive knowledge of the dangerous condition that a reasonably careful inspection would reveal.
    - Had TxDOT actually or constructively known of the sign's condition, TxDOT would be allowed a reasonable time under the law to warn of the sign's condition or replace or repair the sign since the malfunction was the result of an act of God.
- *Sovereign Immunity: Discretionary Functions*—Texas design immunity statutes protect TxDOT from any claim that a roadway where injury, death, or property damage involving a CAV occurs was not designed for CAVs.

- First, the TTCA provides an exception for discretionary functions, applying sovereign immunity to claims based on either (a) the failure of a governmental unit to perform an act that the unit is not required by law to perform or (b) a governmental unit's decision not to perform an act or on its failure to make a decision on the performance or nonperformance of an act if the law leaves the performance or nonperformance of the act to the discretion of the governmental unit. The Texas Supreme Court has held that design of any public work, including roadways, is a discretionary function protected by this statute to which governmental or sovereign immunity applies. Thus, as a governmental unit engaging in design of roadways, TxDOT may not be sued for claims of harm due to dangerous conditions of public properties designed through engineering-based decisions.
- Second, the Texas Transportation Code provides design criteria for transportation projects (excluding maintenance resurfacing projects) that include aspects of safety and durability, cost of maintenance, effects on the environment and surrounding communities, and access to other transportation modes. As such, the law supplies a statutory standard for design. However, under the same section of state statute, TxDOT is not required to contemplate the question of design appropriateness for future modes or vehicles (e.g., CAVs). Thus, TxDOT is not required to take CAVs into consideration under its statutory authority and does not have a duty to post warning signs comprehensible to non-human CAV ADSs unless it had engineering-based data that provided information about what is required to communicate with a CAV.

- *Caps on Damages and Proportionate Responsibility*—If the CAV owner could recover damages from TxDOT, their total monetary damages and prejudgment interest would be limited to $250,000 in money damages for each person, $500,000 for each single occurrence of bodily injury or death, and $100,000 for each single occurrence of injury to or destruction of property. Their damages would be further limited under the principle of "proportionate responsibility," which allows a reduction in a plaintiff's recovery if the plaintiff was partially to blame for their injury, and bars a plaintiff's recovery of damages if their percentage of responsibility is greater than 50 percent.
- *Federal Preemption and Vehicle Safety Certification*—In lieu of federal standards for CAVs, Texas has adopted its own regulatory framework for CAVs, placing responsibility on CAV owners for compliance with traffic and motor vehicle laws and prohibiting CAVs from operating if they are incapable of complying with state traffic and motor vehicle laws, are not equipped with manufacturer-installed recording devices and federally compliant ADSs, are not registered and titled in the state, or are not insured.

  - The CAV owner was responsible for compliance with Texas traffic and motor vehicle laws. As such, in failing to have the CAV equipped with an ADS that could "read" the sign, they may be found in violation of state law.
  - In addition to state accident reporting requirements, the CAV owner was also subject to compliance with NHTSA's Standing General Order Update, issued in June 2021 and amended in August 2021, which created a three-year reporting obligation for named manufacturers, developers, and operators of Level 2 ADAS and Levels 3–5 ADSs in which covered crashes must be reported within 10 days of the incident.

Conclusion

- The CAV owner would not be able to recover damages from TxDOT because TxDOT provided sufficient warning of the premises defect (damaged guardrail) and did not have sufficient notice that the sign warning of the premises defect could not be read by CAVs. Further, due to proportionate responsibility, the CAV owner's recovery of damages would be barred because their percentage of responsibility is greater than 50 percent (i.e., the CAV would not have fallen off the roadway had it "seen" the sign).
- TxDOT could recover from the CAV owner's insurance provider for damage to the roadway shoulder and guardrail because, under state law, owners of CAVs are responsible for compliance with Texas traffic and motor vehicle laws and prohibited from operating CAVs if the vehicle is not equipped with federally compliant ADSs.

Mitigation

- *Policy*—To facilitate warning to CAVs and avoid the situation where the CAV cannot read a sign or signal designed for humans, TxDOT should assess (a) infrastructure-to-vehicle (I2V) communications technologies for CAVs to receive information from highway agencies that are today communicated to human drivers through traffic signs, signals, and warning devices; (b) vehicle-to-infrastructure (V2I) communications technologies to receive information from CAVs regarding roadway and traffic conditions; and (c) data storage, aggregation, and maintenance products and practices to receive, archive, analyze, act on, and/or dispose of I2V and V2I data. From these assessments, TxDOT should develop and implement policies and protocols to receive, store, maintain, and disseminate this information to ADSs, as well as to generate service requests and alert maintenance and operations personnel of the defects, inoperability, or damage to transportation assets.
- *Legislation*—Although it is likely that Texas' design immunity statutes protect TxDOT from liability for a damaged sign that, though legible to humans, a CAV could not read, it may be prudent to consider codifying TxDOT's authority to provide smart infrastructure designed to communicate with CAVs, as well as requirements that CAVs can comply with such devices, and that the waiver of sovereign immunity provided for traffic signals, signs, or warnings be extended to operation of smart infrastructure.
    - The law is silent as to whether the duty to warn of and correct for the absence, condition, or malfunction of traffic signals, signs, or warnings applies to data from traffic control devices or the inability of traffic control devices to effectively communicate with an ADS (as opposed to a human driver). To protect TxDOT from potential liability, Tex. Civ. Prac. & Rem. Code § 101.022 and § 101.060 may need to be amended through legislation to expressly bar the extension of the waiver of sovereign immunity and higher duty of care to I2V or smart infrastructure devices, data, and communications.
    - The law is also silent regarding the authority of TxDOT and other government agencies to place and maintain I2V or other smart infrastructure devices that serve traffic and road control purposes, as well as the rules of the road related to CAV compliance with digital traffic control communications (e.g., to stop, yield, use certain lanes). Thus, for consistency and public policy reasons, Tex. Transp. Code, Title 7, Subtitle C, Chapter 544 should be amended through legislation to expressly extend the authority to

place and maintain I2V or smart infrastructure devices to TxDOT and local authorities, and to require CAV compliance with traffic control data from such devices.

Use Case #2—Digital Sharing of TxDOT Infrastructure Information to CAVs

Facts

- Real-time TxDOT work zone information (regarding lane reconfiguration) is not accurate, telling CAVs that lanes have not been reconfigured.
- A CAV crashes into the work zone and is irreparably damaged.
- A construction worker is killed because the vehicle received bad data.
- The CAV owner reasonably relied on the TxDOT data.
- A federal standard is in place requiring that state DOTs provide real-time data as part of the established CAV Work Zone Protection Program connected to federal funding.
- TxDOT has engaged a third party to coordinate the collection, verification, and dissemination of data related to work zones.
- The worker's family sues the CAV owner and TxDOT for death of worker.
- The CAV owner sues TxDOT for damages to the vehicle.

Issue

- Whether the CAV operator could recover damages from TxDOT for the inaccurate data supplied to the CAV through a third party as part of a federal mandate.
- Whether the family of a TxDOT construction worker can recover damages from a CAV operator whose vehicle crashed into a work zone due to receiving inaccurate TxDOT data.

Source: TTI

Figure 3. Work Zone Operations in Texas.

Rule

Sovereign Immunity: Special Defects:

- Tex. Civ. Prac. & Rem. Code § 101.022(b).
- *City of Daingerfield v. Snyder*, No. 06-21-00101-CV (Tex. App. Mar. 31, 2022).

- *Denton County v. Beynon*, S.W.3d 329 (Tex. 2009).
- *City of Dallas v. Reed*, 222 S.W.3d 903 (Tex. App. 2007).
- *Tex. Dept. of Transp. v. York*, 284 S.W.3d 844 (Tex. 2009).
- *City of Denton v. Paper*, 376 S.W.3d 762 (Tex. 2012).
- *Burk Royalty Co. v. Walls*, 616 S.W.2d 911 (Tex. 1981).

Workers Compensation:

- Jefferson County, Texas v. Ellarene Farris, Individually and as Personal Representative of the Heirs and Estate of James Farris, Appeal from 11th District Court of Harris County (Tex. App. 2018).
- City of Bellaire v. Johnson, 56 Tex. Sup. Ct., J. 633 (Tex. 2013).
- Tex. Lab. Code § 408.001(a).
- Tex. Civ. Prac. & Rem. Code §§101.021(1)(B) and 101.028.
- Duhart v. State, 610 S.W.2d 740 (Tex.1980).

Sovereign Immunity: Condition or Use of Tangible Personal Property:

- Tex. Civ. Prac. & Rem. Code §101.021(2).
- *Harris County v. Shook*, 634 S.W.3d 942 (Tex. 2021).

Sovereign Immunity: Independent Contractors:

- Tex. Civ. Prac. & Rem. Code § 114.003.

Data Management:

- Tex. Gov't. Code §§ 2054.137, 2054.138, and 2062.002.

Texas Deceptive Trade Practices Act:

- Tex. Bus. And Comm. Code, Title 2, Chapter 17.

Analysis

- *Sovereign Immunity: Special Defects*—Although under current statute, the design of a work zone may constitute a discretionary governmental function that protects TxDOT from liability and TxDOT is not required to contemplate design appropriateness for future modes or vehicles (e.g., CAVs), the work zone lane reconfiguration in this scenario could also be considered a special defect or a condition in the same class as an excavation or obstruction on a highway, road, or street that poses a threat to an ordinary user of the roadway.
    - A special defects exception to sovereign immunity triggers a higher duty of care for TxDOT than the exception for conditions or use of property or premises defects. TxDOT's duty to warn is the same that a private landowner owes to an invitee. Under this standard, the CAV owner needs to prove that the condition of the premises created an unreasonable risk of harm to them, TxDOT failed to use ordinary care to protect invitees from danger, and TxDOT's failure was a proximate cause of their injury. They must only prove that TxDOT knew, or should have known, of a condition that created an unreasonable risk of harm.

- TxDOT approved the work zone traffic management plan and the work zone management team complied with it. This demonstrates that TxDOT was actually aware of the inherently dangerous condition presented by the work zone.

- *Sovereign Immunity: Sufficiency of Notice*—Because TxDOT reasonably should have known the work zone data could be inaccurate and cause a crash (i.e., had constructive notice), the agency had a duty to warn the CAV owner or make the condition safe.
  - TxDOT owes those on its highways the duty of ordinary care to provide notice to users of the roadway of a dangerous condition of which TxDOT is or reasonably should be aware. Though neither TxDOT nor the third-party vendor actually knew of the inaccurate data and unintentionally disseminated the data, they both should have known that the data had the potential to be inaccurate and that wrong data could cause a crash.
  - By failing to provide notice to the CAV that the lanes were reconfigured, TxDOT did not sufficiently provide notice to the CAV of the dangerous condition. This failure to warn may be considered the proximate cause of the worker's death and any injuries to passengers in the CAV.
  - Since liability for special defects extends only to personal injury and death, and not to property damages, property damages cannot be recovered.

- *Sovereign Immunity: Workers' Compensation*—TxDOT retained its immunity and provided the highway worker (and his estate) an alternative remedy through workers' compensation coverage.
  - By having workers' compensation insurance or accepting the workers' compensation laws of Texas, TxDOT is entitled to the privileges and immunities granted by the Texas workers' compensation laws to private individuals and corporations.
  - Because TxDOT is immune from liability by having provided workers' compensation, the agency is likewise immune from suit.

- *Sovereign Immunity: Condition or Use of Tangible Personal Property*—The work zone data likely do not constitute tangible personal property that waives TxDOT's sovereign immunity.
  - TxDOT's sovereign immunity would be waived if the injury were caused by a condition or use of tangible personal property, and TxDOT, were it a person, would be liable. The injury and claim for damages was caused by a contemporaneous "action or service" (use) or "state of being" (condition) of the data.
  - However, current statutes and the common law are silent on whether an agency's electronic data can be regarded as tangible personal property, as well as whether the condition or use of government-owned, -produced, or -shared data waives an agency's sovereign immunity if they cause personal injury or death. Though a hard drive or server containing electronic data may be tangible personal property, the condition or use of the information contained within data may not waive liability.

- *Sovereign Immunity: Independent Contractors*—The dissemination of inaccurate work zone data by a third party (i.e., a TxDOT vendor who coordinates the collection, verification, and dissemination of data related to work zones) cannot shield TxDOT from liability.

- TxDOT cannot plead sovereign immunity for damage, injury, or death proximately caused by wrongful acts, omissions, or negligence of its independent contractors.
- TxDOT may, however, pursue the third-party vendor for breach of contract in disseminating the incorrect work zone data.

- *Data Management*—To meet its duty of care and be aware of data conditions that it should know create an unreasonable risk of harm, TxDOT will need to establish statutory data management practices, including designating a data management officer to, among other things, establish an agency data governance program and include a provision in contracts with vendors authorized to access, transmit, use, or store data for the agency requiring the vendor to meet the agency's security controls and provide evidence that they meet the security controls.
- *Texas Deceptive Trade Practices Act (DTPA)*—The Texas DTPA may not apply in this case because (a) TxDOT is not acting as a commercial seller of data and (b) the law is limited to transactions that include goods ("tangible chattels or real property purchased or leased for use") or services ("work, labor, or service purchased or leased for use") and not data.
  - The Texas DTPA may apply if TxDOT were to offer "data-as-a-service" (DaaS) or "software-as-a-service" (SaaS) by providing CAVs a centrally hosted, cloud-based, on-demand data management software tool on a subscription basis that delivers data storage, integration, processing, and/or analytics services.
  - If TxDOT were to sell the work zone data to CAVs and other users as part of a DaaS or SaaS system, it would have a duty to refrain from false, misleading, and deceptive e-business practices.

Conclusion

- TxDOT failed in its duty to the CAV owner to protect against danger from a condition (the work zone lane reconfiguration) that created an unreasonable risk of harm, of which TxDOT actually knew. TxDOT also failed in its duty to protect against the danger of inaccurate data, which TxDOT should have been aware of. Therefore, the CAV operator can recover damages (for injuries or death, but not property damages) from TxDOT.
- The family of the highway worker cannot recover anything from TxDOT other than the workers' compensation payment due to them.
- TxDOT cannot plead sovereign immunity for damage, injury, or death proximately caused by its independent contractors. However, TxDOT could recover damages from the third party that coordinated the dissemination of data due to breach of contract.

Mitigation

- *Standards*—Work zones, as special defects, will still present a potential threat to CAVs. To notify CAVs or otherwise mitigate the danger inherent in work zones, TxDOT should adopt practices similar to those used to notify human drivers of work zones today. Just as static and variable message signs and other traffic control devices are used today to notify human drivers of work zones ahead, TxDOT should consider adopting data dissemination and management standards as part of its work zone traffic management planning process. TxDOT should also adopt data inspection measures similar to the construction

management and work zone inspection practices in place today. These provisions may also be incorporated into construction and data management contracts to ensure that data are correct when disseminated and that vendors have proper processes in place to catch incorrect data.

- *Legislation*—Because the law is silent on whether an agency's electronic data can be regarded as tangible personal property, TxDOT may want to consider proposing legislation that expressly defines "tangible personal property" to exclude electronic data that are owned, produced, or shared by governmental units. This would conform to the court's prior decisions regarding information contained within tangible medical records while leaving government agencies open to waivers of liability for conditions or use of other forms of tangible personal property.
- *Statutory Compliance*—To comply with statutory data management requirements, TxDOT should designate a data management officer and include a provision in contracts with data vendors requiring the vendors to meet the agency's security controls and provide evidence that they meet the security controls.

Use Case #3—TxDOT Receives Data on Maintenance Issues from Private Entities

Facts

- TxDOT receives sensor and GPS data directly, in real time, about unsafe road conditions from a CAV, indicating the presence and location of an icy bridge, similar to the one shown in Figure 4.
- The data received are accurate (i.e., bridge is in fact currently icy).
- The CAV data volume is magnitudes higher than what is received from individual humans calling in to report dangerous roadway conditions. However, it is still received and automatically entered into TxDOT's digital system for processing and responding to roadway condition reports.
- The bridge is put on a list of bridges for TxDOT to treat with sand. The system that ingests data and produces the list does not prioritize items that are reported (they are simply listed in the order in which they are received).
- TxDOT does not have the ability to warn individual vehicles directly of road conditions.
- The bridge is not treated in time, and four hours after TxDOT receives the data, a commercial vehicle driven by a human swerves into the oncoming lane and crashes into another vehicle.
- The crash causes damage to property (the bridge where the truck catches fire, destruction of the truck, totaling of the other vehicle) and injury to people (serious, debilitating, permanent injuries to the truck driver, including brain injury).

