Michigan Telecommunications and Technology Law Review

Volume 23 | Issue 2

2017

A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles

Daniel A. Crane
University of Michigan Law School, dancrane@umich.edu

Kyle D. Logue
University of Michigan Law School, klogue@umich.edu

Bryce C. Pilz
University of Michigan Law School, bpilz@umich.edu

A SURVEY OF LEGAL ISSUES ARISING FROM THE DEPLOYMENT OF AUTONOMOUS AND CONNECTED VEHICLES

*Daniel A. Crane**
Kyle D. Logue
Bryce C. Pilz

Cite as: Daniel A. Crane, Kyle D. Logue, & Bryce C. Pilz,
A Survey of Legal Issues Arising From
The Deployment of Autonomous and Connected Vehicles,
23 MICH. TELECOM. & TECH. L. REV. 191 (2017).
This manuscript may be accessed online at repository.law.umich.edu.

TABLE OF CONTENTS

* The authors would like to thank Erika Giroux, Insung Hwang, John Muhs, Liliya Paraketsova, Jake Rambeau, Christopher Stackhouse, and Cynthia Weaver for their invaluable assistance in researching the underlying issues and in preparing this report.

I. Intro

A. *The World of Autonomous and Connected Vehicles is Rapidly Evolving*

In the nine months since the authors began this research project, one thing has remained constant – the world of autonomous and connected vehicles is rapidly evolving. Contributors to this rapid evolution have included, among others, automotive manufacturers, technology companies, state and federal governments, and research universities. An example of the latter is the University of Michigan, which in July 2015 launched "Mcity," a 32-acre test city, claiming to be "the word's first controlled environment specifically designed to test the potential of connected and automated vehicle technolo-

gies."[1] "Mcity" is run by a public-private partnership between the University of Michigan and industry partners.[2]

One of these industry partners, Ford, was the first manufacturer to test an autonomous car at Mcity.[3] Ford later announced it was tripling its autonomous vehicle fleet[4] and on March 11, 2016, announced it was restructuring to form a subsidiary, Ford Smart Mobility, solely focused on disruptive mobility solutions, such as autonomous and connected vehicles.[5] On the same day, General Motors announced it had acquired autonomous vehicle startup Cruise Automation for $1 billion.[6] This was not General Motors' first major announcement of the year. Just a few months earlier, in January, General Motors had announced that it had invested $500M in ridesharing company Lyft[7] and then shortly thereafter acquired ridesharing startup SideCar.[8]

Other automotive companies were also active. With autonomous vehicles being tested on public roads, Mercedes, Google, and Volvo all made headlines in October 2015 by publicly announcing their companies' willingness to accept fault for crashes involving their autonomous vehicles.[9]

---

1. U. MICH. MOBILITY TRANSFORMATION CTR., U-M Opens Mcity Test Environment for Connected and Driverless Vehicles, (July 20, 2016), http://www.mtc.umich.edu/vision/news-events/u-m-opens-mcity-test-environment-connected-and-driverless-vehicles.

2. The "leadership circle" companies partnering with MTC are BMW; Delphi Automotive PLC; DENSO Corporation; Econolite Group, Inc.; Ford Motor Company; General Motors Company; Honda Motor Co., Ltd.; Iteris, Inc.; LG Electronics, Inc.; Navistar, Inc.; Nissan Motor Co., Ltd.; Qualcomm Technologies, Inc.; Robert Bosch LLC; State Farm Mutual Automobile Insurance Company; Toyota Motor Corporation; Verizon Communications, Inc.; and Xerox Corporation. U. MICH. MOBILITY TRANSFORMATION CTR., *Industry*, http://www.mtc.umich.edu/partners/industry.

3. Alisa Priddle, *First to Test Autonomus Vehicle at Mcity Is a Ford*, DETROIT FREE PRESS (Nov. 13, 2015), http://www.freep.com/story/money/cars/ford/2015/11/13/first-test-autonomous-vehicle-mcity-ford/75679668/.

4. Kirsten Korosec, *Ford Hits the Gas on Self-Driving Cars*, FORTUNE (Jan. 5, 2016), http://fortune.com/2016/01/05/ford-self-driving-car-fleet/.

5. Nathan Bomey, *Ford Forms 'Smart Mobility' Division*, USA TODAY (Mar. 11, 2016), http://www.usatoday.com/story/money/cars/2016/03/11/ford-smart-mobility-ride-sharing-self-driving-cars/81636682/.

6. Gautham Nagesh & Mike Ramsey, *GM Gives Its Self-Driving Effort a Push*, WALL ST. J., (Mar. 11, 2016), http://www.wsj.com/articles/gm-to-acquire-autonomous-vehicle-technology-developer-1457704950.

7. Mike Isaac, General Motors, *Gazing at Future, Invests $500 Million in Lyft*, N.Y. TIMES (Jan. 4, 2016), http://www.nytimes.com/2016/01/05/technology/gm-invests-in-lyft.html?_r=0.

8. Kia Kokalitcheva, *GM Buys Sidecar's Assets as It Preps New Transportation Services*, FORTUNE (Jan. 19, 2016), http://fortune.com/2016/01/19/gm-sidecar-acquisition/.

9. Michael Ballaban, Mercedes, Google, *Volvo to Accept Liability When Their Autonomous Cars Screw Up*, JALOPNIK (Oct. 7, 2015), http://jalopnik.com/mercedes-google-volvo-to-accept-liability-when-their-1735170893.

Volvo's president boldly claimed that the company would "accept full liability whenever one of its cars is in autonomous mode."[10]

Google's statement was put to a small test when, on February 14, 2016, Google's self-driving car collided at low speeds with a bus, in what is being reported as possibly the "first crash that was the fault of the self-driving vehicle."[11] Google has continued its testing of its self-driving car, reaching the 1.4 million mile mark for testing on public roads in Mountain View, California; Austin, Texas; and Kirkland, Washington.[12] Google, perhaps more than any other company, symbolizes the entrance of high-tech companies into the automotive world. But, Google is not alone. In August 2015, the Guardian obtained documents under a public records request indicating that Apple was looking to test an autonomous vehicle.[13] Also, electric vehicle maker Tesla released its "autopilot" feature in October 2015,"[14] making its Model S vehicles "semi-autonomous."

The testing of these vehicles on public roads has been permitted by the early regulatory activity in states like Nevada, California, Florida, and Michigan. Having previously adopted autonomous vehicle testing regulations, the California Department of Motor Vehicles ("California DMV") on December 16, 2015 released its much awaited draft regulations for the non-testing deployment of autonomous vehicles.[15] The draft regulations generated significant commentary, including the headlines:

- "California wants to keep autonomous cars from being autonomous"[16]

10. Jim Gorzelany, *Volvo Will Accept Liability for Its Self-Driving Cars*, FORBES (Oct. 9, 2015), http://www.forbes.com/sites/jimgorzelany/2015/10/09/volvo-will-accept-liability-for-its-self-driving-cars/#7b6a779d3d80.

11. David Shepardson, *U.S. Auto Safety Agency Seeks Details of Google Self-Driving Crash*, REUTERS (Mar. 10, 2016), http://www.reuters.com/article/us-google-selfdrivingcar-id USKCN0WC1YS.

12. David Shepardson, *Google Expands Self-Driving Car Testing to Washington State*, REUTERS (Feb. 3, 2016), http://www.reuters.com/article/us-alphabet-autos-testing-idUSKCN0 VC26R.

13. Mark Harris, *Documents Confirm Apple is Building Self-Driving Car,* GUARDIAN (Aug. 14, 2015), http://www.theguardian.com/technology/2015/aug/14/apple-self-driving-car-project-titan-sooner-than-expected.

14. Teslas Motors Team, *Your Autopilot has arrived,* TESLA BLOG (October 14, 2015), available at: https://www.teslamotors.com/blog/your-autopilot-has-arrived.

15. CAL. DEP'T OF MOTOR VEHICLES, DMV RELEASES DRAFT REQUIREMENTS FOR PUBLIC DEPLOYMENT OF AUTONOMOUS VEHICLES, CA.GOV (Dec. 16, 2015), https://www.dmv.ca .gov/portal/dmv/detail/pubs/newsrel/newsrel15/2015_63 [hereinafter DRAFT REGULATIONS].

16. Jordan Golson, *California Wants to Keep Autonomous Cars From Being Autonomous*, THE VERGE (Dec. 16, 2015), http://www.theverge.com/2015/12/16/10325672/california-dmv-regulations-autonomous-car.

- "California's New Self-Driving Car Rules Are Great for Texas"[17]
- "California, Google Ready for Autonomous Vehicle Showdown in 2016"[18]

The California DMV held public workshops on January 28 and February 2, 2016,[19] when representatives from automotive manufacturers, technology providers, municipalities, and consumer protection groups weighed in.

With concerns rising over the number and variety of state regulations, companies are increasingly looking to the federal government for guidance. Representatives from Google, GM, Lyft, and Delphi testified before Congress on March 15, urging congress to pass a federal law concerning autonomous vehicles.[20] While the passage of any federal legislation is unclear at this time, other parts of the federal government have been extremely active in recent months. In January 2016, the Obama administration proposed a 10-year, $4 billion investment in autonomous vehicle technology.[21] In that same announcement, the Department of Transportation ("DOT") committed to developing model state policy on autonomous vehicles in the first half of 2016.[22] On February 4, 2016, the National Highway Transportation Safety Administration ("NHTSA") responded to Google's request for interpretation with a letter outlining NHTSA's interpretation of the term "driver" as used in several Federal Motor Vehicle Safety Standards ("FMVSSs").[23] On March 11, 2016 the DOT announced public hearings on autonomous vehicles to be held on April 8, 2016 and at one later date.[24] Additionally, on that

17. Alex Davies, *California's New Self-Driving Car Rules Are Great for Texas*, *Wired* (Dec. 17, 2015), http://www.wired.com/2015/12/californias-new-self-driving-car-rules-are-great-for-texas/.

18. Salvador Rodriguez, *California, Google Ready for Autonomous Vehicle Showdown in 2016*, Int'l Bus. Times (Dec. 19, 2015), http://www.ibtimes.com/california-google-ready-autonomous-vehicle-showdown-2016-2233290.

19. Cal. Dep't of Motor Vehicles, Autonomous Vehicles in California, https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/auto.

20. Nathan Bomey, *Self-Driving Car Leaders Ask for National Laws*, USA Today (Mar. 15, 2016), http://www.usatoday.com/story/money/cars/2016/03/15/google-alphabet-general-motors-lyft-senate-commerce-self-driving-cars/81818812/.

21. U.S. Dep't of Transp., Secretary Foxx Unveils President Obama's FY17 Budget Proposal of Nearly $4 Billion for Automated Vehicles and Announces DOT Initiatives to Accelerate Vehicle Safety Innovations, Transportation.gov (Jan. 14, 2016), https://www.transportation.gov/briefing-room/secretary-foxx-unveils-president-obama%E2%80%99s-fy17-budget-proposal-nearly-4-billion.

22. *Id.*

23. NHTSA, Letter to Google, Inc. (Feb. 4, 2016), http://isearch.nhtsa.gov/files/Google%20—%20compiled%20response%20to%2012%20Nov%20%2015%20interp%20request%20—%204%20Feb%2016%20final.htm [hereinafter NHTSA Letter to Google].