Source: weather.com

Figure 4. Photo of Bridge Covered in Ice.

Issue

- Whether TxDOT waives its sovereign immunity and is liable to a truck driver and passenger vehicle driver who suffered property damages and injuries from a crash resulting from TxDOT not treating an icy bridge after being given notice from a CAV.

Rule

Sovereign Immunity: Premises Defects:

- Tex. Civ. Prac. & Rem. Code §§ 101.001, 101.021, 101.022.
- *City of Daingerfield v. Snyder*, No. 06-21-00101-CV (Tex. App. Mar. 31, 2022).
- *Sampson v. Univ. of Tex. at Aus*., 500 S.W.3d 380 (Tex. 2016).
- *Jefferson County, Texas v. Ellarene Farris, Individually and as Personal Representative of the Heirs and Estate of James Farris* Appeal from 11th District Court of Harris County (Tex. App. 2018).

Sovereign Immunity: Condition or Use of Tangible Personal Property:

- Tex. Civ. Prac. & Rem. Code §101.021(2).
- *University of Texas Southwestern Medical Center v. Rhoade*s, 605 S.W.3d 853 (2020).
- *Harris County v. Shook*, 634 S.W.3d 942 (Tex. 2021).

Data Management:

- Tex. Gov't. Code §§ 2054.137, 2054.138, and 2062.002.

Analysis

- *Sovereign Immunity: Premises Defects*—The icy bridge constituted a premises defect because it presented a dangerous condition of real property that caused injury. It does not constitute a special defect because icy bridges are entirely predictable when the weather is conducive to such a condition, unlike a condition in the same class as an excavation or obstruction on a highway, road, or street that poses a threat to an ordinary driver.

- Because the icy bridge constituted a premises defect, TxDOT owed to the truck driver (and other drivers using the bridge) the duty that a private person owes to a licensee on private property. This duty requires that TxDOT not injure users of the bridge by willful, wanton, or grossly negligent conduct, using ordinary care either to warn of the dangerous condition or make it reasonably safe after receiving actual notice of the condition, of which drivers are not aware.
- TxDOT received actual notice of the icy condition on the bridge, as evidenced by the CAV road condition data being entered into TxDOT's digital system and the bridge being put on TxDOT's list of bridges to treat.
- TxDOT may have failed in its duty, however, if it did not warn drivers of the icy conditions on the bridge or do anything to make the bridge safe other than placing it on its list of bridges to treat (i.e., if it can be presumed that the driving public did not know of the risk because they received no warning).
- Therefore, TxDOT may have waived its immunity to liability and may have not met its duty to the truck driver and others injured in the crash.
- Since liability for premises defects extends only to personal injury and death, and not to property damages, property damages cannot be recovered.

- *Sovereign Immunity: Condition or Use of Tangible Personal Property*—The road condition data and the TxDOT digital software system for processing and responding to roadway condition reports likely do not constitute tangible personal property that waives TxDOT's sovereign immunity. Even if they were considered tangible personal property, their condition or use did not actually cause the injury to those involved in the crash. The data and software merely furnished a condition that had the potential to cause injury. In the same way, the list that the bridge is put on for TxDOT to treat, even if printed on paper and tangible, was not the actual cause of the injuries to those involved in the crash, but merely involved.
  - TxDOT's sovereign immunity would be waived if the injury were caused by a condition or use of tangible personal property, and TxDOT, were it a person, would be liable. The data, software, and list were in a condition and being used for a given purpose (tracking reports and requests, and listing bridges to treat). The injury and claim for damages, however, were not caused by any contemporaneous "action or service" (use) or "state of being" (condition) of the data, software, or list, but of the bridge icing during severe weather.
  - Current statutes and the common law are silent on whether an agency's electronic data can be regarded as tangible personal property, as well as whether the condition or use of government-owned, -produced, or -shared data waives an agency's sovereign immunity if they cause personal injury or death. Though a hard drive or server containing electronic data may be tangible personal property, the condition or use of the information contained within data may not waive liability.
- *Data Management*—To meet its duty of care and remain aware of data conditions known to create an unreasonable risk of harm, TxDOT will need to establish updated data management practices.
  - Had a system been in place to rank or prioritize service requests, TxDOT may have put this particular bridge higher up on the list for treatment application and prevented this crash.

- It is currently unclear whether a reasonable expectation exists that TxDOT respond to newly increased volumes of undifferentiated data from CAVs in a way that assesses risks and prioritizes requests, at the same time that it allows the agency to make conditions safe or warn roadway users of dangerous conditions within a reasonable time frame.

Conclusion

- Because TxDOT failed to warn the driver of the icy bridge condition, a premises defect, or make it reasonably safe, the agency may have breached its duty and waived sovereign immunity. Thus, TxDOT might be determined to be liable to the truck driver and passenger vehicle driver for bodily injuries caused by the crash but would not be liable for property damages. If found liable, TxDOT would not be able to recover damages from the passenger vehicle owner or the truck driver for the damage done to the bridge and roadway by the crash and ensuing fire.

Mitigation

- *Operational Measures*—TxDOT should consider implementing operational measures to prepare for the potential future flood of data from CAVs about roadway defects that may strain the agency's capacity to address them within defined notice periods and open them up to potential tort liability. To this end, TxDOT and other government agencies should:
  - Anticipate receiving more and perhaps better information about roadway conditions that will help prioritize repair work more efficiently.
  - Invest in information technology capabilities and increasing staff capacity and ability to access, analyze, and manage data.
  - Test and develop protocols for making agency data available to OEMs for CAV applications, using as examples experiments with providing work zone data to OEMs so that they can notify CAVs and their operators of changes in real time.
  - Become more familiar with CAV sensor data while the industry is nascent and establish processes and standards that can evolve over time, including processes for addressing reports of roadway defects to accommodate CAV data and reports about conditions. It may be most advantageous for the data to be communicated from the vehicle to the OEM (rather than directly to the agency) in the form of reports scheduled at regular intervals. A regular reporting plan from the OEM to the agency will allow the OEM to decide what conditions to report, mimicking the current process where the public selectively reports roadway conditions. Then, agencies can add the service requests into their current system and make decisions on how to grade and prioritize the requests for maintenance.
  - Provide CAVs and their passengers actual notice or warnings of premises defects. These measures could include alerts on the vehicle's display or passenger's communication device as well as data provided to ADSs warning of the dangerous condition and advising how to avoid it.
- *Legislation*—As provided in the prior use case analysis, the law is silent on whether an agency's electronic data can be regarded as tangible personal property, so TxDOT may want to consider proposing legislation

that expressly defines "tangible personal property" to exclude electronic data that are owned, produced, or shared by governmental units.

- *Statutory Compliance*—As provided in the prior use case analysis, TxDOT should designate a data management officer and include a provision in contracts with data vendors requiring the vendor to meet the agency's security controls and provide evidence that they meet the security controls.

Use Case #4—TxDOT Use of Maintenance and Construction CAVs

Facts

- A TxDOT-owned unmanned aerial vehicle (UAV, commonly known as a drone) is approved and used for TxDOT purposes (i.e., bridge inspections).
- A driver in a private car sees a moving camera on the UAV.
- An image from the camera makes its way to an unauthorized place due to not being stored in accordance with TxDOT data management policies.
- TxDOT suffers a data breach, where images may have been accessed.
- Based on their own anti-government surveillance activism and research, the driver files a claim against TxDOT for invasion of privacy.

Source: TTI

Figure 5. Photo of Drones.

Issue

- Whether TxDOT is liable for invasion of a driver's privacy from a drone's capture, storage, and inadvertent dissemination of photos of the driver.

Rule

Use of Unmanned Aircraft:

- Tex. Gov't. Code §§ 423.002, 423.003, and 423.004 (overturned, pending appeal).
- *Nat'l Press Photographers Ass'n v. McCraw*, 504 F. Supp. 3d 568 (W.D. Tex. 2020).

Sovereign Immunity: Motor-Driven Equipment:

- Tex. Civ. Prac. & Rem. Code §101.021(1).
- *Mount Pleasant Indep. Sch. Dist. v. Estate of Linburg*, 766 S.W.2d 208 (Tex. 1989).

Invasion of Privacy:

- *Boyles v. Kerr*, 806 S.W.2d 255 (Tex. App. 1991).
- *Billings v. Atkinson*, 489 S.W.2d 858 (Tex. 1973).
- *Olmstead v. United States*, 277 U.S. 438 (1928).
- *Katz v. United States*, 389 U.S. 347 (1967).

Data Privacy:

- Tex. Transp. Code §§ 730.006 and 730.007.
- Tex. Gov't. Code § 2062.002.

Analysis

- *Use of Unmanned Aircraft*—Even though current state law prohibits the capturing, possessing, disclosing, and distributing of images of drivers from use of a drone, TxDOT would not be in violation of it because the law provides an exception for images of public property and persons on that property and, more importantly, the law has been found to be unconstitutional.
    - Current Texas law declaring it unlawful to "capture an image of an individual or privately owned real property in [Texas] with the intent to conduct surveillance on the individual or property contained in the image" has been found by a federal court to be unconstitutional because it chills engagement in protected First Amendment activity, impermissibly regulates speech on the basis of content and speaker, and is overbroad in not clearly defining "surveillance" and restricting a substantial amount of protected activity.
    - Under the overturned law, the possession, disclosure, display, distribution, or other use of an image from a drone is deemed an offense, but the capturing of images by drones of public real property or a person on that property is allowed. If the law were to be preserved upon appeal, TxDOT's capture of images of the driver from use of a drone would be lawful because the image was of public real property (a TxDOT roadway/public right-of-way) and a person on that property.
    - Without any applicable law, the driver has no legal basis for claiming TxDOT is liable for invading their privacy.
- *Sovereign Immunity: Motor-Driven Equipment*—The driver could assert that TxDOT's use of a drone for bridge inspections subjected the agency to a waiver of sovereign immunity, which, if valid, would open TxDOT up to a claim of negligent invasion of privacy. However, such a finding is not likely.
    - The driver could assert that the TxDOT-owned drone is motor-driven equipment for the purposes of the TTCA because in performing practical bridge inspection work and being put into action, the drone was operated and used by TxDOT. However, there is no legal precedent for finding that a drone constitutes motorized equipment for purposes of the TTCA. TxDOT currently has video cameras on its rights-of-way

and incurs no liability from them because no motor-driven vehicle or equipment is involved. Images from drones used for TxDOT purposes are similar to images from the video cameras currently on the right-of-way, which would likely result in no liability for TxDOT even though a motor is involved.

- TxDOT would have waived sovereign immunity for injuries suffered by the driver if the injuries were proximately caused by the wrongful act, omission, or negligence of TxDOT employees actually operating and using motor-driven vehicles or equipment within their scope of employment. However, the proximate cause of the driver's injuries was the improper storage of data and not TxDOT's operation and use of the drone.
- Because TxDOT did not waive its sovereign immunity, the driver could not claim damages for negligent invasion of privacy.

- *Invasion of Privacy*—The right to privacy is a recognized legal interest in Texas, with invasion of privacy covering four types of torts: (a) intrusion upon the plaintiff's seclusion, solitude, or private affairs; (b) public disclosure of embarrassing private facts about the plaintiff; (c) publicity that places the plaintiff in a false light in the public eye; and (d) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

  - Had TxDOT waived sovereign immunity, the public release of the photo of the driver taken by the drone could be classified under the first three of the tort classifications, amounting to an intrusion into the driver's personal affairs, disclosing embarrassing private matters to the public, and placing them in the false light of appearing to be a person who willingly allowed themselves to be photographed while driving.
  - The fact that the release of the photo was due to a data breach, and therefore unintended, is irrelevant because Texas courts have held that the basis for liability in a privacy action could rest upon a negligent, as well as an intentional, invasion.
  - If the TxDOT employees were personally liable to the driver under Texas law, they would have had a legal duty not to engage in conduct that would result in foreseeable damages to the driver or the driving public. If the circumstances are such that a person of ordinary common sense would recognize that if the employees did not exercise reasonable care in their conduct with regard to the known circumstances, their acts would place another in danger, the duty to use ordinary care to avoid such danger arises. In this case, while the TxDOT employees could have foreseen the likelihood that emotional injury to the driver might result from the drone taking pictures of them, TxDOT employees may not have reasonably foreseen a data breach that would result in the distribution of the images. However, as noted above, TxDOT did not waive its sovereign immunity, so the driver would not have a valid legal basis for claiming damages for negligent invasion of privacy.
  - At the federal level, the U.S. Supreme Court has already begun to embrace a more expansive view of constitutionally protected individual privacy rights as society has become more reliant on technology. In *Olmstead v. United States* in 1928, Justice Brandeis' dissenting opinion argued that the majority had improperly narrowed the focus of the Fourth Amendment to the property of the defendants. He suggested that the drafters of the Constitution intended for the Fourth Amendment to protect the citizenry against "every unjustifiable intrusion by the government upon the privacy of the individual." In

1967, the Supreme Court in *Katz v. United State*s distinguished between what could be visually observed through the glass and what could be heard by electronic surveillance. The Supreme Court held that subsequent decisions necessitated a review of the limits of surveillance without trespass due to the increasing technological ability of policing agencies. Therefore, the protection of privacy under the Fourth Amendment should not, in the future, be based solely upon the existence of actual physical intrusion. Here, the Supreme Court created the two-part privacy test that is used today: first, that a person has exhibited an actual expectation of privacy, and second, that the expectation be one that society is prepared to recognize as "reasonable."

- *Data Privacy*—The inadvertent dissemination of the photo of the driver likely may have violated the duty TxDOT owed to the driver enumerated by statutory requirements.
    - Texas statutes do not expressly require TxDOT to protect personal identifying information contained in photos taken from drones. As noted above, current state law deems it lawful to capture images using unmanned aircraft of public real property or a person on that property, but the law has been found to be unconstitutional.
    - Statutes protect personal information collected by government agencies from distribution without consent. The Texas Department of Motor Vehicles is prohibited by Texas law from disclosing personal information in motor vehicle records (e.g., photos that can identify a person) except to those who are the subject of the information or with their consent. Under state agency data management requirements and procedures enacted in 2021, TxDOT is prohibited from acquiring, retaining, and disseminating information obtained from global positioning system technologies, contact tracing, or technologies designed to obtain biometric identifiers that identify an individual or the individual's location without the individual's written or electronic consent, unless required or permitted by federal or state law or for law enforcement purposes.
    - In light of the statutory limitation on the possession, disclosure, display, distribution, or general use of drone-captured images and prohibition of government agencies from disclosing personal information in motor vehicle records and obtained from global positioning system technologies, contact tracing, or biometric identifying technologies, Texas courts may construe the Texas State Legislature's intent as protective of private information, including photos, that are collected and stored by government agencies from non-consensual disclosure.
    - In allowing an image of the driver from the drone's camera to make its way to an unauthorized place without the driver's consent, not in accordance with the Legislature's intent and TxDOT data management policies, an outcome that a reasonable person may have foreseen, TxDOT may have likely breached its duty to the driver.

Conclusion

- TxDOT's use of a drone for TxDOT purposes (e.g., bridge inspections) would not open the agency to a waiver of sovereign immunity because current state law, which allows taking images of public property and persons on that property using drones, has been invalidated as unconstitutional, providing the driver no legal basis for claiming damages from TxDOT.

- Had TxDOT waived sovereign immunity, the public release of the photo of the driver taken by the drone could be classified as an invasion of privacy as (a) an intrusion upon the plaintiff's seclusion, solitude, or private affairs; (b) public disclosure of embarrassing private facts about the plaintiff; and (c) publicity that places the plaintiff in a false light in the public eye. The TxDOT employees had a legal duty not to engage in conduct that would result in foreseeable damages to the driver. Though they could have foreseen the likelihood that emotional injury to the driver might result from the drone taking pictures of her, they may not have reasonably foreseen a data breach that would result in the distribution of the images.
- Had TxDOT waived sovereign immunity, the inadvertent dissemination of the photo of the driver could be found to violate the duty TxDOT owed to the driver enumerated by statutory requirements, which may be construed by courts as stating the Texas State Legislature's intent that private information, including photos, collected and stored by government agencies be protected from non-consensual disclosure.

Mitigation

- Proactive operational strategies that TxDOT can undertake to acknowledge the new risk considerations created by UAV-mounted cameras—One notable precaution TxDOT has taken thus far is publication of its Unmanned Aircraft System (UAS) Flight Operations and User's Manual. Making this resource available without restriction indicates a level of risk mitigation and awareness of reasonability and foreseeability. However, recognition of privacy rights will likely become more complicated and contextually defined as technology generally, including cameras, are introduced into transportation agency operations at a greater pace. Courts will likely take the lead on defining an individual's expectation of privacy in various situations, though federal legislation will need to materialize to avoid a jurisdictional patchwork and to provide the legislative foundations upon which courts can make decisions. In light of this, TxDOT may want to consider:
    - Testing signage on roadways alerting travelers to the use of drones for inspection purposes where inspections are taking place. The signage would provide notice to drivers that images are being captured for road and bridge safety purposes.
    - Creating an agency procedure where drone operations to inspect infrastructure are only conducted on a section of roadway(s) that has been closed to traffic, regardless of roadway size or number of lanes.
    - Installing artificial intelligence (AI) software within the information management system of the drone's image-capturing capacity that can screen UAV-captured photos for people and immediately delete or blur faces in photos before any TxDOT representatives see the photos or before they are stored on TxDOT servers.
- *Legislation*—Currently, the definition of a motor vehicle does not clearly include drones but could be interpreted to include them. Thus, legislation may be needed to clarify that the definition of a motor-driven vehicle or equipment for purposes of the TTCA does not include drones.

Use Case #5—Third-Party Vendor/Contractor's Use of CAVs

Facts

- TxDOT allows its contractor to use a CAV TMA that meets TxDOT specifications, which are based on industry standards but not federal standards (federal CAV standards are still evolving).

- TxDOT provides data to the contractor for the TMA to use.
- The contractor uses the TMA as specified, which is similar to how TMAs are used today (i.e., in mobile operations where low speeds and distances are maintained).
- The TMA is going uphill on a narrow two-lane road, taking up both lanes due to its size.
- An oncoming private vehicle does not see the TMA in time and crashes into it.
- The driver of the private vehicle sues TxDOT and the third-party contractor for their injuries.

Source: Kratos

Figure 6. Photo of Automated TMA.

Issue

- Whether TxDOT waives its sovereign immunity when its contractor uses an automated TMA that uses TxDOT-supplied data and is operated in accordance with TxDOT standards and industry standards.

Rule

Sovereign Immunity: Motor-Driven Vehicles:

- Tex. Civ. Prac. & Rem. Code §101.021.
- *Leleaux v. Hamshire-Fannett Indep. Sch. Dist*., 835 S.W.2d 49 (Tex. 1992).
- *Tex. Dep't of Transp. v. Self*, No. 02-21-00240-CV (Tex. App. 2022).

Sovereign Immunity: Independent Contractors:

- Tex. Civ. Prac. & Rem. Code § 101.001(2).
- *Tex. Dep't of Transp. v. Self*, No. 02-21-00240-CV (Tex. App. 2022).
- *Olivares v. Brown & Gay Eng'g, Inc*., 401 S.W.3d 363 (Tex. App.- Houston 2013).
- *Fryday v. Michaelski*, 541 S.W.3d 345 (Tex. App.-Houston 2017).

Caps on Damages and Proportionate Responsibility:

- Tex. Civ. Prac. & Rem. Code § 101.023.
- Tex. Civ. Prac. & Rem. Code §§ 33.001 and 33.012.

Automated Motor Vehicle Operation:

- Tex. Transp. Code § 545.043.

Analysis

- *Sovereign Immunity: Motor-Driven Vehicles*—If property damage, personal injury, or death are proximately caused by an act, omission, or negligence of an employee who is operating or using a motor-driven vehicle, then sovereign immunity is waived and TxDOT can be held liable for the injury.
    - Sovereign immunity would have been waived if the plaintiff's damages arose from a TxDOT employee's operation or use of the vehicle. Because the automated TMA was operated by an ADS, no TxDOT employee physically operated the TMA or was in direct control of it. Therefore, TxDOT's sovereign immunity was preserved.
    - The plaintiff could argue that TxDOT's specifications for the TMA and feeding of data to it to use during operation constituted "operation or use" of the TMA. The law is currently unclear as to what type of control over a motor-driven vehicle is required to trigger a waiver of sovereign immunity. One line of cases does not require a state employee to be operating the equipment but does require a state employee to be giving precise direction to a third-party operator. The other line of cases provides that a waiver of sovereign immunity requires physical operation by a state employee.
    - Recently, the Court of Appeals of Texas, Second District, Fort Worth favored limiting governmental liability to situations where the government employee exerts "direct control" over the motor vehicle. Direct control entails both (a) close physical proximity to the vehicle while it is in operation and (b) direction so precise that the state agency employee tells the third party in physical control of the vehicle which direction and how far to move. TxDOT's specifications for the TMA and feeding of data to it to use during operation do not meet this test because no TxDOT employees were close in proximity to the TMA and the data and specifications did not precisely direct the TMA which direction and how far to move. Thus, TxDOT's sovereign immunity was not waived.
    - Even if the automated TMA were operated and used by a TxDOT employee, TxDOT would likely preserve its sovereign immunity. Texas courts have, thus far, limited the TTCA's waiver of liability to acts, omissions, and negligence of a government "employee" who is defined as "a person." This is complicated by provisions authorizing CAVs in Texas in the Texas Transportation Code, which considers an owner of an ADS as the operator of a CAV for purposes of determining compliance with state traffic and motor vehicle laws, regardless of whether a person is physically present in the vehicle while it is in operation. While the courts have not extended this view to the TTCA's waiver of immunity for operation and use of motor-driven vehicles and equipment, the courts could eventually find that it expresses the Legislature's intent to categorize CAV owners as "employees" for purposes of the TTCA.
- *Sovereign Immunity: Independent Contractors*—Texas statutes do not extend sovereign immunity to independent contractors or their agents or employees. As such, TxDOT's contractor cannot plead sovereign immunity to defend against the plaintiff's claim and may be liable for their injuries.

- The plaintiff may argue that the contractor was an "employee" of TxDOT, which would make its operation or use of the TMA attributable to TxDOT and waive TxDOT's sovereign immunity. The determination of whether a person is an employee or an independent contractor can be based on evidence of either a contract that explicitly assigns a right to control or, in the absence of a contract, evidence of actual control over the manner in which the work was performed. TxDOT did not actually control the TMA or the work that the contractor performed. However, the contract between the contractor that operated the TMA and TxDOT would have likely assigned a right to control.
- The independent contractor determination under the TTCA does not require that the contract provide for TxDOT to control every detail of the work performed. If there is evidence that TxDOT controlled the details of the contractor's work in determining the area from which work was to be performed in its contract and through instructions given by TxDOT employees, Texas courts would likely conclude that TxDOT's direction over the roadways on which the TMA was to be operated created a fact question (whether the contractor was an independent contractor or TxDOT's employee).
- TxDOT would have waived its sovereign immunity if its contract with the contractor, instructions from its employees to the contractor, automated TMA specifications, or data provided to the TMA determined exactly where the TMA would operate (i.e., on a specific two-lane road even though it is too large to fit in one lane). If the contract language, instructions from employees, data, and specifications were vague enough to provide the contractor control over where and how it operated and used the TMA, TxDOT would preserve sovereign immunity.

- *Caps on Damages and Proportionate Responsibility*—If the private vehicle driver could recover damages from TxDOT, their total monetary damages and prejudgment interest would be limited to $250,000 in money damages for each person, $500,000 for each single occurrence of bodily injury or death, and $100,000 for each single occurrence of injury to or destruction of property. The damages would be further limited under the principle of "proportionate responsibility," which allows a reduction in a plaintiff's recovery if the plaintiff was partially to blame for their injury, and bars a plaintiff's recovery of damages if their percentage of responsibility is greater than 50 percent.
  - The private vehicle driver would not be able to recover all of their asserted damages from TxDOT because their percentage of responsibility, while not greater than 50 percent, was sufficient to reduce the amount of damages by a percentage equal to their percentage of responsibility.
  - The TMA was being operated at low speeds at a standardized distance from other vehicles when the injured driver saw it coming, but not in time to avoid it. The driver may have been able to swerve to avoid the TMA in time had they seen the TMA in a more timely manner. If the driver did not see the TMA in time because the driver was using their cell phone or was otherwise distracted or under in the influence, then the vehicle owner may be held partially responsible for their injuries.
  - If the contractor is not determined to be an employee of TxDOT for purposes of the TTCA, it could be held partially responsible for the driver's injuries, further reducing TxDOT's liability.

Conclusion

- TxDOT did not waive sovereign immunity from the operation or use of a motor-driven vehicle (i.e., the automated TMA) because no TxDOT employee (nor any person) physically operated the TMA or exerted direct control over it.
- TxDOT may have waived sovereign immunity if its contract with the contractor, instructions from its employees to the contractor, automated TMA specifications, or data provided to the TMA assigned a right to control to the contractor and determined exactly where the TMA was to operate.
- TxDOT's contractor cannot plead sovereign immunity to defend against the plaintiff's claim and may be liable for their injuries.
- The damages owed to the driver of the vehicle struck by the automated TMA would be limited to a specific amount under the TTCA and reduced by a percentage equal to their share of responsibility for the crash, as evidenced by distractions or other factors that would slow their response time, as well as the level of control the contractor possessed over the TMA's operation and use.

Mitigation

- Contractual Terms:
    - TxDOT should consider, to the extent it has not already and to the extent feasible, eliminating contract provisions that assign a right to control over contractors and define them as employees for purposes of the TTCA. In this way, TxDOT would be able to shield itself from liabilities due to acts of its contractors. Contracts should not provide for TxDOT to control the details of a contractor's work in determining the area for which work is to be performed. For construction contracts where TMAs are used, TxDOT should consider elimination of any language that provides direction over the roadways on which the TMA is to be operated. These contract terms should be developed in conjunction with data protocols, specifications, and standard operating procedures that only provide control to contractors in situations where TxDOT is prepared to waive its sovereign immunity.
    - Additional requirements and clauses will need to be considered when contracting for CAV projects, including insurance. The CAV software itself may need to be insured, apart from the operator or owner. Further, this insurance may need to protect against specific functions such as braking, contacting emergency responders, or changing lanes. Specificity will be key in ensuring a vehicle is properly insured against all types of accidents, particularly an evolving technology like CAV. Further, there may be different insurance based on specific levels of automation.
    - Disadvantaged Business Enterprise (DBE) requirements mandate vendors and contractors to make a good faith effort to award a share of contracted work to certified DBEs in obtaining resources and services. Service participation is based on a contractor's labor or "time and efforts provided in a manner consistent with normal business practices that do not involve delivery of a specific end item." In the case of a CAV, the vehicle is working on behalf of the contractor and is still providing labor. It is unclear whether DBE requirements apply only to actual persons or also to CAVs. If CAVs are considered property, then it is unlikely that such guidelines would apply to them. Nonetheless, the DBE guidelines will still dictate what a person can do with CAVs. Therefore, DBE requirements likely do

not prevent the use of CAVs and robots for labor or service if a person is doing the negotiating, contracting, and documentation activities that are critical for meeting DBE requirements. This is likely further supported by the fact that CAVs will need to be monitored from a logistics perspective.

- Legislation:
  - Legislation may be needed to clarify the current ambiguity in common law regarding the type of government employee control over a motor-driven vehicle or motor-driven equipment that is required to trigger a waiver of sovereign immunity. The legislation could codify the Court of Appeals' limitation of governmental liability to situations where a government employee exerts direct control over the motor vehicle, which would entail both (a) close physical proximity to the vehicle while it is in operation and (b) direction so precise that the employee tells the third party in physical control of the vehicle which direction and how far to move. The legislation could also exempt TxDOT equipment and material specifications, as well as data fed to motorized vehicles and equipment, from what constitutes direct control.
  - Legislation could be proposed to revise Tex. Civ. Prac. & Rem. Code §101.021(1)(a) to provide that damages may be recovered from governmental units for property damage, personal injury, or death that "arises from the EMPLOYEE'S operation or use of a motor-driven vehicle or motor-driven equipment" (revision in underlined all caps). This would preserve sovereign immunity if fully autonomous CAVs are operated by ADSs (i.e., without a human operator).

Use Case #6—TxDOT Receives PIA Request for CAV Data

Facts

- TxDOT and the Texas Department of Public Safety receive data for each crash on state roadways.
- CAVs record data identifying personal information, location, and causation factors (e.g., skidding, braking, seat belt use, airbag deployment), as well as photos and videos of the crash, which show defects in roadways and work zones with damaged or missing signs.
- These source data are aggregated and anonymized by the OEM, who also stores all data, before being sent to TxDOT and State Police.
- The OEM mistakenly sends TxDOT the source data for a series of crashes, along with the aggregated and anonymized data.
- A PIA request is sent from an attorney to TxDOT for crash data related to one of those crashes.
- TxDOT sends both the source data and the aggregated and anonymized data to the attorney in response to the PIA request since the data were in its possession.
- TxDOT is sued for the release of confidential and proprietary information.

Source: TTI

Figure 7. Photo of an Accident Scene.

Issue

- Whether TxDOT is liable for negligent release of confidential and proprietary information when it inadvertently releases safety-related source data and aggregated/anonymized data sent by an OEM.
- Whether TxDOT can shield safety-related source data and aggregated/anonymized data from release in response to a PIA request.

Rule

Sovereign Immunity: Condition or Use of Tangible Property:

- Tex. Civ. Prac. & Rem. Code §101.021.
- *Harris County v. Shook*, 634 S.W.3d 942 (Tex. 2021).
- *University of Texas Southwestern Medical Center v. Rhoades*, 605 S.W.3d 853 (Tex. 2020).

Public Information Act:

- Tex. Gov't. Code §§ 552.001, 552.002, 552.108, 552.110, 552.130, 552.137, 552.147.
- Tex. Transp. Code §§ 550.062, 550.065, and 730.003.

Invasion of Privacy:

- *Boyles v. Kerr*, 806 S.W.2d 255 (Tex. App. 1991).
- *Billings v. Atkinson*, 489 S.W.2d 858 (Tex. 1973).

Analysis

- *Sovereign Immunity: Condition or Use of Tangible Personal Property*—The safety-related source data and aggregated/anonymized data likely do not constitute tangible personal property that waives TxDOT's sovereign immunity.

- Current statutes and the common law are silent on whether an agency's electronic data can be regarded as tangible personal property, as well as whether the condition or use of government-owned, -produced, or -shared data waives an agency's sovereign immunity if they cause personal injury or death. Though a hard drive or server containing electronic data may be tangible personal property, the condition or use of the information contained within data may not waive liability.
- If the data were considered tangible personal property, Texas courts could potentially deem their condition or use to have caused the injury to those affected by the inadvertent disclosure. TxDOT's sovereign immunity would be waived if the injury were caused by a condition or use of the tangible personal property (i.e., the injury and claim for damages were caused by a contemporaneous "action or service" [use] or "state of being" [condition] of the data), and TxDOT, were it a person, would be liable. Because the data would be used for a given purpose (i.e., law enforcement investigation, traffic safety) and in a condition (i.e., the source data were not anonymized or aggregated, but revealed personal information) that could cause injury, TxDOT would have a duty to exercise ordinary care and warn of the condition of the source data or make the data reasonably safe from public release after receiving actual notice of its possession of the source data. In this situation, TxDOT could meet this duty by notifying the public of the inadvertent release of the source data or, if possible, retroactively protecting personal information from causing injury before any damage can occur.