24. U.S. Dep't of Transp., Acting to Advance the Development of Autonomous Vehicle Technology, Transportation.gov. (Mar. 11, 2016), https://www.transportation.gov/fastlane/acting-advance-development-autonomous-vehicle-technology.

same date, NHTSA released a report from the Volpe Center analyzing how the FMVSSs would apply to autonomous vehicles.[25] The DOT and NHTSA also released a "Policy Statement Concerning Automated Vehicles" updating its 2013 "Preliminary Statement of Policy Concerning Automated Vehicles."[26] The statement explained that, "[t]his is an area of rapid change, which requires DOT and NHTSA to remain flexible and adaptive as new information and technologies emerge."[27]

B. *Multiple Distinct Tracks of Technology Development*

Autonomous and connected vehicle technologies are developing in at least four distinct "tracks."[28] These tracks include: (i) the steady progression of automated technologies in vehicles, (ii) the near-term development and testing of fully autonomous ("self-driving") vehicles, (iii) connected vehicle technologies like vehicle-to-vehicle and vehicle-to-infrastructure communications, and (iv) ridesharing technologies. While these tracks are progressing somewhat independently, they are not mutually exclusive, even to a single company. For example, as recently reported by Fortune, Ford is both continuing its progression of automated technologies, such as parking assist, and also testing fully autonomous vehicles.[29] Ford has also been heavily involved in connected vehicle technologies along with NHTSA and industry partners, and has also begun piloting ridesharing programs.

1. First Track: Progressive Automation of Vehicles

In one track, companies are progressively increasing the extent to which their vehicles are automated.[30] Such automation includes existing technologies like adaptive cruise control, electronic stability control, and dynamic brake support.[31] Under this track, vehicle manufacturers will progressively deploy models with increasingly automated features until vehicles will eventually be deployed with self-driving capabilities.[32] Indeed, NHTSA's 2013

25. *Id.*

26. U.S. Dep't of Transp., "DOT/NHTSA Policy Statement Concerning Automated Vehicles" 2016 Update to "Preliminary Statement of Policy Concerning Automated Vehicles", http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Autonomous-Vehicles-Policy-Update-2016.pdf [hereinafter 2016 Updated Statement].

27. *Id.*

28. NHTSA, Preliminary Statement of Policy Concerning Automated Vehicles 3 (2013), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf [hereinafter NHTSA 2013 Preliminary Statement].

29. Korosec, *supra* note 4.

30. Stephen P. Wood, Jesse Chang, Thomas Healy & John Wood, *The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles*, 52 Santa Clara L. Rev. 1423, 1428 (2012) ("There is a continuum of these technologies, and many of them are already available today.").

31. NHTSA 2013 Preliminary Statement, *supra* note 29, at 4.

32. Wood et al., *supra* note 30 at 1428.

Preliminary Statement established five levels of vehicle automation to track the progression of vehicles in this track.[33]

Level 0 vehicles have no automation and the driver is in "complete and sole control of the primary vehicle controls (brake, steering, throttle, and motive power) at all times and is solely responsible for monitoring the roadway and for safe operation of all vehicle controls."[34]

At a slightly more automated level, Level 1 vehicles have function-specific automation such as adaptive cruise control, electronic stability control, or dynamic break support. In limited situations, these technologies can assume control of the car or assist with control.[35]

Level 2 vehicles have multiple automated functions that work together such that the vehicle can assume active control of the vehicle in limited driving situations. Tesla's "autopilot" feature has been described as a NHTSA Level 2 technology feature.[36] Level 2 vehicles, such as Tesla's Model S, may use a combination of forward-looking radar, outward facing cameras, sensors, and GPS to visualize the road.[37]

Level 3 vehicles offer limited self-driving automation, enabling the driver to "cede full control of all safety-critical functions under certain traffic or environmental conditions and in those conditions to rely heavily on the vehicle to monitor for changes in those conditions requiring transition back to driver control."[38] The driver must be able to monitor the vehicle and be capable of assuming control of the vehicle in situations where the vehicle is no longer able to support automation.

In Level 4, the vehicle is intended to "perform all safety-critical driving functions and monitor roadway conditions for an entire trip."[39] Google has described its "self-driving car" as a NHTSA Level 4 vehicle.[40]

Tesla's Model S appears to be designed to follow this first track of progressively increasing the automation of vehicles over time. As explained by Tesla, it equipped its Model S "with hardware to allow for the incremental

---

33. NHTSA 2013 PRELIMINARY STATEMENT, *supra* note 28, at 4-5.

34. *Id.* at 4.

35. *Id.*

36. Steve Crowe, *Tesla Jumps Onto Self-Driving On-Ramp with Autopilot*, ROBOTICS TRENDS (Oct. 15, 2015) ("Jalopnik tested the Autonomous Level 2 system in a Model S in New York City traffic [ ]. [I]t's not a 100% self-driving system, [ ] it's the 'holy grail of cruise control.' Autopilot won't drive you to your destination, won't make navigational turns without your input, and it can't comprehend traffic lights or signs.")

37. *See id.*

38. NHTSA 2013 PRELIMINARY STATEMENT, *supra* note 28, at 5.

39. *Id.*

40. NHTSA LETTER TO GOOGLE, *supra* note 24; The Society of Automotive Engineers ("SAE") has also promulgated defined levels of autonomous vehicles, ranging from Level 0 to Level 5. SAE INT'L (2014), *Automated Driving: Levels of Driving Automation are Defined in New SAE International Standard J3016*, http://www.sae.org/misc/pdfs/automated_driving.pdf.

introduction of self-driving technology."[41] Tesla reportedly plans to periodically release software upgrades to increasingly automate its Model S vehicles.[42] Traditional automakers, such as Ford, are also pursuing this track (along with others).[43]

2. Second Track: Near-term Deployment of Autonomous Vehicles

A second track involves the non-progressive development of autonomous vehicles, meaning NHTSA level 3 or level 4 vehicles. Under this track, rather than progressively adding automated features, such as those included in NHTSA Level 2, certain manufacturers are actively testing vehicles that could be described as "self-driving." For example, Google's self-driving car project falls under this track. Google is currently testing 23 Lexus RX450h SUVs and 33 Google prototypes.[44] Since the the project started in 2009, Google has logged over 1.4 million miles in autonomous mode.[45]

Other manufacturers are also developing fully autonomous cars that would fall under this track. Ford's announcement that it plans to triple its fleet of autonomous vehicles and continue testing them on California, Arizona, and Michigan roads falls under this track.[46]

Companies testing autonomous vehicles in this track are typically employing a combination of Lidar sensors (light-based sensors), cameras, and other sensors, that detect objects in all directions, as well as GPS technology.[47] These cars are typically designed to operate without needing to transmit driving information to or from other vehicles or roadside infrastructure.

3. Third Track: Connected Vehicles

In a third track of technology development, cars will be able to communicate with one another and with roadside infrastructure. Connected vehicle technologies are typically referred to as vehicle-to-vehicle ("V2V") technol-

---

41. Tesla Motors, *Your Autopilot Has Arrived*, THE TESLA BLOG (Oct. 14, 2015), https://www.teslamotors.com/blog/your-autopilot-has-arrived.

42. *Id.* ("The release of Tesla Version 7.0 software is the next step for Tesla Autopilot. We will continue to develop new capabilities and deliver them through over-the-air software updates, keeping our customers at the forefront of driving technology in the years ahead.").

43. Korosec, *supra* note 5 (Ford "will continue to add more semi-autonomous features to its vehicles such as helping drivers park and stay in lane on the highway.").

44. GOOGLE, GOOGLE SELF-DRIVING CAR PROJECT MONTHLY REPORT (Feb. 2016), https://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-0216.pdf.

45. *Id.*

46. *Id.*

47. GOOGLE, *How it Drives*, https://www.google.com/selfdrivingcar/how/; *see also* Alex Davies, *Turns Out the Hardware in Self-Driving Cars is Pretty Cheap*, WIRED (Apr. 22, 2015), https://www.wired.com/2015/04/cost-of-sensors-autonomous-cars/.

ogies and vehicle-to-infrastructure ("V2I") technologies.[48]V2V communications would involve on-board equipment including dedicated short-range radio communication ("DSRC") devices. These devices would broadcast information to other vehicles, such as a vehicle's speed, heading, brake status, and other information."[49] V2V connectivity has been the subject of extensive research and development by NHTSA as well as various industry members.[50]

NHTSA released an advance notice of proposed rulemaking ("ANPRM") concerning V2V communications on August 18, 2014.[51] The ANPRM announced potential FMVSS No. 150, which would require all light vehicles to contain V2V capabilities with minimum performance requirements.[52] The Notice of Proposed Rulemaking from NHTSA concerning FMVSS 150 is expected in 2016. Accordingly, if NHTSA were to enact FMVSS 150 requiring V2V technology on all new light vehicles, V2V technology will be on the market in the imminent future.

V2I technology would involve roadside equipment with DSRC devices.[53] These roadside devices would transmit information to vehicles, enabling applications such as red light violation warnings, curve speed warnings, and weather information warnings, among others.[54]

V2V and V2I technologies would not replace automated or autonomous technologies, but instead would supplement those technologies by providing an additional stream of information. NHTSA has proposed various scenarios where V2V might aid crash avoidance beyond the capabilities of vehicle resident autonomous technologies (including those found on NHTSA Level 4, self-driving, cars). In one example, V2V technology could provide "intersection movement assist" With this technology, the driver is warned of a risk of collision from a second vehicle approaching an intersection that is not in

48. "Connected vehicle" can also be used to refer to telematics that transmit and enable various information and "infotainment" applications to vehicles. This report will use the term "connected vehicle" to refer to the vehicle-to-vehicle or vehicle to infrastructure communication technology supporting crash avoidance technologies. This is consistent with the terminology adopted by the Department of Transportation in the V2V Readiness Report. J. HARDING ET AL., NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, VEHICLE-TO-VEHICLE COMMUNICATIONS: READINESS OF V2V TECHNOLOGY FOR APPLICATION, at 2 (2014), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf [hereinafter V2V READINESS REPORT].

49. *Id.* at xiv.

50. *Id.* at 4 ("V2V communications research initially began under the Vehicle Infrastructure Integration Initiative in 2003, but its origins date back to the Automated Highway System (AHS) research of the 1990s.").

51. NHTSA, U.S. DEPARTMENT OF TRANSPORTATION ISSUES ADVANCE NOTICE OF PROPOSED RULEMAKING TO BEGIN IMPLEMENTATION OF VEHICLE-TO-VEHICLE COMMUNICATIONS TECHNOLOGY, NHTSA.GOV (Aug. 18, 2014), https://www.nhtsa.gov/press-releases/us-department-transportation-issues-advance-notice-proposed-rulemaking-begin.

52. Fed. Motor Vehicle Safety Standards, 49 C.F.R. § 571.126.

53. *See* V2V READINESS REPORT *supra* note 49 at 32.

54. *Id.*

the driver's line of sight, perhaps because of a building or other object blocking her view.[55]

One entity heavily involved in the development of V2V technologies has been the Crash Avoidance Metrics Partnership ("CAMP"), a partnership involving Mercedes-Benz, General Motors, Toyota, Nissan, Volkswagon, Hyundai-Kia Motors, Honda, and Ford.[56] CAMP was formed in 1995 with the objective of accelerating the implementation of crash avoidance technology.[57]

4. Fourth Track: Ridesharing through Transportation Network Companies

A fourth track of technology development involves ridesharing. Ridesharing services, such as Uber and Lyft, commonly referred to as transportation networking companies ("TNCs"), offer a smartphone application to connect riders to drivers who typically operate their own vehicles.[58] TNCs have become increasingly relevant in the autonomous vehicle space. In January 2015, according to reports, Uber began aggressively hiring researchers from Carnegie Mellon University's National Robotics Engineering Center ("NREC").[59] Uber has reportedly hired as many as 50 individuals from Carnegie Mellon, and established a 53,000 square foot facility about a mile from NREC.[60] In August 2015, Uber announced a partnership with the University of Arizona to test autonomous vehicles on the university's campus.[61]

Uber is not alone. As mentioned above, GM recently invested $500 million in ridesharing service Lyft.[62] GM has also launched its own carsharing

---

55. *See id.* at 27.