- *Public Information Act*—The OEM's source data from CAVs are not excepted from disclosure under the Texas PIA and other state statutes because they are not confidential motor vehicle records or information held by law enforcement or prosecutors nor information from law enforcement agencies' filing of accident forms. Similarly, the aggregated and anonymized data would be subject to release under the PIA since they do not retain any personal information or relate to law enforcement investigation of a crime.
  - The Texas PIA allows government agencies to withhold from public disclosure information that is considered to be confidential by law, either constitutional, statutory, or by judicial decision. This includes certain motor vehicle records issued by the state or another state or country, such as information related to driver licenses and permits, vehicle titles and registrations, and personal identification documents. The Texas PIA also excepts from release information held by law enforcement agencies and prosecutors, but not other public entities, including TxDOT, if the release would interfere with the detection, investigation, or prosecution of crime, even if the investigation does not result in conviction or adjudication.
  - Accident reports and certain information related to crashes that are written and filed by law enforcement agencies are deemed confidential and privileged under the Texas Transportation Code. While redacted accident reports may be released to certain requestors (including representatives of those involved in the crash), "personal information" from written CR-3 accident report forms is prohibited from release. This includes information that identifies a person, including photos and computerized images, as well as names, addresses, social security numbers, dates of birth, driver identification numbers, and license plate numbers, among other things.

- Because the CAV source data and aggregated data are compiled by the OEM and not a confidential motor vehicle record or part of law enforcement or prosecutorial detection, investigation, or prosecution of crime, they cannot be shielded from disclosure under the PIA.
- Because the CAV source data and aggregated data are not written and filed by law enforcement agencies or sourced from written CR-3 accident report forms, they cannot be shielded from disclosure under state statute.
- TxDOT should produce, upon a PIA request from an attorney, the anonymized and aggregated CAV crash data to the extent that the information constitutes "public information." Presumably, through the anonymization and aggregation process, the data do not retain any personal information or data related to law enforcement investigation of a crime. Thus, the aggregated and anonymized CAV crash data may be public information that "under a law or ordinance or in connection with the transaction of official business" is "written, produced, collected, assembled, or maintained" by or for a governmental unit where the governmental body owns the information or has a right of access to it. As "electronic communication created, transmitted, received, or maintained on any device…in connection with the transaction of official business," the CAV crash data may constitute public information, which can take the form of electronic communications, photographs, sound recordings, maps, and voice, data, or video representation held in computer memory.
- On the other hand, TxDOT should produce, upon a PIA request from an attorney, the anonymized and aggregated CAV crash data to the extent that the information could be considered the OEM's "trade secrets" under the PIA. Data that qualify as trade secrets are those that possess "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." In this case, the anonymized and aggregated CAV crash data do not qualify as trade secrets because they are sent to TxDOT and the Texas Department of Public Safety in the regular course of business.

- *Invasion of Privacy*—TxDOT's mistaken release of the source data in response to the attorney's PIA request would not be classified as an invasion of privacy due to the fact that the release was warranted under the PIA and other state statutes.
  - If the circumstances are such that a person of ordinary common sense would recognize that, if the TxDOT employee who responded to the PIA request did not exercise reasonable care in their conduct with regard to the known circumstances, their acts would place another in danger, the duty to use ordinary care to avoid such danger arises. In this case, the TxDOT employee who responded to the PIA request could not have foreseen the likelihood that emotional injury to the driving public might result from their oversight because the PIA and other state laws do not shield the data from release.

Conclusion

- TxDOT did not waive its sovereign immunity because electronic data have not been deemed tangible personal property that waive TxDOT's sovereign immunity. However, if the data were considered tangible personal property, Texas courts could potentially deem their condition or use to have caused the injury to

those affected by the inadvertent disclosure, which would waive TxDOT's sovereign immunity and trigger a duty to exercise ordinary care and warn of the condition of the data or make it reasonably safe from public release after receiving actual notice of its possession of the source data.

- Even if sovereign immunity is waived, TxDOT would likely not be liable for negligent release of confidential and proprietary information by inadvertently releasing source data from CAVs sent by an OEM in response to the attorney's PIA request. Though the OEM's source data and aggregated data from CAVs may contain personal information, they are not shielded from release under the Texas PIA or other state statutes.

Mitigation

- *Data Protected Under the PIA*—TxDOT may shield source data (similar to the CAV crash data in this use case) from release in response to a PIA request if such information is deemed confidential by law, either constitutional, statutory, or by judicial decision. This includes:
    - Certain motor vehicle records, accident reports, and personal information related to crashes that are written and filed by law enforcement agencies, all of which are deemed confidential and privileged by statute.
    - Information obtained from global positioning system technologies, contact tracing, or technologies designed to obtain biometric identifiers that identify an individual or the individual's location without the individual's written or electronic consent, unless required or permitted by federal or state law or for law enforcement purposes.
    - Email addresses, social security numbers, and information in motor vehicle records, unless consent is provided by the subject of the information.
    - Information held by a law enforcement agency if the release would interfere with the detection, investigation, or prosecution of a crime, even if the investigation does not result in conviction or adjudication. This may include information related to crash causation factors (e.g., skidding, braking, seat belt use, airbag deployment).
- *Operational Measures*—As recommended in Use Case #3, TxDOT should consider implementing operational measures to prepare for the potential future flood of data from CAVs that may strain the agency's capacity to address them within defined notice periods and open TxDOT up to potential tort liability.
    - TxDOT and other government agencies should become more familiar with CAV sensor data while the industry is nascent and establish processes and standards that can evolve over time, including processes for addressing reports of roadway defects to accommodate CAV data and reports about conditions. It may be most advantageous for the data to be communicated from the vehicle to the OEM (rather than directly to the agency) in the form of reports scheduled at regular intervals. A regular reporting plan from the OEM to the agency will allow the OEM to decide what conditions to report, mimicking the current process where the public selectively reports roadway conditions. Then, agencies can add the service requests into their current system and make decisions on how to grade and prioritize the requests for maintenance.

- Regardless of whether data are collected directly by transportation departments or received from third-party data owners, the processes for acquiring and processing crash-related data would benefit from review and development of a framework and set of protocols for managing and protecting data that, if inadvertently released, would expose personal information or trade secrets to the public. These actions would minimize liability for the transportation agency, protect the privacy interests of those whose personal information may be captured in the data, and protect the proprietary interests of those whose technology and business systems were used to manufacture and generate the data. Such actions should include, at minimum, a system of warning the public of the potential for unintended release of personal information collected by CAV OEMs.

Use Case #7—Transit Operator's Operation of Public CAV Bus for General Use

Facts

- A transit operator operates a CAV bus on a state highway via a TxDOT-approved route (approved as part of CAV testing in transit operations).
- The transit operator provides service directly with its own employee as the transit agency safety operator who completed safety training prior to the date of the incident.
- TxDOT assisted in administrating federal funding as well as awarding state funding for capital purchase in acquiring the CAV bus.
- TxDOT infrastructure delivers data to the CAV bus, and the bus collects and sends real-time information to TxDOT.
- The CAV bus malfunctions and is in a crash. The malfunction was not due to reliance on the TxDOT infrastructure data but to the CAV's inability to interpret that there was debris on the roadway.
- The debris was reported to TxDOT two hours before the incident, and crews were on the way the remove it.
- The CAV bus hits the debris, and bus passengers are injured due to the sudden stop.
- The transit agency safety operator for the CAV bus was watching a video on their phone rather than monitoring operations per safety guidelines.
- Passengers were seated normally in their seats (non-standing) and not buckled in (since requiring passengers to buckle their seatbelts is not enforced by the safety operator per transit agency policy) prior to the crash.

Source: TTI

Figure 8. Photo of a Bus on a TxDOT Highway.

Issue

- Whether TxDOT and the transit operator are liable for injuries to transit passengers during a crash when a CAV bus (operated by a transit operator supported by TxDOT and relying on TxDOT data) malfunctions on the highway.

Rule

Federal Transit Funding in Texas:

- FTA Circular 5100.1.

Sovereign Immunity—Operation and Use of Motor-Driven Vehicles:

- Tex. Civ. Prac. & Rem. Code §101.021(1).
- *Mount Pleasant Indep. Sch. Dist. v. Estate of Linburg*, 766 S.W.2d 208 (Tex. 1989).
- *Dallas Area Rapid Transit v. Whitley*, 104 S.W.3d 540 (Tex. 2003).
- *University of Texas Southwestern Medical Center v. Rhoades*, 605 S.W.3d 853 (Tex. 2020).
- *VIA Metropolitan Transit v. Meck*, 620 S.W.3d 356 (Tex. 2020).

Caps on Damages and Proportionate Responsibility:

- Tex. Civ. Prac. & Rem. Code §101.023.
- Tex. Civ. Prac. & Rem. Code §§ 33.001 and 33.012.

Sovereign Immunity: Special Defects:

- Tex. Civ. Prac. & Rem. Code § 101.022.
- *Gunn v. Harris Methodist Affiliated Hosp*., 887 S.W.2d 248 (Tex. App.—Fort Worth 1994).
- *DeWitt v. Harris Cnty*, 904 S.W.2d 650 (Tex. 1995).
- *Texas Dept. of Transp. v. Ramming*, 861 S.W.2d 460 (Tex. App.—Houston [14th Dist.] 1993).
- State Dept. of Highways and Public Transp. v. Payne, 838 S.W.2d 235 (Tex. 1992).

Joint Enterprise:

- Shoemaker v. Estate of Whistler, 513 S.W.2d 10 (Tex. 1974).
- Texas Dept. of Transp. v. Able, 35 S.W.3d 608 (Tex. 2000).
- Tex. Local Gov't. Code §§ 271.151 and 271.160.

Products Liability:

- Tex. Civ. Prac. & Rem. Code §§ 82.002, 82.003, 82.008.
- Tex. Transp. Code § 545.453.

Analysis

- *Federal Transit Funding in Texas*—As a funding partner, TxDOT's responsibilities for allocating and administering FTA grant funds to local recipients are generally consistent between federal transit programs.
    - TxDOT is typically the designated funding recipient for certain regularly occurring FTA programs, while transit operators or local governments are either direct recipients or subrecipients.
    - TxDOT can pass through funds to subrecipients, at which point the subrecipients enter into a written agreement with TxDOT stating they will comply with its obligations to satisfy requirements of the grant program agreement.
    - TxDOT also holds responsibilities for designated recipients of federal transit funding.
- *Sovereign Immunity: Operation and Use of Motor-Driven Vehicles*—The transit operator, but not TxDOT, waived its immunity to liability for injuries to the CAV bus passengers as a result of the crash because its employee, and not TxDOT's, operated and used the vehicle that proximately caused the injuries.
    - Because the CAV bus malfunctioned due to the failure of sensors that did not detect the debris in the roadway and the negligence of the transit agency safety operator, TxDOT did not waive its sovereign immunity under the TTCA's exception for employee operation and use of motor-driven vehicles. TxDOT's responsibilities were strictly related to administrating funding, approving the route, and providing data on the roadway infrastructure, which was accurate and not a proximate cause of injuries. No TxDOT employee was engaged in the operation or use of the bus.
    - The transit operator's employee, on the other hand, was involved in the operation and use of the CAV bus. In watching a video on their phone rather than monitoring operations per safety guidelines, the transit agency safety operator for the CAV bus breached their duty of care to the passengers. The employee was involved in the "operation or use of a motor-driven vehicle" while "acting within [their] scope of employment by putting the CAV bus into action or service. Even though the passengers were not buckled by their own choosing, neither use of the seat belts nor enforcement by the safety operator were required under the transit agency's policy. Sovereign immunity was waived by the transit agency because the operation and use of the CAV bus by the employee proximately caused the passengers' injuries.
    - Governmental units providing transit services waive their immunity under the motorized vehicle and equipment exception to the TTCA and are subject to negligence under the duty of care that a common

carrier holds. Thus, the transit agency operating the CAV bus can be found liable for "slight negligence," which under the common law imposes a duty to exercise a high degree of care on transit providers. This duty would not make the agency strictly liable as insurers or require them to employ the highest degree of care, but the agency would owe a duty to its passengers to act as "a very cautious and prudent person" would act under the same or similar circumstances. In this case, the agency's employee did not act cautiously or prudently in not complying with agency guidelines, rendering it liable for the passengers' injuries.

- *Caps on Damages and Proportionate Responsibility*—If the bus passengers could recover damages from the transit operator and TxDOT, their total monetary damages and prejudgment interest would be limited to $250,000 in money damages for each person, $500,000 for each single occurrence of bodily injury or death, and $100,000 for each single occurrence of injury to or destruction of property. Their damages would be further limited under the principle of "proportionate responsibility," which allows a reduction in a plaintiff's recovery if the plaintiff was partially to blame for their injury and bars a plaintiff's recovery of damages if their percentage of responsibility is greater than 50 percent.
    - The transit operator could show the extent to which the passengers injured had some level of responsibility for not being buckled or otherwise riding unsafely in order to show a portion of responsibility on the passengers.
    - The operator could also demonstrate that the manufacturer of the CAV bus was partially responsible for installing technology on the CAV bus that failed to recognize the obstruction in the roadway.
- *Sovereign Immunity: Special Defects*—The debris in the roadway was a special defect that waived TxDOT's sovereign immunity under the TTCA, but TxDOT did not breach its duty because crews were on the way to remove the debris within a reasonable time.
    - The debris in the roadway would not have constituted a premises defect because, unlike a pothole, it was not a condition of the roadway itself that was unsafe. As such, TxDOT would not be held to a duty to exercise ordinary care and warn of the condition or make it reasonably safe after receiving actual notice of the condition.
    - Instead, the debris was an obstruction in the roadway—a special defect—that posed a threat to ordinary users of the TxDOT roadway. This presented a higher duty for TxDOT to warn of the debris or remove it after receiving either actual or constructive notice of the potential danger it presented.
    - TxDOT had received reports of the debris two hours before the bus crash, so the agency knew of the potential danger presented by the obstruction. Thus, TxDOT had a duty to warn of the debris or remove it within a reasonable time.
    - Because TxDOT knew of the debris, which was an act of a third party and not a TxDOT employee, TxDOT would be allowed a reasonable time under the law to provide notice or remove the debris. Indeed, at the time of the bus crash (two hours after receiving notice of the debris), TxDOT had dispatched personnel that were on the way to remove the debris. Thus, TxDOT had not breached its duty to the bus passengers.

- *Joint Enterprise*—TxDOT's approval of the route for the CAV bus testing and its funding agreement with the transit operator may indicate a joint enterprise, which would waive sovereign immunity for TxDOT and render the agency liable for injuries to the passengers. However, if the transit operator were a local government entity, the contract entered into by the operator and TxDOT would not be considered a joint enterprise for liability purposes.
    - Under the theory of joint enterprise, liability extends to each party involved in a joint enterprise as agents of the other. As such, each is held responsible for the negligent act of the other. The Texas Supreme Court has held that the Legislature intended that a governmental unit enjoying the benefits and advantages of a joint enterprise would also be subject to the same obligations and liabilities that a private person would be if they were engaged in a joint enterprise, so state agencies waive sovereign immunity for the negligence of their joint enterprise partners.
    - The relationship between TxDOT and the transit operator may have been a joint enterprise involving governmental units engaged in (a) an express or implied agreement with each other related to TxDOT's approval of the bus route, administration of federal funding, and award of state funding for capital purchase in acquiring the CAV bus; (b) a common purpose of CAV bus transit services carried out by the group; (c) a "community of pecuniary interest in that purpose" among the group's members, as evidenced by the exchange of state and federal funds; and (d) an "equal right to a voice in the direction of the enterprise," giving an equal right to control of the joint enterprise.
    - If the transit operator were a local government entity (i.e., a municipality, public school or junior college district, or special-purpose district or authority, but not a county or unit of state government), state statute would have determined that TxDOT's agreement with it was not a joint enterprise for liability purposes. Thus, if the transit operator was a local government entity, TxDOT did not waive its sovereign immunity due to the negligence of the transit operator.
- *Products Liability*—The transit agency and TxDOT could pursue the CAV bus manufacturer under products liability laws in the state but would find it challenging due to the statute's relative friendliness to manufacturers and sellers, encouraging the placing of products and component parts thereof into the stream of commerce.
    - To attach liability to the manufacturer of the CAV bus, the transit agency and/or TxDOT would need to prove, by a preponderance of the evidence, that (a) there was a safer alternative design and (b) the defect was a producing cause of the passengers' personal injuries. In doing so, the transit agency and/or TxDOT would have to overcome the rebuttable presumption that the manufacturer is not liable for any injury caused by an aspect of the design of the bus if the manufacturer can prove (a) compliance with mandatory federal safety standards or regulations adopted and promulgated at the time of production; or (b) the product was granted licensing or approval by a federal authority. If the seller took part in the manufacturing of the vehicle or knew of the defect, they could be pursued for liability too.
    - Currently, there is no federal regulatory framework for the manufacturing or design of CAVs or related technology systems, and the FMVSS have not been updated to mandate safety standards for CAVs. In addition, the CAV bus was likely not granted licensing or approval by a federal authority. Thus, the

transit agency and/or TxDOT would be able to overcome the manufacturer's rebuttable presumption of non-liability.

- However, the transit agency and/or TxDOT would find it challenging to prove that the manufacturer had knowledge of the inadequate design of the technology on the CAV bus that failed to recognize the obstruction in the roadway. As long as the vehicle met industry standards and guidance at the time, and the manufacturer was not aware of the defect, the transit agency and/or TxDOT would not be able to prove that the manufacturer was liable.

Conclusion

- The transit operator waived immunity to liability for injuries to the CAV bus passengers as a result of the crash because its employee operated and used the vehicle that proximately caused the injuries.
- TxDOT may have waived its sovereign immunity as a party to a joint enterprise with the transit agency when TxDOT approved the route for the CAV bus testing and entered into a funding agreement with the transit operator. However, if the transit operator were a local government entity, as defined in state statute, no joint enterprise would exist for liability purposes and TxDOT would not have waived sovereign immunity.
- The transit agency and TxDOT may be able to reduce damages awarded to the plaintiffs by proving that the passengers behaved in a way, prior to the collision, that contributed to their injuries.
- The transit agency and TxDOT could also reduce damages awarded to the plaintiffs by proving the manufacturer was partially responsible, asserting there was a safer alternative design for the CAV bus that would have detected the debris and the defect caused the passengers' injuries, or the bus design did not comply with federal standards or was approved by a federal agency. However, this would be challenging to prove by a preponderance of evidence in the absence of federal standards for CAVs.

Mitigation

- *Legislation*—There are two legislative areas that may limit potential liability and damages in this circumstance:
  - As provided in the analysis for Use Case #5, legislation could be proposed to revise Tex. Civ. Prac. & Rem. Code §101.021(1)(a) such that damages may be recovered from governmental units for property damage, personal injury, or death that "arises from the EMPLOYEE'S operation or use of a motor-driven vehicle or motor-driven equipment" (revision in underlined all caps). This would conform to the court's current interpretation of the law and preserve sovereign immunity if fully autonomous CAVs are operated by the ADS without a human operator.
  - Legislation could be proposed to preserve TxDOT's sovereign immunity when it enters into joint enterprises with transit operators. One way to do this would be to amend Tex. Local Gov't. Code § 271.151 such that the definition for a "local government entity" expressly includes as a "special-purpose district or authority" all transit operators in the state, such as metropolitan rapid transit authorities, regional transportation authorities, municipal transit departments, county mass transit authorities, rural and urban transit districts, and other entities described in Subtitle K (Mass Transportation) of Title 6 of the Tex. Transp. Code. This would render any contract entered into by

transit operators, including those TxDOT holds with them, not a joint enterprise for liability purposes under Tex. Local Gov't. Code § 271.160. The other means of preserving TxDOT's sovereign immunity for joint enterprises would be to amend the TTCA—specifically, Tex. Civ. Prac. & Rem. Code § 101.0211—by adding agencies described in Subtitle K (Mass Transportation) of Title 6 of the Tex. Transp. Code to the list of entities that the common law doctrine of vicarious liability due to participation in a joint enterprise does not impose liability upon.

Conclusion

The use case analyses sought to understand what legal issues arose from seven possible near-term scenarios; how state statutes and case law applied to those issues; what legal conclusions could be drawn from the analyses; and what legal, policy, or operational strategies TxDOT could pursue to address potential liabilities. The use cases allowed the TTI research team to explore a range of legal topics, from sovereign immunity to data protection to privacy. They also provided opportunities to research other areas of law, including design immunity, federal preemption, workers' compensation, the Texas Deceptive Trade Practices Act, use of unmanned aircraft, the Texas Public Information Act, and products liability. The areas of law addressed in each use case analysis are shown in Table 18.

Table 18. Areas of Law Addressed in Use Case Analyses.

Legal Issues		Use Case						
		1	2	3	4	5	6	7
Sovereign Immunity	Operation and Use of Motor-Driven Vehicles and Equipment				✓	✓		✓
	Condition or Use of Tangible Property	✓	✓	✓			✓	
	Premises Defects	✓		✓				
	Special Defects & Traffic Signs, Signals, and Warning Devices	✓	✓					✓
	Joint Enterprise & Independent Contractors		✓			✓		✓
	Caps on Damages & Proportionate Responsibility	✓				✓		✓
Data	Data Management		✓	✓				
	Data Privacy				✓			
Discretionary Functions (Design Immunity)		✓						
Federal Preemption and Vehicle Safety Certification		✓						
Workers' Compensation			✓					
Texas Deceptive Trade Practices Act			✓					
Use of Unmanned Aircraft					✓			
Public Information Act							✓	
Invasion of Privacy							✓	
Federal Transit Funding in Texas								✓
Products Liability								✓

Sovereign Immunity

A common theme in performing all the use case analyses was first asking the threshold question of whether TxDOT waived its sovereign immunity. In this way, the basis for analysis was the TTCA, which narrowly limits liability for governmental agencies like TxDOT to claims where an intentional or negligent act of an employee proximately causes property damage, injury, or fatality.

The diagram in Figure 9 shows a flowchart that simplifies this initial analysis, starting with the question of whether TxDOT has waived or not waived its sovereign immunity in the facts presented in the use case

scenario. For those use cases where TxDOT has waived sovereign immunity, the waiver was based on an employee's operation and use of a motor vehicle or motorized equipment, dangers presented by infrastructure or data (e.g., condition or use of property; premises defects; special defects; traffic signs, signals, and warning devices), or both.

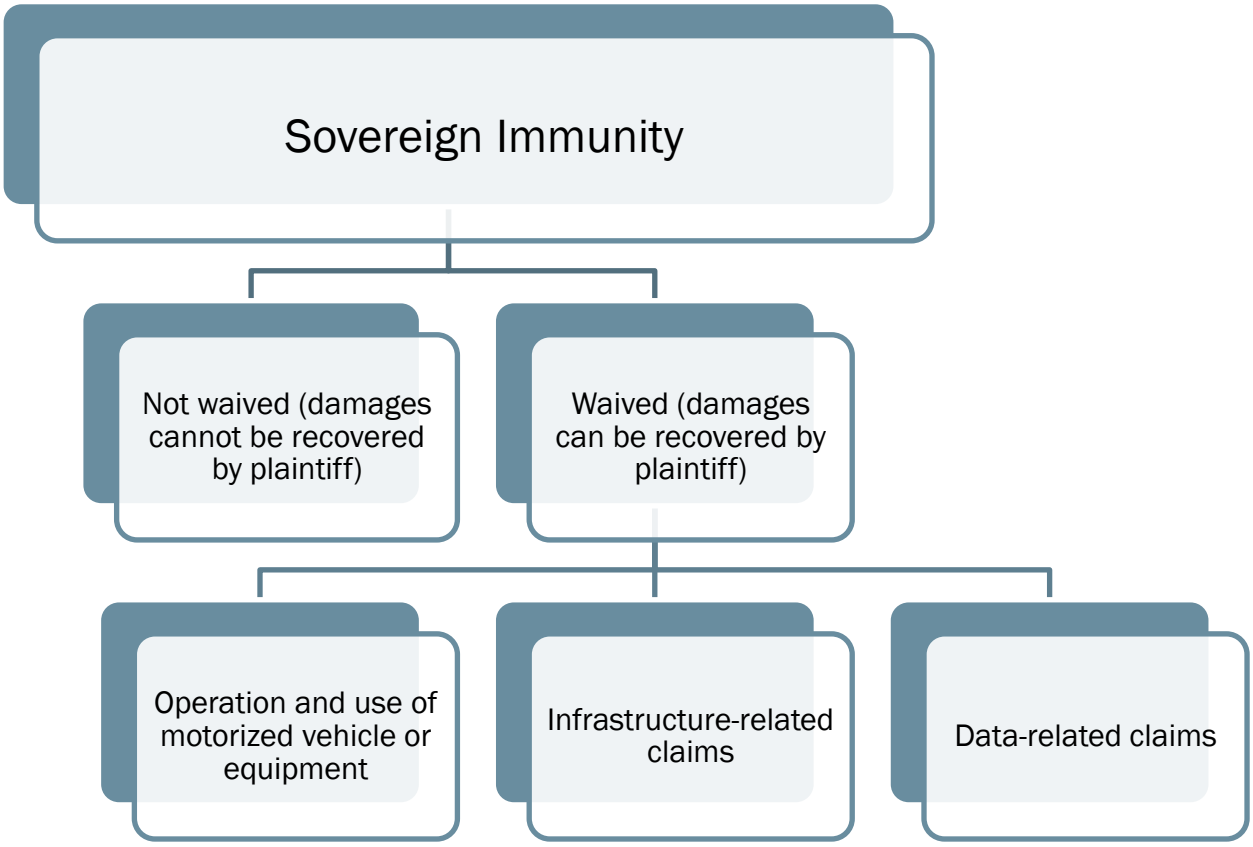

Figure 9. Flowchart of Sovereign Immunity Analysis.

Liability was likely to attach to TxDOT if the facts comprising the use case involved government-owned vehicles or equipment; condition or use of property; premises defects; special defects; traffic signs, signals, and warning devices; or the acts of third parties. Otherwise, TxDOT was likely protected by sovereign immunity. In cases where sovereign immunity had been waived, plaintiffs could recover damages from TxDOT if they could prove that the agency breached its duty to users of the roadway.

Mitigation Strategies

Each use case presented strategies that TxDOT may consider to address current gaps in the law or mitigate potential liabilities presented by the operation of CAVs in the state. While Texas laws are already fairly protective of state agencies and may not need to change for TxDOT to avoid tort liability from CAVs, TxDOT may want to introduce more uniform and stringent practices regarding data handling than it has in place today.

Below is a summary of the legislative and operational mitigation strategies that TxDOT may consider in order to best prepare for managing or avoiding the risks identified in this task. Legislative mitigation strategies mostly consist of ways to amend existing sections of the Texas Civil Practices and Remedies, Transportation, and Local Government Codes to expand or narrow definitions or requirements related to preserving or strengthening TxDOT's sovereign immunity. Operational mitigation strategy recommendations fall into three main categories: data management, unmanned aerial vehicles, and contracting. All strategies are embedded within the use case analyses, as are their rationales.

Legislative Strategies

- Amend Tex. Civ. Prac. & Rem. Code § 101.022 and § 101.060 to expressly bar the extension of the waiver of sovereign immunity and higher duty of care to I2V or smart infrastructure devices, data, and communications.
- Amend Tex. Transp. Code, Title 7, Subtitle C, Chapter 544 to expressly extend the authority to place and maintain I2V or smart infrastructure devices to TxDOT and local authorities, and to require CAV compliance with traffic control data from such devices.
- Amend Tex. Civ. Prac. & Rem. Code § 101.021 to expressly define "tangible personal property" to exclude electronic data that are owned, produced, or shared by governmental units.
- Amend Tex. Civ. Prac. & Rem. Code § 101.001 to exclude drones from the scope of motor vehicles or equipment for purposes of the TTCA.
- Amend the TTCA to clarify the current ambiguity in common law regarding the type of government employee control over a motor-driven vehicle or motor-driven equipment that is required to trigger a waiver of sovereign immunity. The legislation could limit governmental liability to situations where a government employee exerts direct control over the motor vehicle or equipment. The legislation could also exempt TxDOT equipment and material specifications, as well as data fed to motorized vehicles and equipment, from what constitutes direct control.
- Amend procurement statutes to clarify that DBE requirements likely do not prevent the use of CAVs and robots for labor or service if a person is doing the negotiating, contracting, and documentation activities that are critical for meeting DBE requirements.
- Amend Tex. Civ. Prac. & Rem. Code §101.021(1)(a) to provide that damages may be recovered from governmental units for property damage, personal injury, or death that "arises from the EMPLOYEE'S operation or use of a motor-driven vehicle or motor-driven equipment" (revision in underlined all caps). This would preserve sovereign immunity if fully autonomous CAVs are operated by ADSs and not a human.
- To preserve TxDOT's sovereign immunity where it enters into joint enterprises with transit operators, either (a) amend Tex. Local Gov't. Code § 271.181 such that the definition for a "local government entity" expressly includes entities described in Subtitle K (Mass Transportation) of Title 6 of the Tex. Transp. Code or (b) amend Tex. Civ. Prac. & Rem. Code § 101.0211 to add agencies described in Subtitle K (Mass Transportation) of Title 6 of the Tex. Transp. Code to the list of entities that the common law doctrine of vicarious liability due to participation in a joint enterprise does not impose liability upon.

Operational Strategies

- Data Management:
  - Review and develop a framework and set of protocols for managing and protecting data that, if inadvertently released, would expose personal information or trade secrets to the public. These actions would minimize liability for the transportation agency, protect the privacy interests of those whose personal information may be captured in the data, and protect the proprietary interests of those whose technology and business systems were used to manufacture and generate the data.
  - Assess (a) I2V communications technologies for CAVs to receive information from highway agencies that are today communicated to human drivers through traffic signs, signals, and warning devices; (b) V2I communications technologies to receive information from CAVs regarding roadway and traffic conditions; and (c) data storage, aggregation, and maintenance products and practices to receive, archive, analyze, act on, and/or dispose of I2V and V2I data. From these assessments, develop and implement policies and protocols to receive, store, maintain, and disseminate this information to ADSs, as well as to generate service requests and alert maintenance and operations personnel of the defects, inoperability, or damage to transportation assets.
  - Consider adopting data dissemination and management standards as part of the work zone traffic management planning process. Adopt data inspection measures similar to the construction management and work zone inspection practices in place today. These provisions may also be incorporated into construction and data management contracts to ensure that data are correct when disseminated and that vendors have proper processes in place to catch incorrect data.
  - Anticipate receiving more but better information about roadway conditions that will help prioritize repair work more efficiently, and therefore invest in information technology capabilities and increasing staff capacity and ability to access, analyze, and manage data.
  - Test and develop protocols for making agency data available to OEMs for CAV applications, using as examples experiments with providing work zone data to OEMs so that they can notify CAVs and their operators of changes in real time.
  - Become more familiar with CAV sensor data while the industry is nascent and establish processes and standards that can evolve over time, including processes for addressing reports of roadway defects to accommodate CAV data and reports about conditions. It may be most advantageous for the data to be communicated from the vehicle to the OEM (rather than directly to the agency) in the form of reports scheduled at a regular interval. A regular reporting plan from the OEM to the agency will allow the OEM to decide what conditions to report, mimicking the current process where the public selectively reports roadway conditions. Then, agencies can add the service requests into their current system and make decisions on how to grade and prioritize the requests for maintenance.
  - Provide CAVs and their passengers actual notice or warnings of premises defects. These measures could include alerts on the vehicle's display or passenger's communication device as well as data provided to ADSs warning of the dangerous condition and advising how to avoid it.

- Designate a data management officer and include in contracts with data vendors a provision requiring the vendors to meet the agency's security controls and provide evidence that they meet the security controls.