56. Rachel King, *Automakers Tackle the Massive Security Challenges of Connected Vehicles*, WALL STREET J. (June 25, 2015), http://blogs.wsj.com/cio/2015/06/25/automakers-tackle-the-massive-security-challenges-of-connected-vehicles/.

57. CAITLIN MOTSINGER & TODD HUBING, A REVIEW OF VEHICLE-TO-VEHICLE AND VEHICLE-TO-INFRASTRUCTURE INITIATIVES, THE CLEMSON UNIVERSITY VEHICULAR ELECTRONICS LABORATORY (Oct. 3, 2007), http://www.cvel.clemson.edu/Reports/CVEL-07-003.pdf.

58. *See* Talia G. Loucks, *Travelers Beware: Tort Liability in the Sharing Economy*, 10 WASH. J. L. TECH. & ARTS 329, 335-36 (Spring 2015).

59. Josh Lowenshohn, *Uber Gutted Carnegie Mellon's Top Robotics Lab to Build Self-Driving Cars*, THE VERGE (May 19, 2015), http://www.theverge.com/transportation/2015/5/19/8622831/uber-self-driving-cars-carnegie-mellon-poached.

60. *Id.*

61. Russell Brandom, *Uber Will Partner With University of Arizona for Self-Driving Car Research*, THE VERGE (Aug. 25, 2015), http://www.theverge.com/2015/8/25/9207229/uber-university-of-arizona-tucson-autonomous-self-driving-cars.

62. Isaac, *supra* note 7.

service, Maven, in Ann Arbor, Michigan[63] and both GM[64] and Ford[65] reportedly have launched ridesharing pilots.

C. *Terminology Used in this Report*

Several individuals have commented on the confluence of terminology related to autonomous vehicles and connected vehicles.[66] As noted above, some of this confusion arises from the multiple tracks of technology development. In this report, the authors use the term "automated vehicle" to refer to technologies providing various levels of control to the vehicle, whether or not the car is autonomous. The authors use the term "autonomous vehicle" or "AV" to refer to a vehicle equipped with NHTSA level 3 or 4 technology. The authors use the term "connected vehicle" or "CV" to refer to a vehicle equipped with V2V or V2I technology. In the majority of instances, the authors will refer to "autonomous or connected vehicles" or "ACVs" in discussing legal or regulatory issues common to both classes of vehicles. Where the distinction matters, the authors will particularly point out the issue as related to "automated," "autonomous," or "connected vehicles," independently.

D. *Overview of Existing Scholarship and Analysis of Legal and Regulatory Issues*

Several significant contributions have already been made to the scholarly literature concerning the legal and regulatory issues related to ACVs. The early stages of the authors' research involved examining the existing scholarly literature related to ACVs.

It is worth noting a few particular works. Santa Clara Law School held a conference titled "Driving the Future: The Legal Implications of Autonomous Vehicles" in 2012.[67] This conference generated a number of important early works, including a comprehensive overview of NHTSA's regulatory framework authored by Stephen Wood, Jesse Chang, Thomas Healy, and

63. Andrew Krok, *General Motors' Maven Is All About Car Sharing, Not Ride Sharing*, ROAD SHOW BY CNET (Jan. 20, 2016), http://www.cnet.com/roadshow/news/general-motors-maven-car-sharing/.

64. Greg Gardner, *GM to Launch Maven Car-Sharing in Ann Arbor*, DETROIT FREE PRESS (Jan. 21, 2016), http://www.freep.com/story/money/cars/general-motors/2016/01/21/gm-ride-sharing-maven-general-motors/79059648/.

65. Chantal Tode, *Ford Pilots On-Demand Ride-Sharing Service to Innovate Personal Mobility*, MOBILE MARKETER (Dec. 14, 2015), http://www.mobilemarketer.com/cms/news/software-technology/21859.html.

66. CA DMV, *Autonomous Vehicle Workshop (Jan. 28 at California State University, Sacramento)*, YOUTUBE (Jan. 28, 2016), https://www.youtube.com/watch?v=EZr_N-6Y62E [hereinafter January 28, 2016 Workshop].

67. *See* Santa Clara Law School, Aroma Sharma, *"Driving the Future": The Legal Implications of Autonomous Vehicles Conference Recap* (2012), http://law.scu.edu/hightech/autonomousvehicleconfrecap2012/.

John Wood from NHTSA and the DOT, "The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles" ("Wood et al.").[68]

Among other valuable publications, Anderson, et al.'s report "Autonomous Vehicle Technology: A Guide for Policymakers," published through RAND ("RAND Report") overviews the state of the technology at the time of publication and the legal and regulatory environment for autonomous vehicles.[69] Bryant Walker Smith's article "Automated Vehicles are Probably Legal in the United States"[70] ("Smith") provides one of the first comprehensive analyses of the regulatory issues concerning autonomous vehicles. More recently, Dorothy Glancy, Robert Peterson, and Kyle Graham have issued a draft report, "A Look at the Legal Environment for Driverless Vehicles" ("Glancy et al.") providing a detailed overview of the relevant technologies, a history of various legal and regulatory approaches to new technologies, and an overview of the important legal, regulatory, and insurance regimes concerning autonomous vehicles.[71]

E. *Background and Purpose of this Research*

The authors are a team of faculty at the University of Michigan Law School. The authors conducted this research with funding from MTC. This research project involves three stages. The first stage involved initial research, drafting, and then dissemination of a draft report. The second stage involved a conference to be held at the University of Michigan Law School on April 15, 2016.[72] In the third stage, based on comments received at the conference, the authors finalized and published their final report.

The goal of this project was to prepare a survey of the legal and regulatory issues concerning ACVs and a framework for future analysis. The authors recognize that several important works addressing the legal and regulatory issues relating to autonomous vehicles exist, and others are likely being prepared. Therefore, the authors have attempted to focus on recent developments, potential hurdles not yet addressed, and perspectives not yet shared. Through their affiliation with MTC, and in particular the MTC Legal Working Group, the authors have benefitted greatly from conversations with MTC staff and member companies. The authors have also benefitted greatly from the generosity of numerous other individuals and entities in sharing

68. Wood et al., *supra* note 30.

69. James M. Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, RAND, (2016)[hereinafter RAND REPORT] (explicating the current state of technology, arguing that the existing liability regime is equipped to handle driverless vehicles, suggesting that determination of liability include a more global cost-benefit analysis, and offering other policy guidance).

70. Bryant Walker Smith, *Automated Vehicles Are Probably Legal in the United States*, 1 TEX. A&M L. REV. 411 (2014).

71. Dorothy J. Glancy et al., *A Look at the Legal Environment for Driverless Vehicles*, NCHRP LEGAL RESEARCH DIGEST 69, Pre-publication draft (Oct. 2015).

72. *See*, https://www.law.umich.edu/events/automatedvehicles/Pages/default.aspx.

their perspectives related to ACVs. These perspectives came from existing automotive manufacturers, suppliers, technology companies, insurance providers, startup companies, federal and state governments, local municipalities, academics, and attorneys in private practice, among others. The authors' research has been aided greatly by these conversations and the variety of perspectives shared.

This report focuses on the following topics. Part II addresses the state and regulatory issues related to autonomous and connected vehicles, and the possibility of preemptive federal action. Our research, in particular our conversations with industry participants from a diversity of perspectives, unambiguously indicated that the state and federal regulatory issues will likely serve a significant gating function as to which technologies and business models come to market. There appears to be a consensus forming around the need for uniformity in regulatory approaches, and increased activity from NHTSA around clarifying automotive regulations and standards related to ACVs. Accordingly, this section also addresses the framework for federal preemption of state regulations.

Part III addresses legal and regulatory issues related to new models of industry coordination and technology integration. While there is uncertainty around which business models for ACVs will prevail, there is certainty around the fact that existing and new entities in the automotive space will be coordinating in new ways. Also, there will be significant integration of technology not only in each vehicle but also in a sophisticated transportation network that will evolve. Therefore, participants will face new incentives and new risks. This Part first addresses potential evolutions in the existing supply chain model and the apportionment of risk achieved through its unique contracting regime. Second, this Part analyzes NHTSA's proposed Security Credential Management System, as an example of a potential networked and integrated transportation network model that will require companies to consider which roles and risks to assume. Third, this Part lays out the framework for cybersecurity liability and how it will impact the integrated and networked technology supporting ACVs. Last, this Part assesses how the existing automotive insurance regime may adapt in light of how the deployment of ACVs may shift liability risk.

Part IV lays out the tort liability models that would apply to the deployment of ACVs. This Part addresses products liability generally, component part supplier liability, including aftermarket liability, standard-setting organization liability, and liability for automated warning devices. Lastly, this Part frames the analysis for joint tort liability, which may present new or enhanced risks in light of the new models of industry coordination and technology integration.

Lastly, Part V addresses the topic of incentivizing innovative networks. Many aspects of the potential deployment of ACVs will require significant investment. This Part addresses questions and models for subsidizing that

investment. First, this Part looks at NHTSA's authority to require expenditures on the part of the so-called original equipment manufacturers (OEMs), vehicle operators, and local and state governments. Second, this Part addresses government liability, and the potential exposure of governments in deploying connected vehicle infrastructure. Third, this Part analyzes models for incentivizing innovative networks.

II. State and Federal Regulations and Preemption

Rather than rehash all of the early state activity related to AV legislation and regulation, this report attempts to:

- address the recent regulatory activity from NHTSA and how it might impact state regulations;
- identify the primary points of contention in the existing and proposed state rules, with a focus on California's draft operational regulations;
- analyze the real business implications of state regulations; and
- articulate the current legal and regulatory framework concerning preemption and show how federal standards concerning AVs might preempt state laws.

In the following sections we review the regulatory framework at the federal and state levels.[73]

A. *The Role of The National Highway Traffic Safety Administration*

For the last fifty years, the National Traffic and Motor Vehicle Safety Act of 1966 ("Safety Act") has served as the pillar of federal regulation of automotive safety. Congress passed the Safety Act with the stated purpose to "reduce traffic accidents and deaths and injuries resulting from traffic acci-

73. Much has been written about the various state regulations related to AVs. One of the early works on this topic, authored by a number of NHTSA and DOT attorneys, derived from Santa Clara Law School's Symposium in 2012. Wood et al., *supra* note 31. Smith's article *Automated Vehicles are Probably Legal in the United States* provides a detailed analysis of the 1949 Geneva Convention on Road Traffic, federal regulations promulgated by NHTSA, and the early state regulations. Smith, *supra* note 71, at 424-57. Smith's article starts with the premise that unless something is expressly illegal, it is legal. Id. at 414. Andrew Swanson's article *"Somebody Grab the Wheel!": State Autonomous Vehicle Legislation and the Road to a National Regime* also provides a thorough analysis of the regulatory framework for AVs through early 2014. Andrew Swanson, *"Somebody Grab the Wheel!": State Autonomous Vehicle Legislation and the Road to a National Region*, 97 Marq. L. Rev. 1085, 1126-45 (2014). The RAND Report provides a detailed overview of the state law and legislative activity as of 2014. RAND Report, *supra* note 70, at 41-53. Additionally, the draft publication from Dorothy Glancy, Robert W. Peterson, and Kyle F. Graham titled "A Look at the Legal Environment for Driverless Vehicles" overviews the relationship between the federal and state regulations. Glancy et al., *supra* note 72, at 87-93.

dents."[74] The Safety Act directed the Secretary of Transportation to establish safety standards that all motor vehicles must satisfy.[75] The Secretary of Transportation delegated this automotive safety authority to the National Highway Traffic Safety Administration ("NHTSA").

1. Background of NHTSA and the FMVSSs

In regulating automotive safety, NHTSA has promulgated over 60 Federal Motor Vehicle Safety Standards ("FMVSSs"). The Safety Act requires that all FMVSSs be practical, meet the need for motor vehicle safety, and be stated in objective terms. The FMVSSs are binding on all manufacturers and importers of motor vehicles and motor vehicle equipment.[76]

The FMVSSs serve as minimum standards. A manufacturer or distributor of a motor vehicle or equipment must certify at delivery that the vehicle or equipment complies with the FMVSSs.[77] If motor vehicles or equipment fail to comply with a FMVSS or contain a defect that poses an unreasonable risk to motor safety, then the Safety Act requires manufacturers to recall and remedy without charge.[78]

As explained by Wood et al., the Safety Act's broad definition of "motor vehicle equipment" effectively authorizes NHTSA "to regulate anything that is included with the motor vehicle at the time it is produced for sale to a member of the public.[79] Indeed, as further explained in the Wood et al., NHTSA has previously determined that GM's Onstar technology constitutes "motor vehicle equipment," therefore falling under NHTSA's authority. Accordingly, ACV equipment installed in a new motor vehicle at the time of manufacture would fall under NHTSA's authority.[80]

NHTSA's authority is not unlimited. NHTSA does not regulate vehicle owner activity, motor vehicle operation, or how vehicles are maintained and repaired once they are in use. Also, NHTSA can only limit after-market parts or modifications to the extent they remove or reduce the effectiveness of the vehicle's safety features required by NHTSA.

2. NHTSA's Activity Related to ACVs

a. NHTSA's Researching of Advanced Automated Technologies

NHTSA has been researching advanced automated vehicle technologies, such as automated crash avoidance safety systems, for several years.[81] In

74. National Traffic and Motor Vehicle Safety Act of 1966, Pub. L. No. 89-563, 80 Stat. 718, (codified as amended at 49 U.S.C. §§ 30101-03, 30111-26, 30141-47, 30161-69).
75. 49 U.S.C. § 30111(a) (2015).
76. 49 U.S.C. §§ 30101-69 (1994).
77. 49 U.S.C. § 30112(a)(2015).
78. 49 U.S.C. § 30120 (2015).
79. Wood et al., *supra* note 31 at 1441-42.
80. V2V Readiness Report, *supra* note 49, at 33-37.
81. NHTSA 2013 Preliminary Statement, *supra* note 29, at 2-3.

addition, for more than a decade, the Department of Transportation and NHTSA have been researching vehicle-to-vehicle communications.[82] NHTSA has explained the added benefits of V2V communications beyond the on-board crash avoidance technologies deployed on AVs:

> While these "vehicle-resident" crash avoidance technologies can be highly beneficial, V2V communications represent an additional step in helping to warn drivers about impending danger. V2V communications use on-board dedicated short-range radio communication devices to transmit messages about a vehicle's speed, heading, brake status, and other information to other vehicles and receive the same information from the messages, with range and "line-of-sight" capabilities that exceed current and near-term "vehicle-resident" systems – in some cases, nearly twice the range. This longer detection distance and ability to "see" around corners or "through" other vehicles helps V2V-equipped vehicles perceive some threats sooner than sensors, cameras, or radar can, and warn their drivers accordingly. V2V technology can also be fused with those vehicle-resident technologies to provide even greater benefits than either approach alone. V2V can augment vehicle-resident systems by acting as a complete system, extending the ability of the overall safety system to address other crash scenarios not covered by V2V communications, such as lane and road departure. A fused system could also augment system accuracy, potentially leading to improved warning timing and reducing the number of false warnings.[83]

NHTSA's V2V research has included driver clinics at six sites across the United States to access V2V user acceptance. A model deployment was conducted by the University of Michigan Transportation Research Institute in Ann, Arbor, Michigan from August 2012 to February 2014. This model deployment comprised approximately 2,800 vehicles operating on public streets within a highly concentrated area. The vehicles were equipped with connectivity devices using DSRC to emit signals containing information about vehicle position and heading.[84]

Additionally, NHTSA has also been testing the effectiveness of V2I communications. NHTSA has tested roadside equipment with DSRC devices transmitting information to vehicles. V2I connectivity may enable such safety applications as alerts about potential violations of upcoming red lights, curve speed warnings, alerts about when it is unsafe to enter an intersection, reduced speed zone warnings, weather condition warnings, railroad

82. V2V Readiness Report, *supra* note 50, at xiii.
83. *Id.* at xiv.
84. *Id.* at 9.

crossing warnings, and warnings to oversized vehicles about obstacles such as low bridges or tunnels.[85]

b. NHTSA's 2013 Preliminary Statement of Policy

NHTSA issued a Preliminary Statement of Policy Concerning Automated Vehicles in 2013 ("2013 Preliminary Statement"). According to NHTSA, it issued the statement "to help states implement [automated] technology safely so that its full benefits can be realized."[86] NHTSA recognized that "confusion or disarray on the safety issues would be a significant impediment to the development of these technologies."[87] NHTSA also explained that several states and companies seeking to develop automated technologies had requested NHTSA to make recommendations "on how to safely conduct [ ] testing [of automated vehicles] on public highways."[88]

The 2013 Preliminary Statement provides preliminary guidance to states seeking to allow automated vehicles to operate on public roadways. NHTSA recognized that "states are well suited to address issues such as licensing, driver training, and conditions for operation related to specific types of vehicles."[89] NHTSA went on, however, to express "considerable concerns" about states attempting to provide detailed regulations on the safety of "self-driving vehicles."[90] Indeed, NHTSA recommended against states permitting operation of self-driving vehicles for any purpose other than testing.[91]

NHTSA made clear that it was basing its recommendations on the assumption that Level 4 automation systems would not be ready for development in the near-term and even Level 3 automated systems were still in the "earlier stages of testing/development."[92] Accordingly, NHTSA believed that state regulation of such systems was premature.

NHTSA went on to make the following sets of preliminary recommendations concerning state regulations for the testing of self-driving vehicles.[93] First, NHTSA recommended ensuring that the driver understands how to operate a self-driving vehicle safely, such as through driver's license endorsements conditioned on completion of a training program. Second, NHTSA made a set of recommendations for how states should control the testing of self-driving vehicles. These recommendations included: (i) taking steps to minimize the risks to other road users, such as through manufacturer certification of some prior threshold of testing; (ii) requiring that a properly

85. *Id.* at 32-33.
86. NHTSA 2013 PRELIMINARY STATEMENT, *supra* note 28, at 1.
87. *Id.*
88. *Id.*
89. *Id.* at 10.
90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.* at 10-14.

licensed driver be seated in the driver's seat and ready to assume control of the vehicle; (iii) limiting testing to conditions suitable for the capabilities of the tested vehicles (such as limiting testing to limited access highways or inside certain geographical locations); and (iv) establishing reporting requirements to monitor the performance of self-driving technology during testing. Third, NHTSA recommended basic principles for testing of self-driving vehicles. These basic principles included: (i) ensuring that the transition from self-driving mode to driver control mode is "safe, simple, and timely;" (ii) test vehicles having the capability of detecting, recording, and informing the driver that the system of automated technologies has malfunctioned; (iii) ensuring that installation and operation of any self-driving vehicle technologies does not disable any federally required safety features or systems; and (v) ensuring that self-driving test vehicles record information about the status of the automated control technologies in the event of a crash or other safety event. Lastly, NHTSA went on to recommend against states authorizing the operation of self-driving vehicles for any purpose other than testing.[94]

c. DOT/NHTSA's 2016 Statement

In early 2016, the Department of Transportation and NHTSA issued a joint statement entitled "DOT/NHTSA Policy Statement Concerning Automated Vehicles" with the subtitle "2016 Update to 'Preliminary Statement of Policy Concerning Automated Vehicles'" ("2016 Updated Statement").[95] This statement began by recognizing that the rapid development of automated technologies had rendered the 2013 Preliminary Statement outdated and that both "partially and fully automated vehicles are nearing the point at which widespread deployment is feasible."[96] The 2016 Updated Statement went on to make two major announcements. First, it announced that in six months NHTSA would propose "best-practice guidance to industry on establishing principles of safe operation for fully autonomous [NHTSA level 4] vehicles."[97] Second, it announced that NHTSA, also within six months, would "work with states to craft and propose model policy guidance that helps policymakers address issues in both testing and the wider operational deployment of vehicles at advanced stages of automation and offers a nationally consistent approach to autonomous vehicles."[98]

The 2016 Statement went on to encourage manufacturers to seek NHTSA's exemption authority in order to receive permission to field test fleets. NHTSA's exemption authority allows it to exempt from its FMVSSs

94. *Id.*
95. 2017 UPDATED STATEMENT, *supra* note 26.
96. *Id.*
97. *Id.*
98. *Id.*

a limited number of vehicles for testing purposes.[99] NHTSA also recognized that its existing authority "is likely insufficient to meet the needs of the time and reap the full safety benefits of automation technology" and that NHTSA would reassess the need to update its authority.[100]

d. NHTSA's February 2016 Response to Google's Request for Interpretation

As explained by Smith, while the FMVSSs do not expressly prohibit AVs, some of the standards do present complications. For example, multiple FMVSSs appear to require particular actions by a "driver." As Smith pointed out, FMVSS 108, as interpreted by NHTSA in the past, likely requires hazard flashers capable of being manually activated by a driver.[101] Accordingly, questions exist as to how a fully AV, that does not even require a driver, could comply with FMVSSs requiring vehicle equipment with which a "driver" engages.

In light of some of these complications, Google submitted letters to NHTSA on November 12, 2015 and January 11, 2016 requesting NHTSA to interpret various provisions in the FMVSSs as they apply to Google's Self-driving car.[102] NHTSA's Chief Counsel, Paul Hemmersbaugh, responded to the letters on February 4, 2016.[103] In that letter, NHTSA explained that the FMVSSs "were drafted at a time when it was reasonable to assume that all motor vehicles would have a steering wheel, accelerator pedal, and brake pedal, almost always located at the front left seating position, and that all vehicles would be operated by a human driver."[104] Because of this assumption, NHTSA explained, several FMVSSs require that "a vehicle device or basic feature be located at or near the driver or the driver's seating position."[105] Accordingly, Google sought NHTSA's interpretation as to what could constitute a "driver" under the FMVSSs, and proposed multiple possible interpretations.

NHTSA generally agreed with one of Google's proposed interpretations, that the term "driver" as used in the FMVSSs refers to Google's Self-driving System ("SDS"). However, as explained below, even under Google's suggested interpretation, problems still arise in how Google could certify its compliance with specific aspects of the FMVSS, such as those requiring the "driver" to perform certain actions.

---

99. *See also Consumer Product Safety Guide Letter No. 1099*,(CCH), Consumer Prod. Safety Guide 396264, Iss. No. 1769 at 4 (Jan. 26, 2016) ("Exemption authority allows NHTSA to enable the deployment of up to 2,500 vehicles for up to two years if the agency determines that an exemption would ease development of new safety features.").

100. 2017 UPDATED STATEMENT, *supra* note 27.