- Unmanned Aerial Vehicles:
  - Test placing a sign on a roadway alerting travelers to the use of drones for inspection purposes where such inspections are taking place. The sign would provide actual notice to drivers that images are being captured and used for road and bridge safety purposes.
  - Consider creating an agency procedure where drone operations to inspect infrastructure are only conducted on a section of roadway(s) that has been closed to traffic, regardless of roadway size or number of lanes.
  - Consider installing AI software within the information management system of the drone's image-capturing capacity that can screen UAV-captured photos for people and immediately delete or blur faces in photos before any TxDOT representatives see the photos or before they are stored on TxDOT servers.

- Contracting:
  - Consider eliminating contract provisions that assign a right to control to contractors and define them as employees for purposes of the TTCA. In this way, TxDOT would be able to shield itself from liabilities due to acts of its contractors. Contracts should not provide for TxDOT to control the details of a contractor's work in determining the area from which work is to be performed. For construction contracts where TMAs are used, TxDOT should consider elimination of any language that provides direction over the roadways on which the TMA is to be operated. These contract terms should be developed in conjunction with data protocols, specifications, and standard operating procedures that only provide control to contractors in situations where TxDOT is prepared to waive its sovereign immunity.
  - Consider adding requirements and clauses when contracting for CAV projects, including insurance. The CAV software itself may need to be insured, apart from the operator or owner. Further, this insurance may need to protect against specific functions such as braking, contacting emergency responders, or changing lanes. Specificity will be key in ensuring a vehicle is properly insured against all types of accidents, particularly an evolving technology like CAV.

6. Peer Symposium

The purpose of the March 7, 2023, Peer Symposium was to understand experiences of stakeholders in the context of a moderated group discussion. The TTI research team virtually convened a group of practitioners involved in the testing and deployment of CAV technologies on behalf of public agencies and that could speak to the issues of tort liability, invited symposium participants to share their experiences about issues that arose in their jurisdictions and what approaches were taken to address those issues, and video-recorded and professionally edited the event and made the event available through YouTube and a web-based tool.

The TTI research team approached the Peer Symposium with the goal of soliciting feedback on project findings and exploring related ideas from knowledgeable and targeted attendees. This effort was intended to gather information and discuss themes and issues that have arisen to date on the project. For the reasons noted below, the research team views the Peer Symposium as a success. It accomplished the goals of aiding the team in ground-truthing existing findings and building a more robust bank of information on CAV liability issues through the lens of TxDOT.

Methodology

Event Process and Planning

To prepare for the event, the research team conducted multiple internal strategy meetings, created planning documents, and rehearsed hosting and administering the event ahead of time. This preparatory work helped ensure the effective delivery of the information presented to lend insights into future project deliverables. The advance planning also helped ensure the virtual event went as smoothly as possible by considering the unknowns that could arise with virtual platforms.

A key consideration for the research team was how to align the Peer Symposium with previous project findings. Thoughtful event pacing was the solution; the team planned the agenda (Table 19) such that the event would start by explaining project findings to date, transition into expert panels, and conclude with virtual breakout rooms to support audience engagement.

Table 19. Peer Symposium Agenda.

Time	Activity	Facilitator/Presenter
60 minutes total	**Part 1:** Setting the Stage	
5 minutes	Opening & Welcome • Introductions (Presenters Only)	Gretchen Stoeltje, TTI
15 minutes	Project Focus and Findings to Date • Mentimeter Poll 1 *Poll #1: In your experience, what CAV liability challenges are the most difficult to deal with?*	Billy Hwang, TTI
40 minutes • 5 mins. each for introduction • 25 mins. for discussion questions • 5 mins. for Q&A	How are CAVs operating in Texas? • Introduction • Q&A	• Moderator: Jackie Beckwith, Stantec • Panelists: Darran Anderson, TxDOT & Tom Bamonte, NCTCOG

Time	Activity	Facilitator/Presenter
5 minutes	Break	
75 minutes total	Part 2: Legal Considerations in Focus	
5 minutes	Overview of both panels and quick introductions of panels	Greg Rodriguez, Stantec

35 minutes	Panel 1: What are key liabilities around CAVs?	• Panel 1 Moderator: Greg Rodriguez, Stantec
		• Panel 1 Panelists:
		  ○ Patty Doersch, Squire Patton Boggs
		  ○ Melody Drummond-Hansen, BakerHostetler
		  ○ William Hubbard, University of Baltimore School of Law

35 minutes	Panel 2: Sovereign Immunity and Risk Mitigation	• Panel 2 Moderator: Greg Rodriguez, Stantec
		• Panel 2 Panelists:
		  ○ Hyattye Simmons, Judge
		  ○ Pete Calcaterra, Connecticut DOT
		  ○ Ben Lewis, Edge Case Research

65 minutes total	Part 3: Virtual Roundtables & Close-out	
5 minutes	Introduce break out groups and send participants to them	Greg Rodriguez, Stantec
40 minutes	Virtual Roundtables	• Table Leaders
20 minutes	Conclusion/Wrap-up • PollEverywhere Poll 2 – Billy Hwang, TTI Poll #2: Which of the presented mitigation strategies will be the most effective for your organization (select up to 3 solutions)? • Break-out Report Out – Greg Rodriguez, Stantec • Next Steps – Gretchen Stoeltje, TTI	• Gretchen Stoeltje and Billy Hwang, TTI • Greg Rodriguez, Stantec

At the same time that the agenda was developed, the research team produced a run of show document to provide expectations and direct the moderators for each portion of the agenda. The research team also developed a PowerPoint presentation to guide the Peer Symposium ahead of the event.

Throughout the Peer Symposium, the research team administered live, virtual polls to incorporate dynamic audience interaction. The research team used PollEverywhere as the polling platform for the event to ask questions and collect input from participants.

When considering appropriate speakers for each panel discussion, the research team identified individuals knowledgeable about CAV activities in Texas along with attorneys or those working on issues directly related to liability and risk mitigation. The research team made the strategic decision for Darran Anderson and Tom Bamonte to participate in Part 1 of the Peer Symposium to further focus the discussion on Texas and ensure the audience had an understanding of ongoing activities around CAVs within Texas.

The people listed below graciously volunteered their time to support the virtual event and contribute their knowledge:

- Darran Anderson, TxDOT.
- Tom Bamonte, North Central Texas Council of Governments (NCTCOG).
- Melody Drummond-Hansen, BakerHostetler.
- Patricia Doersch, Squire Patton Boggs.
- William Hubbard, University of Baltimore School of Law.
- Hyattye Simmons, Municipal Judge for the City of Combine, TX.
- Ben Lewis, Edge Case Research.

Peter Calcaterra from the Connecticut Department of Transportation had been scheduled to participate in a panel discussion. Unfortunately, he gave notice the day of the symposium that he was not able to participate due to unforeseen circumstances.

The research team organized multiple panel preparatory calls once speakers were finalized to review the proposed run of show and suggested questions. Speakers were advised that audience participation would be sought throughout the event via the virtual chat box, and the list of invitees was created with that level of engagement in mind.

Invitees and Attendees

When constructing the event invite list, the research team selected CAV industry stakeholders from a variety of sectors to ensure that audience engagement would be rich, diverse, and robust. Attendees included CAV developers, state DOT representatives, interest group spokespeople, insurance experts, academia, and attorneys; many of these individuals attended at least part of the symposium if not the entire event.

Invitees received a mass email invitation and personalized follow-up emails before the date of the Peer Symposium. All registered attendees received a reminder email the day before the event. The event was not shared publicly, but instead intended to provide a curated attendance list to ensure attendees, including those from TxDOT, with working experience around CAVs were in the audience. Additionally, the research team did not want the focus of the Peer Symposium to be advocacy of specific positions, but to ensure information gathering based on data and experience.

Attendance remained at 45 participants for the majority of the event and only dropped to 33 participants after breakout rooms concluded. Again, the research team views this as a large success considering this was a virtual 3.5-hour event.

Summary of Symposium Discussions

Following an opening, welcome, and introductions, the research team provided a brief overview of project findings to date. By sharing this information, attendees could immediately engage, orient their understanding of the event, and contribute accordingly. The research team asked attendees to insert any questions or comments into the videoconference chat box at any point throughout the symposium, and the audience participated accordingly. Throughout the entire 3.5-hour event, the chat box was very active. Members of the research team picked up on threads and asked follow-up questions in the chat to support information gathering in support of the project. The level of audience engagement was notable and gratifying.

The research team handled the start of the event and the findings review, while also being responsible for the back-end logistics and managing the panels, breakout rooms, and poll administration.

Panel 1: How are CAVs operating in Texas?

The first panel featured Darran Anderson of TxDOT and Tom Bamonte of NCTCOG. Jackie Beckwith of Stantec moderated the panel and began the conversation by sharing the various slides both Mr. Anderson and Mr. Bamonte had prepared. Their slides reviewed the current legislative environment in Texas, where CAV deployments had taken place and are taking place, and provided insight into how TxDOT and NCTCOG are collaborating with others to invite CAV operations in Texas.

Mr. Anderson and Mr. Bamonte were asked four questions about the regulatory state of CAVs, priorities for the future, and personal experiences:

- What is the range of CAV use cases Texas has seen thus far, and what are the expected use cases moving forward? How do they align with the future mobility goals of your agencies?
- TxDOT and NCTCOG have invested resources to support coordination and information sharing around CAVs within the state. What is the one issue that comes up the most within the context of CAV deployment and liability?
- The issues of safety and liability appear to go hand in hand. Who do you think should take on liability for CAV deployment as we continue to move through the development stage of CAVs? Private sector, state DOT, combination of both?
- Given the volatility of the CAV industry, how should government agencies account for “booms” and “busts” while maintaining that forward-looking view around CAVs?

The following themes arose in the responses to these questions:

- *Connectivity.* The panel members stressed that an area where policymakers can be reliably assured they will have both influence and public funds is in the connected environment. Connectivity will create a broader environment of data sharing and autonomy, and smart vehicles will allow states to further communicate and share data without needing to add physical infrastructure.
- *Roles and responsibilities.* The panel members discussed how state governments will approach the challenges inherent in an industry that regularly undergoes market changes and fluctuations. Mr. Anderson and Mr. Bamonte discussed the importance of having the federal government address existing regulatory gaps as opposed to either state or local entities, though some time was spent

discussing Senate Bill 2205 (Texas Legislative Session 85(R), 2017). Specifically, Mr. Anderson noted that the requirement for AVs to abide by local traffic laws is more important and stringent than it may seem. The panel members left the audience with an important question regarding these regulatory gaps, "Who regulates, consumers or government?"

- *Chat box activity.* The chat box followed this conversation closely. Attendees discussed whether state resources should be focused on AVs, ADAS, or CAV technology. Other conversations included data issues and state responsibilities regarding new technology, safe operations, safety assessments, and data sharing.

When the conversation with Mr. Anderson and Mr. Bamonte concluded, the research team announced a brief break. When everyone reconvened, the event transitioned into two legally focused panels, both of which were moderated by Greg Rodriguez of Stantec.

Panel 2: What are key liabilities around CAVs?

The goal of Panel 2 was to discuss legal issues arising around the question of liability and CAVs. Panel speakers included Melody Drummond-Hansen of BakerHostetler, Patricia Doersch of Squire Patton Boggs, and Will Hubbard of the University of Baltimore School of Law.

Mr. Hubbard began by highlighting a recent study he had conducted for the Maryland Department of Transportation that found that 851 state laws in their current forms would be "problematic" if applied to CAVs. The primary reason for that finding was how the word "driver" is defined. This research includes all levels of automation and not just highly automated vehicles where drivers would no longer be needed or only needed when operating outside of a CAV operational design domain.

After this, panel members were asked four questions and engaged in back-and-forth discussion:

- In your experience working on legal and regulatory issues around vehicle safety, what tension points do you see around state AV legislation and federal jurisdiction over vehicle safety?
- Given the different potential use cases for AV operations (i.e., passenger and goods movement; street vs. sidewalk operations; transit), what are the top liability considerations around AV deployment? Are there national best practices around evolving issues related to torts and contracting that come with emerging technologies?
- How can and should laws be updated when considering the new operational considerations that come with AVs? For example, how does a word like "driver" need to be modified or left behind?
- Since we are also considering CVs in this conversation, how does infrastructure design potentially impact liability considerations? What are liabilities from data sharing?

The following themes arose in the responses to these questions:

- *Jurisdictional considerations.* Panelists explained there is a political reality to operate within for CAVs, and while this political reality exists, states and local governments have done an excellent job filling certain existing gaps. Congress should change its view that legislation is too cumbersome and instead view it as a foundational tool that can spur innovation.

- *Data sharing.* Speakers recommended states and municipalities cooperate and share data about transportation technology projects while states continue to build relations with private industry.
- *Navigating liability.* To tackle how CAV liability will be handled, panel members commented on how federal solutions would be helpful because tort concepts such as negligence per se and contracts remedies can be manipulated to create a highly litigious space for technological advances. As data, products, and other infrastructure converge, there will be a muddying of legal categories and states may have to re-evaluate how infrastructure is built for nonhuman entities.
- *Chat box activity.* The legal discussion was accompanied by questions in the chat box, with one participant asking where duty in torts lies. Members and participants mentioned there is a duty to educate consumers, and even though states have a duty to ensure that CAVs are capable of specific driving behaviors, they do not currently have a duty to people who may be within those CAVs. Participants in the chat mentioned ways to minimize liability, including allocating CAV ownership to private entities, changing definitions in the law for CAVs, considering personally-owned versus fleet-owned concepts for CAVs, and noting where NHTSA's legal authority exists.

Panel 3: Sovereign Immunity and Risk Mitigation

This panel focused on sovereign immunity and risk mitigation, both of which are issues that have been key focus areas for the research project and findings to date. Panel speakers included Judge Hyattye Simmons, Municipal County Clerk for the City of Combine, Texas, and Ben Lewis of Edge Case Research. The two panelists discussed how sovereign immunity in Texas is unique and how to create liability and insurance products appropriate for a variety of actors.

Panel members were asked four questions and engaged in a discussion concerning sovereign immunity and risk mitigation:

- How might sovereign immunity impact state DOTs where there are CAV deployments on public roads?
- With CAV deployments, how should risk be allocated to support development of the technology? Should all the risk be one party or are there models that promote risk sharing?
- What are examples of risk mitigation strategies specific to CAVs from the perspective of state DOTs?
- Which issues relevant to CAV deployments on public roads are we not talking about enough when it comes to risk assessment and mitigation?

The following is a summary of the responses from the panelists:

- *Mr. Lewis* discussed safety frameworks and mentioned three major things to look at within the safety case framework: (1) safety of operations, (2) organizational safety and decision-making processes, and (3) engineering (i.e., how the technology is built). From a risk mitigation perspective, a focus point has been how to limit business interruptions in order to support the safe deployment of CAVs.
- *Judge Simmons* focused on legal issues and mentioned primacy and specialty effects of law, which create a duty to warn versus a duty to save from harm, respectively. He also talked about the nuances of making a roadway safe for a vehicle operating using artificial intelligence. Judge Simmons discussed the nuances around sovereign immunity and how its application differs depending on whether being applied to claims

for torts or contractual related damages. Overall, TxDOT should be protected under sovereign immunity in most scenarios, but the deployment of CAVs does create some grey areas at this point in time.

- *Chat box activity.* Discussions in the chat box included the possibility of considering the manufacturer of an ADS the driver or operator of the vehicle, vicarious liability laws with no damages caps, and if CAV industry players should receive funding incentives prior to demonstrations. Other points included advertising by auto companies about driverless vehicles and their capabilities, and if those companies are over promising the technology's capabilities. Chat box participants discussed CAV ownership and specifically fleet versus personal ownership and how that will change manufacturing, sales, and liability models in comparison to the existing paradigms around vehicle sales and ownership.

Virtual Breakout Groups

The final part of the event was focused around virtual breakout groups. The research team sought to provide space for attendees to interact with each other on what they had heard and learned during the event. Thus, the team used the "breakout groups" tool embedded in the MS Teams videoconference platform. The goal behind creating these smaller spaces was to differentiate this event from the myriad of other webinars and enable attendees to concretely support and inform the research team's work.

The number of attendees was high enough to merit five distinct breakout groups, and each virtual "room" was led by a member of the research team. There were six questions each group was asked to consider, and research team members took anonymized notes on their group's discussion using an identical template:

- How should roles and responsibilities around CAVs be managed through the lens of potential liability (i.e., federal versus state versus local)?
- Are there issues not discussed today that you would like to add for consideration as part of this research project?
- How should state DOTs approach data collection and management from CAVs? This includes considerations around open records laws.
- Which collaborative risk management strategies can and should be promoted within public agencies to address emerging technologies like CAVs?
- Where it exists, how should sovereign immunity be modified in consideration of cases involving CAVs, including where data around infrastructure conditions may be communicated to a DOT?
- Is existing product liability law the appropriate way to approach defective design, manufacture, and instruction of AVs (with consideration that the technology is still maturing)?

Notable themes and comments from the five breakout groups included the following:

- *Data.* Discussions outlined expectations for data disclosure, whether a national privacy framework can and will be adopted, data sharing and aggregation to overcome user privacy concerns, updating digital infrastructure, and liability due to breaches of data agreements or privacy laws. With regard to data sharing, one group started to discuss if there is an opportunity in data laws for "escrow" type data managers that can help control access to data and mitigate concerns for protection around proprietary data or trade secrets.

- *Appropriate jurisdiction.* Discussions also touched on how CAV technology should be considered with existing enforcement of vehicle laws, including the roles of state DOTs and local agencies in keeping roads safe. How and if existing regulatory structures should change around the operation of vehicles on public roads was a point of discussion.
- *Operational design domains.* Interesting questions that emerged included what the operational design domain is for humans and whether it can be expected that CAVs and human driven vehicles safely operate together. Attendees discussed opportunities around user education and training, in addition to incorporating CAVs into drivers' education.
- *Insurance.* Attendees noted that when considering insurance provisions, some requirements may only be able to be met by larger companies, which could limit smaller companies from being able to participate. This can also be a barrier with wanting to broaden testing to all parts of the country, including rural areas.
- *Legal liabilities.* Participants raised the question of whether there could be criminal liability associated with CAVs, particularly in the instance of coding malfunctions. This also led to discussions around how the safety of vehicles can be verified on a regular basis, particularly with the expectation that vehicles will require software updates similar to smart phones.

These smaller groups were allotted approximately 30 minutes to discuss before the research team ended the breakout groups.

Polls and Symposium Close-Out

After the research team called attendees back to the main room, they reviewed general themes from each breakout group. At that point, the second poll using questions for open response was administered in real time. The research team also shared and discussed the results from the first poll. The results from the first poll are included in Figure 10.

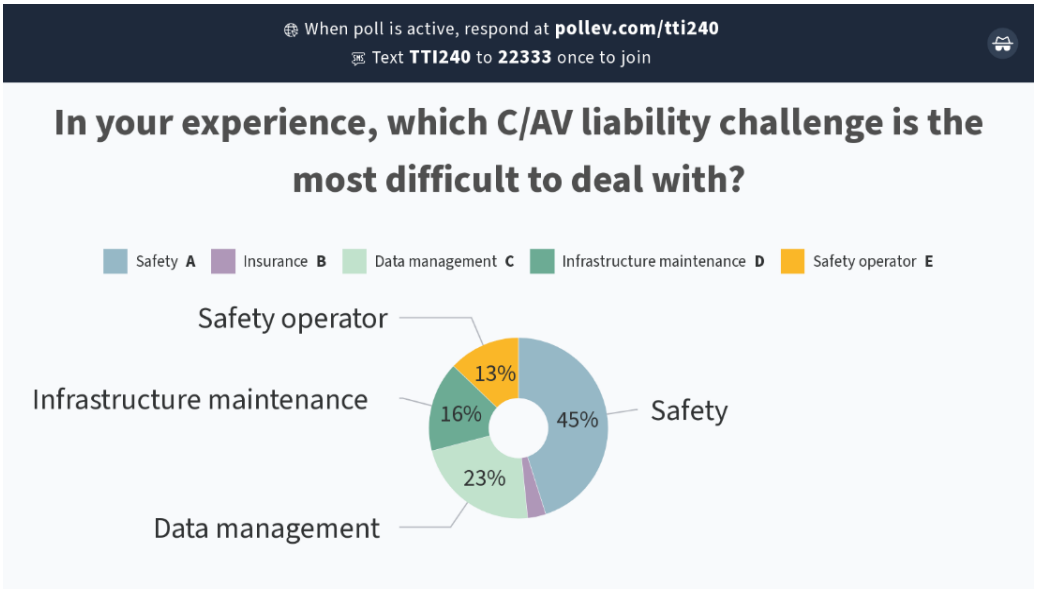

Figure 10. Poll One Question and Responses.

The second poll included the following questions and responses:

- Which of the presented mitigation strategies will be the most effective for your organization?
    - AV data sharing.
    - It will require a combination of strategies, probably starting with state legislatures. Any views about the AV model code (uniform law)?
    - While I don't work for a government organization, I think the approach Ben Lewis mentioned about conducting a 3-part risk assessment that considers the safety of operations, organizational safety, and the technology itself seems like it would be most effective.
    - Contract revisions.
    - Implementation of a complete UL 4600 conformant safety case and safety performance indicators (metrics).
    - A federal law, beyond the guidelines, and detailed and resourced federal management of AV, especially of safety, cybersecurity and privacy, would be of great help.
- Which of the presented mitigation strategies will be the most effective for your organization?
    - Sovereign immunity helps us a lot. But open public discussion with stakeholders will help us get to better approaches to use and support of AV techs.
    - Need to include legal advice in any development of CV capabilities/plans. Data privacy, cybersecurity, validity, reliability, accuracy, timeliness are all concerns that need to be addressed in the planning.
    - One of my favorite comments today and that I wholeheartedly agree with is "instead of waiting and complaining of federal inaction, think instead: when and where do we need the federal government?" Instead of waiting for the feds to build a framework and answer all the issues, let's collaborate to agree on necessary aspects that need help now with federal/national rules of engagement and get busy addressing those together.
    - Education and training internal to our organization and external to partners and the public.

The event concluded with brief remarks from the research team on next steps and the research team's contact information.

Conclusion

Reflecting on the symposium during an immediate debrief meeting, the research team was pleased with the overall event. Attendance was high throughout the entire 3.5 hours, the panel speakers delivered excellent points, and audience engagement via the chat box was high. The virtual breakout groups provided interesting takeaways, and the two polls allowed for dynamic feedback.

In considering how the themes of the project to date align with the takeaways from the Peer Symposium, the following points were noted by the research team:

- Event attendees were largely in agreement with many of the project findings.
- There is an absence of existing case law from which to draw direct analogies because many of the questions around risk, immunity, and CAVs have yet to be decided.

- Inaction on behalf of the federal government has hindered further regulatory and legal developments, leaving states to manage these nascent questions.
- Because of the role state agencies have found themselves in, regular communication between local governments, state DOTs, and members of the CAV industry are critical.

The research team received some attendee feedback, all of which was positive. Participants appreciated the relative novelty of this topic and the event's interactivity, flow, and organization. There was demonstrated interest in receiving updates on the project as it continues to develop and an appreciation for hosting this public forum. In fact, the research team has already received many requests for the recording of the Peer Symposium. The research team paid special attention to the various panelists and sent personalized thank you notes within a few days of the event.

7. Conclusion

CAVs present the opportunity for momentous and positive changes to most aspects of modern life. When the technology is described, the impact to mobility is imagined as safer and more efficient. This potential impact from CAVs comes from the chance to build a self-driving and connected network of vehicles, infrastructure, and supporting data exchanges.

CAV technologies may also necessitate changes in the law, particularly when discussing "highly" autonomous vehicles with little to no need for a human operator. The still-evolving technology and use cases contribute to legal uncertainty due to grey areas around laws developed with human drivers in mind.

Questions of liability dominate conversations about how to manage new mobility paradigms like CAVs, including in areas of tort liability. Although Texas governmental entities typically enjoy some level of sovereign immunity, the TTCA expressly identifies areas where government agencies have waived that immunity and can have limited liability for specific torts.

Because CAV technologies were not contemplated when laws providing immunity were enacted, there are grey areas around whether existing protections for governmental entities apply without updates to those protections.

As a leader in seeking to promote the safe and transformational deployment of CAV technologies, TxDOT developed and issued for research proposals one of on one of the first CAV research projects focused on liability issues from the state DOT perspective. The research team, consisting of TTI and Stantec, embarked on a 24-month project consisting of the following research tasks to identify potential tort liability for TxDOT from the deployment of C/AV technologies.

Sovereign Immunity: A Major Theme of the Project

A common theme in performing the project was the need to first ask the threshold question of whether TxDOT waived its sovereign immunity in various CAV scenarios. Most of the analyses were based on the TTCA, which narrowly limits liability for governmental agencies like TxDOT to claims where an intentional or negligent act of an employee proximately causes property damage, injury, or fatality.

For those use instances where TxDOT was determined to have waived sovereign immunity, the waiver was based on an employee's operation and use of a motor vehicle or motorized equipment, dangers presented by infrastructure or data (e.g., condition or use of property; premises defects; special defects; traffic signs, signals, and warning devices), or both.

Literature Review

Question

How have states and other governmental entities addressed or responded to issues of tort liability from CAV technologies?

Approach

The research team reviewed 45 guidance, policy, research, and legal documents. These documents included legally focused papers, statutes, and case law. The goal of the review was to identify which tort liabilities may

arise for state DOTs and local governments within the context of C/AV operations, and any mitigation techniques those entities undertook. Areas of investigation included:

- Sovereign Immunity.
- Federal Preemption/Supremacy Clause.
- Design Immunity.
- Data Management, Security, and Privacy.
- Notice Regarding Infrastructure Conditions.
- Vehicle Safety Certification.
- Insurance.

Key Findings

The literature reviewed focused on the issue of tort liability as it relates to vehicle or component manufacturers, suppliers, and sellers (i.e., product liability), in addition to the ability of third parties to recover from insured drivers and manufacturers of CAVs. Few sources included discussions about the liability of state DOTs or other public regulators, specifically regarding CAV deployments. The existing literature also lacks insights into issues related to proprietary data sharing and potential notice from CAVs around infrastructure deficiencies, such as potholes.

Additional Takeaways

- State products liability law should continue to govern tort liability matters for defective design, manufacture, and instruction.
- States should retain their authority over human driver licensing, vehicle registration, traffic laws, and enforcement.
- Until NHTSA issues new FMVSS for CAVs, these technologies will continue to blur the clear lines that now exist between state and federal legal authority over the safety of vehicles.
- States should strongly consider legally defining and investing resources in legal teams to proactively address new questions of law that do not fit neatly into existing legal frameworks, including tort law and existing immunities.
- Case law concerning tort liability for state DOTs involving CAVs is scarce but is anticipated to increase as more CAVs are deployed onto public roads.

Stakeholder Interviews

Question

Since CAVs are only now beginning to operate on a scaled basis, how may questions of existing immunities for public agencies be interpreted, especially around vehicle operator liability, data ownership and privacy, and the state's duty to cure a traffic, road, or other infrastructural condition or defect, particularly upon receiving notice of a potential defect?

Approach

The research team conducted interviews with 14 practitioners in transportation, with backgrounds in law, industry, research, planning, and engineering.

Key Findings

Compared to other states, Texas enjoys significant protection from tort liability through its sovereign immunity laws. Deployment of CAV technologies should not affect the state's immunity, especially since private operators are not seeking special infrastructural accommodations for CAV vehicles now. New interpretations of liability could arise around a state's management of data in areas of data protection, data privacy, and data ownership.

Additional Takeaways

- Due to open records laws, private companies are and will continue to be wary of partnering with governmental entities unless they formalize mechanisms to protect certain information from disclosure.
- CAVs will potentially give rise to more data regarding infrastructure conditions and defects than governmental entities currently manage, so agencies may need to consider data management and response policies and procedures, and may need to seek out additional legislative protections under sovereign immunity laws.
- State DOTs and local governments should anticipate receiving more, but also better, information about roadway conditions that will help prioritize repair work more efficiently.
- Transportation agencies that provide data or products that CAV manufacturers can obtain and use may need to provide a user agreement or a warning that clearly states that the information may not be accurate or may be limited in other ways to reduce potential liability.
- Lawsuits involving CAVs will likely be tried under products liability theories and lead to a long evolution in case law. In most states, products liability and rules of the road are handled similarly but differ with respect to caps on economic damages.

State and Federal Law Analysis

Questions

- Has Texas or federal law addressed the liability issues identified in prior tasks?
- How does tort limitation affect TxDOT's efforts in deployments of CAV technologies?
- How do TxDOT and local government entities position themselves to address increased liability concerns?
- What can be learned from existing laws that may indicate what liability TxDOT and local jurisdictions might have?

Approach

The research team conducted this analysis by first searching Texas statutory codes and case law, as well as federal legislation and case law. Analyses of state and federal law fall into five major areas:

1. Federal and state roles.
2. Tort liability and immunity.
3. Data collection and management.
4. Notice of infrastructure conditions.
5. Products liability.

Key Findings

- *State law*: The TTCA narrowly limits liability for governmental agencies like TxDOT to claims where, unless waived, an intentional or negligent act of an employee arising from the operation of a motor vehicle or motor vehicle equipment proximately caused damage to property or human injury or fatality. In other words, whether the facts comprising the claim also involved data, CAVs, roadway or traffic signal defects, or the acts of third parties, these threshold elements must be present for liability to attach to a state agency. If they are not, that agency is likely protected by sovereign immunity.
- *Federal law*: There are currently no federal laws in place around CAVs; however, legislation and rulemakings directly related to CAVs are being considered. There is also activity on related issues, including data management and privacy, artificial intelligence, and workforce.

Additional Takeaways

The three general topics where the law has not been tested or is silent are in three general areas: (a) electronic data, (b) whether FMVSS requirements and recent Texas state law may be in conflict, and (c) whether product-related injuries may expose the agency to tort liability.

Due to the grey areas that currently exist around some aspects of how existing laws and regulations may apply to CAVs from a torts and liability perspective, legally focused risk management is recommended for ensuring the safe operation of CAVs on public roads.

Use Case Analyses

Question

What is TxDOT's potential liability in seven near-future use cases arising from the deployment of CAV technologies? What recommendations are necessary to address any liability concerns arising in these scenarios?

Approach

The research team worked with TxDOT to develop seven use cases that represent specific issues of concern to TxDOT related to CAV operations, as well as issues that revealed themselves during the early project tasks. These include:

1. A CAV reports icy bridge conditions in real time.
2. A CAV cannot read a damaged road sign and crashes.
3. A maintenance drone causes an invasion of privacy.
4. Incorrect work zone data delivered to CAV causes fatality.
5. Automated TMA in wrong lane crashes into oncoming vehicle.
6. Data leak from PIA request.
7. Public transit CAV crash.

Key Findings

Liability was likely to attach to TxDOT if the facts comprising the use case involved government-owned vehicles or equipment; condition or use of property; premises defects; special defects; traffic signs, signals, and warning devices; or the acts of third parties. Otherwise, TxDOT was likely protected by sovereign immunity. In cases where sovereign immunity had been waived, plaintiffs could recover damages from TxDOT if they could prove that the agency breached its duty to users of the roadway.

Each use case also presented strategies that TxDOT may consider to address current gaps in the law or mitigate potential liabilities presented by the operation of CAVs on public roads in the state.

Additional Takeaways

Findings for legislative mitigation strategies mostly consist of ways to amend existing sections of the Texas Civil Practices and Remedies, Transportation, and Local Government Codes to expand or narrow definitions or requirements related to preserving or strengthening TxDOT's sovereign immunity.

Operational mitigation strategy recommendations focus on:

- Data management.
- Contracting.
- Proactive risk identification and mitigation in coordination with counsel.

Peer Symposium

Question

What is the best way to ground-truth project findings with informed peers and build a more robust bank of information on CAV liability issues through the lens of TxDOT's research questions?