101. Smith, *supra* note 71, at 459-460.

102. NHTSA LETTER TO GOOGLE, *supra* note 23.

103. *Id.*

104. *Id.*

105. *Id.*

As explained by NHTSA, FMVSS 135 requires service brakes that are activated by foot control, and a separate parking brake that may be activated by either hand or foot control. While NHTSA agreed with Google's interpretation that the SDS may constitute the "driver," that interpretation still does not allow Google to comply with the plain language of FMVSS 135. Google's Self-driving car would have no foot or hand control by which the service and parking brakes could be activated.[106]

NHTSA then addressed FMVSS 101, requiring certain controls to be located so as to be operable by the driver. It also requires indicators to be located in a place visible to the driver. Even interpreting the SDS to constitute the "driver," NHTSA stated that it "would be unable to conduct confirmatory testing to satisfy ourselves that the Google vehicle is compliant." NHTSA explained that additional rulemaking would be required to determine how the required controls and indicators could be located to be "operable by" and "visible to" the SDS. Alternatively, NHTSA suggested that Google may petition the agency for an exemption from these provisions as an interim solution.[107]

NHTSA next analyzed FMVSS 108 and 111. FMVSS 108 requires that the turn signal be cancellable by manual control and requires headlamp switches operable by movement of the driver's hand or foot. Even interpreting the SDS to be the driver, Google's car would not satisfy these provisions. FMVSS 111 requires vehicles to display a rearview image to the vehicle operator. Even construing the SDS as the driver or operator, NHTSA explained that it would have no way of confirming Google's certification that it was complying with this provision.[108]

Similarly, FMVSS 114 requires, for automatic transmissions with a park position, that the service brake be depressed prior to the transmission shifting from park. NHTSA agreed with Google's interpretation that the SDS could control the service brake and "accomplish the intent of this provision." NHTSA said it would require more information from Google about the functionality of its service brake mechanism to fully assess compliance.[109]

Next, FMVSS 126 contains test procedures that refer to particular measurements of steering wheel angle for purposes of testing a vehicles electronic stability control systems. NHTSA explained that it would need more information to understand how to test Google's self-driving car for compliance with this standard and then undertake rulemaking in order to adopt new test procedures. NHTSA also noted that Google could petition for an exemption from this provision.[110]

---

106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *Id.*

NHTSA provided similar commentary for other FMVSSs for which Google had sought interpretation via a table attached to its letter. As with the other provisions, NHTSA was in general agreement with Google's proposed interpretation of "driver" to include the SDS, but noted various provisions under which NHTSA could still not test for compliance under the existing FMVSS language.[111]

The Safety Act authorizes manufacturers to apply for temporary exemptions from the FMVSSs.[112] Upon receiving an application for exemption, NHTSA publishes notice of the application and provides an opportunity for comment.[113] In order to qualify for an exemption, NHTSA must find that the exemption is consistent with the public interest and the Safety Act, and in addition, one of the following four situations must exist. First, the manufacturer has tried to comply with the standard, and compliance would cause the manufacturer to incur substantial economic hardship. Second, development or field evaluation of a new safety feature providing improved safety benefits would be made easier. Third, development or field evaluation of a low-emission vehicle that does not unreasonably lower the vehicle's safety level would be made easier. Fourth, the manufacturer's compliance with the standard would prevent it from selling a vehicle with an overall safety level at least equal to the safety levels of nonexempt vehicles.

The first basis for an exemption is available only if the manufacturer did not produce more than 10,000 vehicles in the prior production year. An exemption granted on the first basis may not be granted for more than three years. The second, third, and fourth basis may be used to grant exemptions for not more than 2500 vehicles to be sold in the U.S. in any 12-month period. These exemptions may only be granted for a maximum of two years. NHTSA's decision and the reason for that decision are made public.[114]

e. Volpe Center Report

During the drafting of this report, the Volpe Center issued a report "Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles: Identifying potential barriers and challenges for the certification of automated vehicles using existing FMVSS" ("Volpe Center Report").[115] The Volpe Center Report identifies a number of FMVSSs that may "create certification challenges for automated vehicle concepts."[116]

---

111. *Id.*
112. 49 U.S.C. § 30113(b)(1),(2)(1998).
113. 49 U.S.C. § 30113(b)(2) (1998).
114. 49 U.S.C. § 30113(g) (1998); 49 C.F.R. § 555.7(d), (e)(1999).
115. Anita Kim, David Perlman, Dan Bogard & Ryan Harrington, *Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles: Identifying Potential Barriers and Challenges for the Certification of Automated Vehicles Using Existing FMVSS (Preliminary Report)*, U.S. Dep't of Transp. & John A. Volpe Nat'l Transp. Systems Ctr. (Mar. 2016).
116. *Id.* at viii.

B. *State AV Regulation*

1. History of State AV Regulations

Several commentators have extensively analyzed the timing, content, and procedure involving several of the early state regulations related to AVs.[117] The National Conference of State Legislatures maintains a website covering the enacted and proposed state AV laws.[118] Additionally, the University of Washington School of Law's Technology and Policy Clinic published the "Autonomous Vehicle Law Report and Recommendations to ULC" comparing the existing state AV law provisions.[119] Accordingly, this report will not repeat that information in detail.

To summarize the current situation at the state level concerning regulations of AVs, Nevada, in 2011, became the first state to pass AV legislation.[120] Nevada's DMV issued its first set of regulations in March 2012. Since then, other states or territories, including Florida,[121] California,[122] Michigan,[123] and the District of Columbia,[124] have passed laws governing AVs. Arizona's governor issued an executive order covering AVs.[125] Additionally, the Uniform Law Commission formed a "Study Committee on State Regulation of Autonomous Cars"[126] that has published recommendations for a uniform law on that topic.[127]

The following section overviews some of the major issues addressed in the enacted state laws.

---

117. Smith, *supra* note 72, at 501-08; Swanson, *supra* note 74, at 1125.

118. NAT'L COUNSEL OF ST. LEGISLATURES, *Autonomous Vehicles: Self-Driving Vehicles Legislation*, http://www.NCSL.org (Feb. 23, 2016), http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx.

119. U. Wash. Sch. of Law Tech. Law & Pol. Clinic, *Autonomous Vehicle Law Report and Recommendations to the ULC: Based on Existing State AV Laws, the ULC's Final Report, and Our Own Conclusions about What Constitutes a Complete Law*, https://www.law.washington.edu/Clinics/technology/Reports/AutonomousVehicle.pdf.

120. *See* NEV. REV. STAT. § 482A (2011).

121. FLA. STAT. § 316.85.

122. CAL. VEHICLE CODE § 38750.

123. MICH. COMP. LAWS §§ 257.663 – 257.665.

124. D.C. CODE § 50-2351 - 2354.

125. Ariz. Exec. Order No. 2015-09 (2015*), Self-Driving Vehicle Testing and Piloting in the State of Arizona; Self-Driving Vehicle Oversight Committee*, http://azgovernor.gov/executive-orders.

126. UNIFORM LAW COMMISSION, *New ULC Study and Drafting Committees Will Be Appointed*, WWW.UNIFORMLAWS.ORG (July 30, 2014), http://www.uniformlaws.org/NewsDetail.aspx?title=New%20ULC%20Study%20and%20Drafting%20Committees%20will%20be%20Appointed.

127. Uniform Law Commission Subcommittee on Issues, *Revised Report of the Subcommittee on Issues*, UNIF. L. COMM'N (2015).

2. Primary Issues Addressed

The enacted state laws typically begin with a definition of autonomous technology, autonomous vehicle, or both. Many of the states expressly carve-out existing NHTSA Level Two (or lower) technologies from the definition of "autonomous vehicles" covered under the act. For example, Michigan's Law defines "Automated technology" as "technology installed on a motor vehicle that has the capability to assist, make decisions for, or replace an operator." The law then defines "Automated motor vehicle" as "a motor vehicle on which automated technology has been installed, either by a manufacturer or automated technology or an upfitter that enables the motor vehicle to be operated without any control or monitoring by a human operator." The law continues in its definition of "Automated motor vehicle" to make clear that it does not cover existing NHTSA Level Two (or lower) technologies:

> Automated motor vehicle does not include a motor vehicle enabled with 1 or more active safety systems or operator assistance systems, including, but not limited to, a system to provide electronic blind spot assistance, crash avoidance, emergency braking, parking assistance, adaptive cruise control, lane-keeping assistance, lane departure warning, or traffic jam and queuing assistance, unless 1 or more of these technologies alone or in combination with other systems enable the vehicle on which the technology is installed to operate without any control or monitoring by an operator.

Many states expressly prohibit the use of AVs beyond the expressly permitted uses in the state laws. For example, the Michigan law prohibits the operation of AVs except under the express provisions of the law (e.g., for testing).[128]

The Michigan law permits testing of automated vehicles, under certain conditions. The manufacturer must submit proof of insurance to the secretary of state.[129] The vehicle must only be operated by an employee, contractor or other designated individual of the manufacturer conducting the testing.[130] During testing on public roads, the vehicle must have present a licensed driver capable of monitoring the vehicle's performance and, if necessary, taking control of the vehicle.[131] Michigan's law requires special plates for AVs in testing.[132]

---

128. MICH. COMP. LAWS § 257.663 (2000).

129. MICH. COMP. LAWS § 257.665(1) (2000); Other states actually provide particular insurance or bond minimums. California, for example, requires manufacturers have $5 million insurance policies, a $5 million bond, or make a $5 million deposit or bond with the state DMV as proof of financial responsibility and capability to cover liabilities.

130. *Id. at* § 257.665(2)(a) (1949).

131. *Id. at* § 257.665(2)(b)(c) (1949).

132. *Id. at* §257.225 (1949).

The Michigan law requires the state transportation department, in consultation with the secretary of state and industry experts, to submit a report covering the additional legislative or regulatory action necessary for the continued safe testing of automated motor vehicles.[133]

Similar to several of the other states that have enacted AV laws, Michigan's laws grants immunity to manufacturers for damages arising from aftermarket modifications to an automated vehicle.[134]

Some of the state laws address the presence and use of electronic data recorders in AVs. For example, Nevada's law requires electronic data recorders during testing.[135]

The states that address the operation of AVs, beyond the purposes of testing, all require some form of certification. For example, California requires the manufacturer to certify the following: certain operational characteristics of the vehicle;[136] the vehicle meets, and the technology does not render inoperative, the FMVSSs as well as any other relevant state and federal regulations;[137] and the manufacturer has tested the vehicle on public roads and complied with the testing standards.[138] The law provides the California DMV the right to issue further testing and performance certification standards.[139]

3. California's Draft Rules for the Non-testing Operation of AVs

California passed Senate Bill 1298 on September 25, 2012 expressly permitting the testing of AVs on public roads.[140] The California Statute conditioned AV testing on: (i) the AV is operated solely by employees, contractors, or designated personnel of the manufacturer; (ii) a driver is in the driver's seat, monitoring the vehicle, and capable of taking over control; and (iii) the manufacturer provides insurance or equivalent protection of at least $5,000,000.[141]

California's statute contemplates the possibility that at least some AVs would not have a human actively monitoring the vehicle or even present in the "driver's seat."[142]

---

133. *Id. at* §257.665(6) (1949).
134. *Id. at* §257.817.
135. NEV. ADMIN. CODE. § 482A.110(2)(b) (2012).
136. CAL. VEH. CODE § 38750(c)(1)(A)-(D) (2015).
137. *Id.* at § 38750(c)(1)(E)-(F).
138. *Id.* at § 38750(c)(2).
139. *Id.* at § 38750(d)(1).
140. *Id.* at § 38750(b).
141. *Id.* at § 38750(b)(1)-(3).
142. *See id.* at §38750(a)(4) (defining "operator" of an autonomous vehicle is "the person in the driver's seat, or, if there is no person in the driver's seat, causes the autonomous technology to engage."); *See id.* at § 38750(d)(2) (directing the DMV to adopt regulations "for safe operation of autonomous vehicles on public roads, with or without the presence of a driver inside the vehicle.").

The California Statute directs the California Department of Motor Vehicles ("California DMV") to adopt regulations governing: (i) "the submission and approval of an application to operate an autonomous vehicle;" and (ii) "any testing, equipment, and performance standards, in addition to those established [under the statute]."[143] The California DMV broke the regulatory process into two phases. In the first phase, the California DMV adopted regulations concerning the testing of AVs on May 19, 2014, which became effective on September 16, 2014.[144] As of March 22, 2016, the California DMV had issued Autonomous Vehicle Testing Permits to: Volkswagen Group of America, Mercedes Benz, Google, Delphi Automotive, Tesla Motors, Bosch, Nissan, Cruise Automation, BMW, Honda, Ford, and Zoox, Inc.[145] Accident and Disengagement Reports for these testing activities are available on the California DMV website.[146]

In the second phase, the California DMV is currently seeking to establish regulations concerning the operation of AVs in California. The California DMV held multiple public hearings on its proposed regulations.[147] On December 16, 2015, California issued its long awaited draft regulations ("Draft Regulations").[148]

Among other requirements, the Draft Regulations require the following:

- a licensed operator to be present inside the vehicle and capable of taking control of the vehicle;
- manufacturers to certify their compliance with specific AV safety and performance requirements;
- a third-party testing organization must verify a vehicle's performance;
- manufacturers to regularly report on the performance, safety, and usage of the vehicles;

143. *Id. at* § 38750(d).

144. *Cal. Code Regs. tit. 13 § 227* (2014), https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/testing.

145. CA DEP'T OF MOTOR VEHICLES, *Autonomous Vehicles in California: Testing of Autonomous Vehicles* (2014), https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/testing.

146. *Id.*

147. The DMV held public workshops in April 2013, March 2014 and January 2015. *See CA DMV*, *CA DMV Public Workshop on Autonomous Vehicle Regulations*, YOUTUBE (Mar.11 2014), https://www.youtube.com/watch?v=cKSHs8cEPOg*; see also Autonomous Vehicles Workshop (January 27, 2015) - Part 1* (Jan. 27, 2015), https://www.youtube.com/watch?v=oRTo230aN1k; *see also id., Autonomous Vehicle Regulations Public Workshop - Part 2* (Mar. 14, 2014), https://www.youtube.com/watch?v=W_zxk4JA7Ro. Additionally, a Request for Information released in July 2014, collected information from entities interested in conducting third-party safety certifications of autonomous vehicles or technology.

148. CA DEP'T OF MOTOR VEHICLES, *Autonomous Vehicles in California: Deployment of Autonomous Vehicles for Public Operation*, https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/auto.

- manufacturers to disclose, and obtain operator approval, if the manufacturer collects information other than what is needed for safety purposes; and
- vehicles must be equipped with diagnostics that detect and respond to cyber-attacks, alerting the operator, and allowing the operator to over-ride.

The Draft Regulations have received significant commentary. In particular, manufacturers have expressed concerns about several aspects of the Draft Regulations, as further discussed below.

a. Licensed Operator

Perhaps the most controversial provision of the Draft Regulations is its requirement of the presence of a licensed driver in the car. Section 227.52 prohibits the testing or deployment of any vehicle that is "capable of operation without the presence of an operator inside the vehicle."[149] The Draft Regulations require that this operator hold both a valid driver's license and a certificate for operating AVs.[150] Further, the operator must be "capable of taking over immediate control of the vehicle in the event of an autonomous technology failure or other emergency.[151] The practical impact of these provisions is that California would prohibit the operation of fully autonomous cars, typically labeled as NHTSA Level 4. In particular, these regulations would prohibit the "Self-Driving" car that Google has been developing.

i. Objections from Individuals with Disabilities

This provision has received significant concern from the disabled community. One of the primary use cases for Google's Self-Driving car, as well as other fully autonomous vehicles, is to provide mobility to individuals previously unable to drive, such as the disabled, or the elderly. At the two workshops held by the California DMV, representatives of the disabled community expressed extensive concerns.[152] Generally speaking, these comments made clear that fully autonomous (NHTSA Level 4) vehicles can provide much needed access to transportation and commerce to groups lacking that access.[153]

---

149. DRAFT REGULATIONS, *supra* note 16, at § 227.52(5).
150. *Id.* at § 227.84(a).
151. *Id.* at § 227.84(c).
152. *January 28, 2016 Workshop*, *supra* note 67, at 25:40-38:00; *CA DMV, Autonomous Vehicle Workshop*, YOUTUBE (Feb. 2, 2016) at 12:00-27:00, https://www.youtube.com/watch?v=nQx3nWWEeVA [hereinafter *February 2, 2016 Workshop*].
153. *January 28, 2016 Workshop*, *supra* note 67, at 27:40.

ii. Safety Determinations

Potential vehicle manufacturers, technology providers, and other interested commentators also expressed concerns. Several expressed the view that including the driver in the operational loop and expecting a driver to be able to resume control of the car, actually makes the cars less safe.[154] Many of these commentators pointed to studies showing the amount of time it takes a non-engaged driver to orient themselves to safely resume control of the vehicle.[155]

In response, the California DMV has stressed that the California statute requires the regulations for the deployment of autonomous vehicles to ensure "safety."[156] With both sides indicating they are seeking the safest mechanism for deploying AVs, there appears to be a fundamental disagreement about the safest model for vehicle operation for NHTSA Level 4 vehicles. On one hand, it appears the Draft Regulations reflect a view that it is safer to have a licensed operator in the vehicle in order to assume control of the car when autonomous function is not possible.

On the other hand, Google submits that an autonomous vehicle would be safer if a passenger was prohibited from resuming control of the car. As explained by Chris Urmson, the director of Google's self-driving car project, "We need to be careful about the assumption that having a person behind the wheel will make the technology more safe." He continued to explain that "[i]t's a generally understood problem with people monitoring for long durations of fairly robust technology. They do it poorly. Failures result from it."[157] In testifying before Congress, Urmson cited research from the Virginia Tech Transportation Institute showing that human operators of partially autonomous vehicles took up to 17 seconds to respond to alerts and assume full control of the vehicle.[158]

---

154. *Id.* at 38:45; *February 2, 2016 Workshop*, *supra* note 153, at 49:00; 1:18:00.

155. *See, e.g.*, *id.* at 49:00.

156. *Id.* at 4:43.

157. Alison Vekshin, *Self-Driving Cars Would Need a Driver in California*, BLOOMBERG BUS. (Jan. 28, 2016), http://www.bloomberg.com/news/articles/2016-01-28/self-driving-cars-would-need-a-driver-under-california-rules.

158. GOOGLE, *Testimony of Dr. Chris Urmson, Director of Self-Driving Cars, Google [x] Before the Senate Committee on Commerce, Science and Technology Hearing: "Hands Off: The Future of Self-Driving Cars"*, (Mar. 15, 2016), http://www.commerce.senate.gov/public/_cache/files/5c329011-bd9e-4140-b046-a595b4c89eb4/BEADFE023327834146FF4378228B8CC6.google-urmson-testimony-march152016.pdf [hereinafter Urmson March 15, 2016 Testimony] (citing NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *Human Factors Evaluation of Level 2 and Level 3 Automated Driving Concepts*, (July 2014), http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812044_HF-Evaluation-Levels-2-3-Automated-Driving-Concepts-f-Operation.pdf).

iii. Entrenchment

Several manufacturers expressed concerns that other states might follow California in adopting the licensed driver requirement and thus this requirement could become entrenched. One manufacturer explained that while driverless cars might not be currently ready for deployment, we should all hope that they become available within the lifetime of the Draft Regulations.[159]

This concern about "entrenchment" could be addressed, at least in part, by calling for the licensed operator requirement to be revisited in the near future. The authors are not aware of any manufacturer indicating it is ready to publicly deploy a driverless car in the very near future. Accordingly, the concern is that the licensed operator requirement, while irrelevant now, could remain in effect even later, at a point in time when driverless cars are ready for safe road use. Providing an express mechanism for revisiting this issue might appease the parties concerned with this provision on "entrenchment" grounds.

iv. Licensed Operator Requirement Not Mandated by Statute

Additionally, one manufacturer's legal counsel pointed out that the California Statute permits the possibility of driverless cars and does not require the California DMV to adopt regulations requiring the licensed driver.[160] This speaker was correctly referencing the express statement in the California statute calling on the DMV to pass regulations for "for safe operation of autonomous vehicles on public roads, with or without the presence of a driver inside the vehicle."[161]

v. Deciding Between Technology Tracks

One manufacturer representative pointed out that the technology is moving along at least two tracks. One is an incremental approach where the level of automated technology in a car will increase until it eventually becomes fully autonomous. The other track is one where fully autonomous vehicles, currently under development and testing, would be available for deployment in the near future. This commentator pointed out that the Draft Regulations were clearly adopting the incremental approach and would therefore be inhibiting the development of one track of the technology.[162]

This commentator raises the point made in Section 1.B. above. ACV technology is developing in at least four distinct tracks simultaneously. Vari-

159. *January 28, 2016 Workshop*, *supra* note 67, at 1:16:01.

160. *Id.* at 1:12:00.

161. *See* CAL. VEH. CODE § 3870(a)(4) (defining "operator" of an autonomous vehicle as "the person in the driver's seat, or, if there is no person in the driver's seat, causes the autonomous technology to engage."); *See id.* at § 3870(d)(2) (directing the DMV to adopt regulations "for safe operation of autonomous vehicles on public roads, with or without the presence of a driver inside the vehicle.").

162. *February 2, 2016 Workshop*, *supra* note 153, at 1:31:00.

ous companies are developing business models around these tracks. It is worth noting that some of the provisions in the state regulations, such as California's Draft Regulations, will impact, if not determine, the business models for ACV's that come to market. For example, at least one version of Google's self-driving car does not include a steering wheel and is intended to not require a licensed driver.[163] Some of Google's primary use cases for its vehicles involve unlicensed individuals, such as the elderly,[164] and the disabled.[165] State regulations that require a licensed operator in the car would essentially eliminate the possibility of one of the business models for autonomous vehicles.

It is also worth noting, that a misalignment of interests exists between the entities developing AVC's on at least some of the provisions at issue in state regulations. Although not reflected in the public commentary, it is possible that a company developing technology along the track of progressive automation of vehicles is not as opposed to the licensed operator requirement as a company seeking to bring NHTSA Level 4, driverless, vehicles to market in the near term.

b. Certification and Third-Party Testing

The draft regulations provide requirements for an application for a permit to allow deployment of AVs on California's public roads.[166] Among other requirements, the application must include a certification from the manufacturer. First, the manufacturer must certify that the AVs perform certain behavioral competencies identified on the application.[167] The manufacturer must also certify that it adheres to "an established safety plan for the design and development of the subject autonomous vehicles."[168] The manufacturer must certify that the AV's autonomous technology is designed to comply with California's Vehicle Code and local regulation related to detecting and responding to roadway situations.[169]

---

163. GOOGLE, *Google Self-Driving Car Project*, https://www.google.com/selfdrivingcar/how/ ("We removed the steering wheel and pedal, and instead designed a prototype that lets the software and sensors handle the driving.").

164. Brian Fun, *The Future of Google's Driverless Car Is Old People*, WASH. POST, (May 28, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/05/28/the-future-of-googles-driverless-car-is-old-people/.

165. Paul Stenquist, *In Self-Driving Cars, a Potential Lifeline for the Disabled*, N.Y. TIMES (Nov. 7, 2014), https://www.nytimes.com/2014/11/09/automobiles/in-self-driving-cars-a-potential-lifeline-for-the-disabled.html.

166. DRAFT REGULATIONS, *supra* note 15, at § 227.56.

167. *Id.* at § 227.58(b)(1); The California DMV also issued a draft form OL 318 titled "Application for Permit to Deploy Autonomous Vehicles on Public Streets." CA DMV, *Application for a Permit to Deploy Autonomous Vehicles on Public Streets*, https://www.dmv.ca.gov/portal/wcm/connect/19360b4c-1ac0-4fbf-b8d7-432d8289cb08/ol318.pdf?MOD=AJPERES.

168. DRAFT REGULATIONS, *supra* note 15, at § 227.56(b)(2).

169. *Id.* at § 227.56(b)(4).