Approach

The research team virtually convened a group of informed practitioners who are involved in the testing and deployment of CAV technologies. The focus of experience was on practitioners who could speak to the issues of tort liability and from perspectives of public agencies, industry, and academia.

The program consisted of three structured panel discussions, group polling, virtual breakout rooms, and discussion in the chat box. The event was video-recorded and the recording professionally edited. Portions of the recordings will be available through the web-based tool for the project.

Key Findings

Participants and panelists expressed concerns over a wide range of liability challenges. Safety was the leading issue, followed by multifaceted questions around data use and management, appropriate jurisdiction for enforcement of vehicle laws for CAV technologies, operational design domains, insurance, and the role of sovereign immunity. There was also a robust chat discussion around infrastructure considerations for CAVs.

Additional Takeaways

In considering how the themes of the project to date align with the takeaways from the Peer Symposium, the research team noted the following points:

- Event attendees were largely in agreement with many of the project findings.
- There is an absence of existing case law from which to draw direct analogies because many of the questions around risk, immunity, and CAVs have yet to be adjudicated.
- Due to laws and regulations still being developed at the federal level, states are on the front lines managing these nascent legal questions.
- Because of the role state agencies have found themselves in, communication between local governments, state DOTs, and members of the CAV industry present opportunity for collaborative risk mitigation.

Key Project Takeaways

State Law

Sovereign Immunity

The TTCA provides sovereign immunity against tort claims for government agencies like TxDOT. That immunity can be waived where an intentional or negligent act of an employee arising from the operation of a motor vehicle or motor vehicle equipment proximately caused damage to property or human injury or fatality. Regardless of whether the facts comprising the claim also involved data, CAVs, roadway or traffic signal defects, or the acts of third parties, these threshold elements constituting a waiver must be present for liability to attach to a state agency. If they are not, that agency is likely protected by sovereign immunity.

Gaps and Silences in the Law

The research project affirmed that the law has not been tested or is silent with respect to (a) electronic data, (b) whether FMVSS requirements and recent Texas state law may be in conflict, and (c) whether product-related injuries may expose the agency to tort liability.

The law is clearer with regard to premises defects, special defects, and traffic signs, signals, warning devices, and other traffic control devices (including lane markings). Liability for these issues is likely similar in an environment with C/AVs in operation as it is in the current environment without CAVs.

Dangerous roadway conditions will still potentially create unreasonable risk of harm to passengers in C/AVs as they do in human-operated vehicles.

Federal Law

For a variety of reasons, it has been difficult for Congress to act on CAVs. However, there continue to be rulemakings and requests for comments around CAVs. The information being gathered by USDOT through such rulemakings will hopefully lead to informed regulatory action that considers the flexibility needed as CAV technologies continue to mature and use cases evolve. While there are few specific references to CAVs in federal legislation at this point in time, there are several bills being debated that address issues touching CAVs; this includes legislation focused on privacy, smart cities, and infrastructure focused on intelligent transportation solutions.

Operational, Legal, and Relational Considerations

The results of this project's analysis are that there are a number of legislative, operational, and relational mitigation considerations for TxDOT to best prepare for managing or mitigating the risks identified through this project around the growing operation of CAV on Texas roads.

Legislative considerations to mitigate risks mostly consist of ways to amend existing sections of the Texas Civil Practices and Remedies, Transportation, and Local Government Codes to expand or narrow definitions or requirements related to preserving or strengthening TxDOT's sovereign immunity. There are also opportunities to clarify protections for proprietary and confidential information resulting from public and private partnerships, particularly in the pilot projects phase.

Relational strategies to mitigate risks include a number of comments from the Peer Symposium focused on fostering robust collaboration between different levels of government and the CAV community. This collaboration is needed to understand capabilities and use cases for the technology, supporting public engagement and adoption, and ensuring resources are in place to support changes that may be needed to support full commercial deployment, including investment in data management protocols.

Operational strategies to mitigate risks fall into three main categories:

1. **Data management strategies** to address data management protocols for protection of personal information or trade secrets that include direct data transfers between the agency and CAVs; work zone traffic management processes; receiving more but better information about roadway conditions; making data available to OEMs; increasing familiarity with CAV sensor data; provision of notice or warnings to travelers; and contractual requirements with vendors for security control.
2. **Strategies for addressing unmanned vehicles** that include providing notice to travelers of the presence of inspection drones; evaluating whether closing the sections of roadways where drone inspections are occurring is advisable; and using AI software to immediately obfuscate photographic images of people captured by drones.
3. **Contractual mitigation strategies** that include eliminating contract provisions that assign a right to control to contractors and define them as employees; including new requirements and clauses to CAV contracts regarding insurance coverage against all types of CAV incidents; and considering alternative dispute resolution approaches that ensure matters are being heard by adjudicators that understand the evolving technologies of CAVs.

8. References

Adler, A. (2023, February 24). *Autonomous platooning startup Locomation denies reports of its demise*. Retrieved from Freightwaves: https://www.freightwaves.com/news/reports-autonomous-platooning-startup-locomation-closing-its-doors

Adler, A. (2023, March 3). *Embark Trucks laying off 70% of employees, winding down business*. Retrieved from Freightwaves: https://www.freightwaves.com/news/embark-trucks-laying-off-70-of-employees-winding-down-business

Anderson, J. K. (2016). *Autonomous Vehicle Technology: A Guide for Policymakers.* Rand Corporation.

Association of Metropolitan Planning Organizations. (2019). *National Framework for Regional Vehicle Connectivity and Automation Planning.* Retrieved from Association of Metropolitan Planning Organizations: https://www.ampo.org/wp-content/uploads/2019/04/2019-AMPO-Framework-11.pdf

Bellan, R. (2022, June 30). *Cruise robotaxis blocked traffic for hours on this San Francisco street*. Retrieved from TechCrunch: https://techcrunch.com/2022/06/30/cruise-robotaxis-blocked-traffic-for-hours-on-this-san-francisco-street/

Bellen, R. (2022, March 8). "Pony.ai to Issue Recall of Autonomous Driving Software". *TechCrunch*. Retrieved from https://techcrunch.com/2022/03/08/pony-ai-to-issue-recall-of-autonomous-driving-software/

Canis, B. (2021, April 23). *Issues in Autonomous Vehicle Testing and Deployment.* Congressional Research Service. Retrieved from https://crsreports.congress.gov/product/pdf/R/R45985

Canton, D. a. (2021, August 17). *Privacy Torts: 4 Types of Invasion of Privacy.* Retrieved 2023, from Harrison Pensa LLP: https://hptechlaw.com/blog/2021/8/16/invasion-of-privacy

Channon, M. a. (2021). THE Liability for Cybersecurity Breaches of Connected and Autonomous Vehicles. *Computer Law & Security Review, Vol. 43*. Retrieved from https://doi.org/10.1016/j.clsr.2021.105628

Chatman, D. G. (2019). *Autonomous Vehicles in the United States: Understanding Why and How Cities and Regions Are Responding.* University of California Institute of Transportation Studies. Retrieved from https://escholarship.org/uc/item/29n5w2jk#author

Evans, D. G. (2014, June 12). *Texas Tort Claims Act Basics.* Retrieved from Texas Municipal League: https://www.tml.org/DocumentCenter/View/329/Texas-Tort-Claims-Act-PDF?bidId=

Glancy, D. J. (2016). A Look at the Legal Environment for Driverless Vehicles—Part 1. *NCHRP Legal Research Digest, No. 69*. Retrieved from https://www.trb.org/Main/Blurbs/173557.aspx

Glancy, D. P. (2016). A Look at the Legal Environment for Driverless Vehicles—Part 2. *NCHRP Legal Research Digest, No. 69*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2722236

Hubbard, S. (2018). Automated Vehicle Legislative Issues. *Transportation Research Record: Journal of the Transportation Research Board, Vol. 2672, No. 7*, 1-13. Retrieved from https://doi.org/10.1177/0361198118774155

Jones Day. (2021, July). *Autonomous Vehicles: Legal and Regulatory Developments in the United States.* Retrieved from Jones Day: file:///C:/Users/w-hwang/Downloads/Autonomous%20Vehicles%20Legal%20and%20Regulatory%20Developm.pdf

Jones Day. (2021, July). *Autonomous Vehicles: Legal and Regulatory Developments in the United States.* Retrieved from Jones Day: https://www.jonesday.com/-/media/files/publications/2021/05/autonomous-vehicles-legal-and-regulatory-developments-in-the-us/files/autonomous-vehicles-legal-and-regulatory-developme/fileattachment/autonomous-vehicles-legal-and-regulatory-developm.pdf

Judicial Council of California. (2020). *Judicial Council of California Civil Jury Instructions.* LexisNexis.

Kockelman, K. a. (2018). *Smart Transport for Cities and Nations: The Rise of Self-Driving & Connected Vehicles.* Austin, TX: University of Texas at Austin. Retrieved from https://www.caee.utexas.edu/prof/kockelman/public_html/CAV_Book2018.pdf

Kockelman, K. L.-O. (2016). *Best Practices Guidebook for Preparing Texas for Connected and Automated Vehicles.* Austin, TX: Center for Transportation Research/Texas Department of Transportation. Retrieved from https://library.ctr.utexas.edu/ctr-publications/0-6849-p1.pdf

Kockelman, K. L.-O. (2017). *Best Practices for Modifying Transportation Design, Planning, and Project Evaluation in Texas.* Austin, TX: Center for Transportation Research, University of Texas at Austin. Retrieved from https://rosap.ntl.bts.gov/view/dot/31989

Korosec, K. (2022, October 26). *Ford, VW-backed Argo AI is shutting down*. Retrieved from TechCrunch: https://techcrunch.com/2022/10/26/ford-vw-backed-argo-ai-is-shutting-down/

Kortum, K. L. (2019). TRB Forum on Preparing for Automated Vehicles and Shared Mobility: Mini-Workshop on the Importance and Role of Connectivity. *Transportation Research Circular, No. E-C247*, 18.

Lederman, J. G. (2016, January). Fault-y Reasoning: Navigating the Liability Terrain in Intelligent Transportation Systems. *Public Works Management & Policy, Vol. 21, No. 1*, 5-27. Retrieved from https://doi.org/10.1177/1087724X15592891

Lewis, P. a. (2019). *Beyond Speculation 2.0: An Update to Eno's Action Plan for Federal, State and Local Policymakers.* Washington, DC: Eno Center for Transportation.

Lewis, P. R. (2017). *Adopting and Adapting: States and Automated Vehicles.* Washington, DC: Eno Center for Transportation. Retrieved from https://www.enotrans.org/wp-content/uploads/2017/06/StateAV_FINAL-1.pdf

McGehee, D. B. (2016). *Review of Automated Vehicle Technology: Policy and Implementation Implications.* University of Iowa.

National Highway Traffic Safety Administration. (2022, June). *Summary Report: Standing General Order on Crash Reporting for Level 2 Advanced Driver Assistance Systems.* Retrieved from https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-06/ADAS-L2-SGO-Report-June-2022.pdf

Roshanzamir, P. (2018, June). *Piercing the Government Immunity—When Crossing the Road.* Retrieved from FORUM/Consumer Attorneys of California: https://jassimlaw.com/wp-content/uploads/2020/09/Piercing-the-Government-Veil.pd

Society of Automotive Engineers. (2021, April 30). *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_202104*. Retrieved from Society of Automotive Engineers Standards: https://www.sae.org/standards/content/j3016_202104/

Stamatiadis, P. G. (2018). *Strategic Planning for Connected and Automated Vehicles in Massachusetts.* Lowell, MA: Department of Civil and Environmental Engineering, University of Massachusetts Lowell. Retrieved from https://www.mass.gov/doc/strategic-planning-for-connected-and-automated-vehicles-in-massachusetts/download

Texas State Legislature. (2021, June 2). *SB 15, 87(R), Bill Analysis.* Retrieved from https://capitol.texas.gov/tlodocs/87R/analysis/pdf/SB00015F.pdf#navpanes=0

Trimble, T. E.-O. (2018). *Implications of Connected and Automated Driving Systems, Vol. 1: Legal Landscape.* Washington, DC: Transportation Research Board. Retrieved from https://doi.org/10.17226/25296

Trimble, T. W.-O. (2018). *Implications of Connected and Automated Driving Systems, Vol. 3: Legal Modification Prioritization and Harmonization Analysis.* Washington, DC: Transportation Research Board. Retrieved from https://nap.nationalacademies.org/catalog/25293/implications-of-connected-and-automated-driving-systems-vol-3-legal-modification-prioritization-and-harmonization-analysis

Trimble, T. W.-O. (2018). *Implications of Connected and Automated Driving Systems, Vol. 4: Autonomous Vehicle Action Plan.* Washington, DC: Transportation Research Board.

Trimble, T. W.-O. (2018). *Implications of Connected and Automated Driving Systems, Vol. 5: Developing the Autonomous Vehicle Action Plan.* Washington, DC: Transportation Research Board. Retrieved from https://doi.org/10.17226/25291

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

U.S. Department of Transportation. (2020). *Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0.* Retrieved from U.S. Department of Transportation: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf

U.S. Department of Transportation. (2021, March 30). *Automated Driving System Demonstration Grants*. Retrieved from U.S. Department of Transportation Automated Vehicles: https://www.transportation.gov/av/grants

U.S. Department of Transportation. (2021). *Standing General Order on Crash Reporting for Levels of Driving Automation 2-5*. Retrieved from National Highway Traffic Safety Administration: https://www.nhtsa.gov/sites/nhtsa.gov /files/2021-08/First_Amended_SGO_2021_01_Final.pdf

Zmud, J. G. (2017). *Strategies to Advance Automated and Connected Vehicles.* Washington, DC: Transportation Research Board. Retrieved from https://doi.org/10.17226/24873

9. Value of Research Analysis

Overview

CAVs promise momentous and positive changes to most aspects of modern life. Mobility is likely to be characterized by collaborative, communicative, and driverless vehicles operating in a connected network of vehicles, infrastructure, and wireless devices. One of the most uncertain and yet undefined areas where change can be expected is legislation surrounding the licensing and operation of these technologies. Questions of liability dominate research and conversation about how to manage new mobility paradigms, including in areas of state and local government tort liability. And although governmental entities typically enjoy some level of sovereign immunity, there are areas identified in state law where they have limited liability for specific torts. This research project identifies potential tort liability for TxDOT and other governmental agencies associated with CAV technologies. It provides foundational research necessary for TxDOT to proactively identify, assess, and address legal liabilities that may arise under current law and legal liabilities that may arise under new law as the result of CAV implementations.

It is difficult to quantify the economic benefits of situations or circumstances that are avoided, especially those of a legal nature. Each case has unique characteristics that impact the costs and benefits of investigation and disposition. However, there are qualitative benefits from this research. Working with the PMC, the areas of "Level of Knowledge" and "Management and Policy" were selected to qualitatively demonstrate the value of this research project.

Project Details

While the value of research (VOR) is qualitative, the research team did use the VOR template provided by TxDOT. Pertinent details of the project are noted below:

Project #: 0-7130

Project Name: Investigate Potential Connected and Automated Vehicle (CAV) Liability Issues within TxDOT

Project Duration: 2 years

Project Budget: $299,476

Project Benefits

Level of Knowledge

This project provides foundational research that expands the level of knowledge of TxDOT's general counsel and prepares them to proactively identify, assess, and address legal liabilities that may arise as a result of CAV implementation.

Management and Policy

This project also identifies areas of concern where TxDOT and other governmental entities may want to establish policies or procedures that serve to limit agency tort liability. Additionally, scenarios were developed that exposed risks. TxDOT's general counsel can work proactively with legislative staff to recommend changes to laws that may serve to reduce liability.

The rapidly evolving nature of the technology and its implementation further complicates the determination of the long-term value of this research. New laws at all levels of government have the potential to impact tort liability. Nonetheless, the value of this foundational research is significant. This is the first exploration of case law and statute related to CAV technology undertaken by TxDOT. It identified relevant statutory and case law and examined them in the context of specific topical areas of potential liability. The research identified issues, as well as gaps and silences in the law, and identified potential issues and associated legal and technical mitigation strategies.