Additionally, the manufacturer must also submit the results of the third-party vehicle demonstration test.[170] This third-party vehicle test is further explained in § 227.58 and §227.60 of the Draft Regulations, which provide significant detail about the nature of the third-party test and the requirements for the third-party.[171] In particular, the third-party test organization must both review the manufacturer's own test data (for example showing it meets the known behavior competencies) and independently test the vehicle on California roads.[172] The Draft Regulations also provide requirements concerning the third-party test organization's expertise related to AVs and independence from the manufacturers submitting vehicles for testing.[173]

Furthermore, manufacturers are responsible for educating the vehicle operator on the operation and competency of the AV. The manufacturer must submit this education plan as part of its application.[174] Commentators have also expressed concerns about the certification and third-party testing requirements. Many manufacturers generally opposed the third-party testing requirements. These manufacturers pointed to their long history of working in a self-certification framework as required by NHTSA.[175] Manufacturers pointed to new technologies such as anti-lock brakes that required drivers to unlearn old practices, yet did not require a special certificate.[176] These manufacturers pointed out that a licensed driver in California can drive a motorhome or pull a larger trailer without any special certification or education.[177]

One manufacturer explained that the third party certification requirement in combination with the relatively general and vague behavioral competencies of different regulatory bodies was a dangerous combination. It was pointed out that NHTSA has experienced researchers capable of developing and assessing such competencies.[178]

Another concern raised was how the third-party testing requirement may inhibit the incremental expansion of the technology package with software updates. As explained by one manufacturer, manufacturers may desire to expand the autonomous functionality of the car through incremental software releases. The Draft Regulations might require a separate testing procedure prior to each software release.[179] Another manufacturer pointed out that the amendment application process dictated by the Draft Regula-

170. *Id.* at § 227.56(b)(3).
171. *Id.* at § 227.58, 227.60.
172. *Id.* at § 227.58.
173. *Id.* at § 227.60.
174. *Id.* at 227.56(b)(3).
175. *January 28, 2016 Workshop*, *supra* note 67, at 1:12:00.
176. *Id.* at 1:19:30.
177. *Id.*; *February 2, 2016 Workshop*, *supra* note 152, at 1:47:33.
178. *January 28, 2016 Workshop*, *supra* note 153, at 2:47:00.
179. *Id. at* 2:14:00.

tions might be implicated by many software updates, thus causing significant delays in the release of critical updates.[180]

c. Privacy and Cyber-Security Requirements

The Draft Regulations require the manufacturer to certify that the AV has "self-diagnostic capabilities that meet current industry best practices and are capable of detecting and responding to cyber-attacks, unauthorized intrusions, and false or spurious messages, and then alert the operator."[181] The vehicle must be able to alert the operator of a cyber-attack and allow the operator's commands to override the commands generated by the autonomous technology.[182]Additionally, a manufacturer must disclose, and receive written approval from the operator, prior to collecting information that is not necessary for vehicle safety.[183]

One commentator pointed out that the privacy disclosure and approval requirement does not make sense in the context of a TNC such as Uber or Lyft.[184] The "operator" would likely be the independent contractor of the TNC, whereas the sensitive personal information (such as pickup and drop-off locations) would likely belong to the TNC customer. Accordingly, the requirement to obtain written approval from the "operator" likely does not address the primary privacy concerns in that context (i.e., the privacy of the TNC customer).

d. Uniformity Concerns

One manufacturer's legal counsel pointed out the dangers of having a variety of different regulations among the states.[185] The suggestion was made to work closely with NHTSA and other states in forming a uniform fifty-state rule.[186] California's DMV indicated that it was, indeed, working closely with NHTSA and a group of state regulators on model state regulation.[187]

Others involved in preparing to deploy AVCs have echoed this desire for uniformity expressed by the above OEM counsel. As explained by Volvo's president:

> The US risks losing its leading position due to the lack of Federal guidelines for the testing and certification of autonomous vehicles. [ ] The absence of one set of rules means car makers cannot conduct

180. *February 2, 2016 Workshop*, *supra* note 153, at 2:12:00.
181. DRAFT REGULATIONS, *supra* note 15, at § 227.56(b)(10).
182. *Id.*
183. *Id.* at §227.76(a).
184. *February 2, 2016 Workshop*, *supra* note 152, at 2:45.
185. *Id.*
186. *Id.*
187. *January 28, 2016 Workshop*, *supra* note 66, at 1:32:00.

> credible tests to develop cars that meet all the different guidelines of all 50 U.S. states.[188]

A spokesperson for Audi has explained:

> The technology benefits [from] uniformity from state to state and between states and federal regulations. National standards are critical to the trucking industry, especially with respect to new and innovative technologies.[189]

There are multiple avenues for achieving uniformity. First, states could coordinate so that their regulations are consistent on the critical provisions that impact ACV design and development. Some state coordination exists on this topic. The American Association of Motor Vehicle Administrators has assembled an "Autonomous Vehicles Best Practices Working Group,"[190]

Alternatively, the federal government could pass regulations that preempt state laws. Commentators have also suggested the need for federal preemption of state laws in order to create a uniform set of standards for AVs.[191] Section II.D addresses the possibility of federal preemption.

4. NHTSA's Model State Policy Guidance

Indeed, it appears NHTSA is aware of the need for uniformity in ACV regulations. U.S. DOT Secretary Foxx announced on January 14, 2016 that NHTSA would "work with states to craft and propose model policy guidance that helps policymakers address issues in both the testing and wider operational deployment of vehicles at advanced stages of automation and offers a nationally consistent approach to autonomous vehicles."[192] NHTSA committed to releasing this model policy within six months.[193]

---

188. *US Urged to Establish Nationwide Federal Guidelines for Autonomous Driving*, VOLVO CAR GROUP (Oct. 7, 2015), https://www.media.volvocars.com/global/en-gb/media/pressreleases/167975/us-urged-to-establish-nationwide-federal-guidelines-for-autonomous-driving.

189. Alex Davies, *The Feds Will Have Rules For Self-Driving Cars in the Next 6 Months*, WIRED (Jan. 14, 2016), http://www.wired.com/2016/01/the-feds-want-rules-for-self-driving-cars-in-the-next-6-months/.

190. *See Autonomous Vehicles Best Practices Working Group*, AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS, http://www.aamva.org/Autonomous-Vehicle-Best-Practices-Working-Group/.

191. *See, e.g.*, Julie Goodrich, *Driving Miss Daisy An Autonomous Chauffeur System*, 51 HOUS. L. REV. 265, 293 (2013) (suggesting a need for federal regulations preempting state laws on autonomous vehicles in order to achieve uniformity); Orly Ravid, *Don't Sue Me, I Was Just Lawfully Texting & Drunk When My Autonomous Car Crashed Into You*, 44 SW. L. REV. 175, 189 (2014) (suggesting a need for uniformity in state laws regarding autonomous vehicles).

192. 2017 UPDATED POLICY STATEMENT, *supra* note 26, at 2.

193. *Id.*

While it appears NHTSA is heeding the concerns related to the issues raised with California's Draft Regulations, it is unclear what impact the NHTSA model policy guidance will have on states. Section II.C. addresses the possibility of federal preemption of state regulations related to AVCs.

5. Google's Request for Congressional Action

Google's Chris Urmson testified on March 15, 2016 before the Senate Committee on Commerce, Science and Technology.[194] At that hearing, Google requested that Congress take action to empower the Department of Transportation to facilitate the safe deployment of self-driving AVs:

NHTSA's reply to our request for interpretation and its 2017 Congressional budget request both highlighted that "[n]ew authorities may be needed when they are necessary to ensure that fully autonomous vehicles, including those designed without a human driver in mind, are deployable in large numbers when demonstrated to provide an equivalent or higher level of safety than is now available."

> We strongly support NHTSA's goals and believe that Congressional action is needed to keep pace with safety technologies being developed by vehicle manufacturers and technology innovators, including fully self-driving cars.
>
> To achieve this goal, we propose that Congress move swiftly to provide the Secretary of Transportation with new authority to approve life-saving safety innovations. This new authority would permit the deployment of innovative safety technologies that meet or exceed the level of safety required by existing federal standards, while ensuring a prompt and transparent process.[195]

Google reportedly followed up its testimony with a letter to DOT providing further specifics on the Congressional action it was requesting.[196]

C. *The Potential for Federal Preemption*

Currently, the only federal agency claiming jurisdiction over the safety aspects of ACVs is NHTSA.[197] NHTSA views autonomous vehicles and the

194. GOOGLE, *Hands Off: The Future of Self-Driving Cars* (Mar. 15, 2016) (U.S. Senate Committee on Commerce, Science and Technology testimony of Dr. Chris Urmson, Director, Self-Driving Cars, Google), https://www.commerce.senate.gov/public/_cache/files/5c329011-bd9e-4140-b046-a595b4c89eb4/BEADFE023327834146FF4378228B8CC6.google-urmson-testimony-march152016.pdf.

195. *Id.* at 5 (emphasis removed).

196. Justin Pritchard, *Google Gives Federal Plan for Self-Driving Car*, AP (Mar. 17, 2016, 11:56PM), http://bigstory.ap.org/article/e163176d93e34b818672915480f4fba8/apnews break-google-details-federal-fix-self-driving-car.

197. As discussed, other agencies, such as the FTC for cybersecurity and the FHWA for roadside infrastructure will also impact aspects of ACV deployment.

accompanying technologies as the next wave of traditional automotive safety,[198] meaning that these technologies fall well within NHTSA's established jurisdiction.[199] Moreover, NHTSA's authorizing statute defines "motor vehicle" in a way that omits any reliance on a human driver and thus appears to encompass autonomous vehicles: "a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways."[200] It therefore seems unlikely that, absent new federal legislation, another federal agency would attempt to take primary responsibility for regulating safety and technology features in autonomous cars. The other types of technological or social developments to which autonomous vehicles have been compared in various capacities—specifically, industrial robots, vaccines, and aviation autopilot—have little relevance as relating to federal regulation.[201] There have been calls for the creation of a Federal Robotics Commission to deal with the increasingly complex interaction among computer programming, software, and hardware in independently regulated devices, but this proposal has yet to gain traction in the federal government.[202]

However, the Federal Communications Commission (FCC) may eventually assume a significant role in the regulation of autonomous vehicle technologies. In 1999, the FCC reserved the 5.9 GHz band solely for vehicle-to-vehicle (V2V) communications.[203] Mounting pressure from lawmakers to open up portions of this band for other technologies appears to have increased the urgency among federal agencies to encourage development of V2V technologies and demonstrate their value.[204] In recent months, the DOT and FCC have been working closely to expedite proposed regulations requiring V2V technologies in all new vehicles.[205] With regard to data privacy, autonomous vehicle technologies present many of the same issues as cellular

198. *See* NHTSA 2013 PRELIMINARY STATEMENT, *supra* note 28, at 1-3.

199. *See* 49 U.S.C. § 30101 (1994).

200. 50 U.S.C. § 30102(a)(6); *see also* 49 U.S.C. § 30102(a)(7)–(9).

201. These areas are all regulated by topic-specific federal agencies, similar to NHTSA: the Occupational Safety and Health Administration regulates industrial robots, the Centers for Disease Control cover vaccines, and the Federal Aviation Administration sets standards for aircraft.

202. Ryan Calo, *The Case for a Federal Robotics Commission*, BROOKINGS (2014), http://www.brookings.edu/research/reports2/2014/09/case-for-federal-robotics-commission.

203. Michael O'Rielly & Jessica Rosenworcel, *Steering into the Future with More Wi-Fi by Sharing the Upper 5 GHz Band*, FCC BLOG (Sept. 16, 2015, 4:45 PM), https://www.fcc.gov/news-events/blog/2015/09/16/steering-future-more-wi-fi-sharing-upper-5-ghz-band.

204. *Id*.

205. Antuan Goodwin, *US Transportation Secretary Foxx Talks Autonomous Cars in Silicon Valley*, ROADSHOW (May 13, 2015, 3:55 PM), http://www.cnet.com/roadshow/news/us-transportation-secretary-anthony-foxx-talks-autonomous-cars-v2v-communication-requirements-in/; Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 49270 (proposed Aug. 20, 2014)(to be codified at 49 C.F.R. pt. 571).

phones and Internet usage,[206] and thus the FCC may at least be an important collaborator, if not co-regulator, with NHTSA.

Several commentators have addressed the possibility of the preemptive effect of NHTSA's FMVSSs.[207] The Motor Vehicle Safety Act includes an express pre-emption clause, stating:

> When a motor vehicle safety standard is in effect under this chapter, a State or a political subdivision of a State may prescribe or continue in effect a standard applicable to the same aspect of performance of a motor vehicle or motor vehicle equipment only if the standard is identical to the standard prescribed under this chapter.[208]

This clause is subject to a savings clause, stating that "[c]ompliance with a motor vehicle safety standard prescribed under this chapter does not exempt a person from liability at common law."[209] Accordingly, while NHTSA can preempt state safety standards related to "motor vehicles" and "motor vehicle equipment," the preemptive effect of FMVSSs on state tort liability is less clear. On one hand, the Supreme Court in 2000, in a 5-4 decision, held that FMVSS 208 involving airbags preempted a state tort action that "frustrated the purpose" of the safety standard.[210] On the other hand, the Supreme Court in 2011, unanimously ruled that FMVSS 208, as it relates to seatbelts, does not preempt state tort suits claiming that a manufacturer should have installed a particular type of seat belt.[211]

The University of Washington's Technology Law and Policy Clinic has put together an informative research memo about the likelihood of federal preemption based on NHTSA's initial statement of policy.[212] Their team found it unlikely that NHTSA would preempt state testing or administrative regulations regarding licensing, permits, and driver training and likely that NHTSA would preempt most state safety standards.[213] This prediction essentially lines up with NHTSA precedent for traditional automobiles.

---

206. William J. Kohler & Alex Colbert-Taylor, *Current Law and Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles*, 31 SANTA CLARA HIGH TECH. L.J. 99, 120–21 (2015).

207. Gary E. Marchant & Rachel A. Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, 52 SANTA CLARA L. REV. 1321, 1338 (2012); Glancy et al., *supra* note 72, at 88.

208. 49 U.S.C. § 30103(b)(1).

209. 49 U.S.C. § 30103(e).

210. *See Geier v. Am. Honda Motor Co*., 529 U.S. 861, 873-74 (2000).

211. *See Williamson v. Mazda Motor of Am., Inc.,* 562 U.S. 323, 326 (2011).

212. TECH. LAW & POL'Y CLINIC, U. OF WASH., *The Risks of Federal Preemption of State Autonomous Vehicle Regulations* (2014), http://techpolicylab.org/wp-content/uploads/2014/12/UW-Law-Clinic-Research-Memo-to-the-ULC-The-Risks-of-Federal-Preemption-of-State-Regulations-of-Autonomous-Vehicles.pdf.

213. *Id.* at 1–2.

It is worth noting, however, that most of the prior analysis of NHTSA's likelihood of preemption is based on NHTSA's 2013 Preliminary Statement. The 2016 announcement from DOT and NHTSA, and in particular, the plan to adopt model policy guidance for states, indicates that NHTSA is increasingly active in AV regulation. By referring to its upcoming work as "model policy guidance" it is still unlikely that NHTSA is planning broad regulatory preemption of AV testing, licensing, permits, or driver training. The upcoming public hearings hosted by DOT on autonomous vehicles may reveal further information about the likelihood of preemptive rulemaking from NHTSA.

As discussed in Section II.B.5. above, Google has requested Congress to consider a legislative framework for AVs.[214] The above discussion relates to the possibility of preemption under NHTSA's current rulemaking authority. Commentators are in agreement that if Congress were to become involved, it could enact uniform national legislation concerning ACVs what would preempt any state AV laws or regulations.[215]

III. Issues Arising from Industry Coordination and Technology Integration

Most commentators agree that as vehicles become increasingly autonomous, the liability associated with vehicular accidents will shift from the driver to those involved in deploying the technology.[216] With a greater percentage of fault for accidents resting on those involved in deploying the technology, the risk allocation as between these companies may become critical. For a variety of reasons, companies involved in deploying ACVs will be faced with new relationships and strategic considerations due to new models of industry coordination and technology integration. As explained in a recent Boston Consulting Group report:

> Strategic trade-offs will influence decisions about whether to make or buy key components. On one hand, by keeping certain technology development—such as sensor fusion and software development—in-house, OEMs can limit their liability exposure and build competitive advantage. On the other hand, partnering with suppliers can be economically advantageous and obviate the need for investments in building internal capabilities. What's more, changes in lia-

214. Justin Pritchard, *Google Gives Federal Plan for Self-Driving Car*, PHYS.org, (March 17, 2016), http://phys.org/news/2016-03-google-federal-self-driving-car.html.

215. Glancy et al, *supra* note 72, at 93.

216. RAND Report, *supra* note 70, at 115-17 (discussing likely shift in fault from the driver to the manufacturer); Glancy et al., *supra* note 72, at 43-44 ("Existing analyses have reached the shared conclusion that a proliferation of driverless vehicles eventually will lead to an "upward" shift in the locus of civil liability for everyday accidents, away from drivers and toward the manufacturers of these devices.").

> bility laws may transfer a greater share of risk to OEMs. Bringing about such changes would require greater coordination among multiple stakeholders, including suppliers, insurance companies, lawmakers, and governments.[217]

As discussed in the following section, (i) as new players enter the automotive supply chain it is possible that the long-established automotive procurement contracting model will evolve; (ii) NHTSA's proposed SCMS system is an example of a technology network that will present manufacturers with new relationships involving industry coordination and technology integration; (iii) the increasingly integrated network of vehicles will present new risks related to cybersecurity; and (iv) it is possible that the existing automotive insurance model will evolve in reaction to the new transportation business models.

A. *An Evolving Supplier Contract Model*

Under any track (or combination of tracks) in which ACVs come to market, the amount of new technology, and software in particular, integrated in vehicles will increase significantly. By 2009, the standard new vehicle already had over 100 microprocessors, 50 electronic control units, five miles of wiring, and approximately 100 million lines of code.[218] The Boston Consulting Group recently explained that the in-vehicle software will continue to become more complex:

> The other critical technology in need of further development is the software that will interpret sensor data and trigger the actuators that govern vehicle braking, acceleration, and steering. The software will need to be highly intricate to contend with the complexity of the driving environment. To put things in perspective, the software in the latest Mercedes S-class vehicle, which is loaded with several ADAS features, contains roughly 15 times more lines of code than the software in a Boeing 787. The quantity of code required will multiply as vehicle manufacturers move from ADAS to partial autonomy and then full autonomy.[219]

---

217. Xavier Mosquet et al., *Revolution in the Driver's Seat: The Road to Autonomous Vehicles,* 23 Boston Consulting Group (April 2015), https://www.bcgperspectives.com/Images/BCG-Revolution-in-the-Drivers-Seat-Apr-2015_tcm80-186097.pdf.

218. Arthur Carter, David Freeman & Cem Hatipoglue, *An Overview of NHTSA's Electronics Reliability and Cybersecurity Research Programs*, 1 Nat'l Highway Traffic Safety Admin., http://www-esv.nhtsa.dot.gov/proceedings/24/files/24ESV-000454.pdf.

219. Xavier Mosquet et al., *Revolution in the Driver's Seat: The Road to Autonomous Vehicles*, 14 Boston Consulting Group (April 2015), https://www.bcgperspectives.com/Images/BCG-Revolution-in-the-Drivers-Seat-Apr-2015_tcm80-186097.pdf.

These software requirements will necessitate the entrance of new technology companies into the supply chain. These new players are likely to change the way the automotive procurement process functions. Some changes may be positive for OEMs. For example, a recent report by Mckinsey noted that "AV technologies could help to optimize the industry supply chains and logistics operations of the future, as players employ automation to increase efficiency and flexibility."[220] On the other hand, OEMs will likely be forced to interact with new types of technology providers. This might disrupt some of the existing efficiencies in the existing supply-chain contracting model, and might test the bargaining leverage historically imposed by the OEMs.

1. Structure of the Automotive Supply Chain

Historically, the automotive supply chain has been structured with OEMs like Ford, GM, Fiat-Chrysler, Toyota, Honda, and others at the top of the chain. OEMs assemble cars based on parts and subassemblies received from suppliers.[221] "Tier 1" suppliers, such as Delphi and Bosch, supply parts and subassemblies directly to OEMs.[222] Tier 1 suppliers purchase parts directly from Tier 2 suppliers, and so on. OEMs award supply contracts through competitive bidding.[223] While price and part design are heavily negotiated, the legal terms of the transaction have been typically dictated through boilerplate terms and conditions imposed by the OEMs.[224]

2. Auto Supply Contracts Generally

Several law firms offer ongoing analyses of OEM terms and conditions.[225] There are several provisions that are unique to automotive supply agreements. First, supply agreements are typically requirements contracts that place the risk of supply fluctuations largely on the suppliers.[226]

Second, buyers typically retain unilateral rights of termination.[227] An example of this is shown in paragraph 34 of GM's 2014 revised General Terms and Conditions:

---

220. Michele Bertoncello & Dominik Wee, *Ten Ways Autonomous Driving Could Redefine the Automotive World*, 5 McKinsey & Company (June 2015), http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/ten-ways-autonomous-driving-could-redefine-the-automotive-world.

221. Omri Ben-Shahar & James J. White, *Boilerplate and Economic Power in Auto Manufacturing Contracts*, 104 Mich. L. R. 953, 955-56 (2006).

222. *Id.*

223. *Id.* at 956.

224. *Id.* at 956.

225. Butzel Long, *Automotive Industry: Terms & Conditions and the Legal Matters Resource Center*, https://www.butzel.com/terms-and-conditions.

226. Butzel Long, *OESA Terms and Conditions and Current Legal Issues* 148 (Oct. 2015), http://www.oesa.org/Doc-Vault/Presentations/2015/2015-10-01-Updated-Butzel-Presentation.pdf.

227. Omri Ben-Shahar & James J. White, *supra* note 222, at 958.

> In addition to any other rights of Buyer to terminate this Contract, Buyer may, at its option, terminate all or any part of this Contract before the expiration date set forth in this Contract, at any time and for any reason, by giving notice to Seller.[228]

Upon termination under this provision, GM agrees to make certain payments for parts already completed and for costs of works-in-progress.[229]

Third, the OEMs typically require significant warranties and remedies.[230] The remedies typically include broad damages (direct, indirect, incidental, and consequential damages, as well as all fees) related to any recall or other corrective service action.[231]

Fourth, OEMs also typically require the supplier to continue to supply service parts for several years after the current model production ends.[232] A recent version of GM's Terms and Conditions provides:

> During the 15-year period after Buyer completes current model purchases, Seller will sell goods to Buyer to fulfill Buyer's past model service and replacement parts requirements. Unless otherwise agreed to by Buyer, the price(s) during the first 5 years of this period will be those in effect at the conclusion of current model purchases. For the remainder of this period, the price(s) for goods will be as agreed to by the parties.[233]

This term may have significant economic consequences because it requires a supplier to maintain production capacity for parts even when the vehicle is no longer in production, and therefore the OEM is not purchasing parts at scale.[234]

Fifth, OEMs typically obtain favorable IP rights. For example, OEMs require broad IP licenses (including "foreground" and "background" intellectual property) in the event the supplier fails to deliver.[235] This is likely driven by the "just-in-time" supply model, and the OEMs need to quickly source the parts in the event the supplier fails to perform. Additionally,

---

228. Tom Manganello & Jeena Patel, WARNER NORCROSS, *The Updated GM General Terms and Conditions* para. 35 (Feb. 2014), https://www.wnj.com/WarnerNorcrossJudd/media/files/uploads/Documents/Full_Presentation-The_Updated_GM_General_Terms_and_Conditions_2-20-14_2.pdf [hereinafter *2014 GM Terms & Conditions*].

229. *Id.* at para. 34.

230. Omri Ben-Shahar & James J. White, *supra* note 222, at 959-60; *See also 2014 GM Terms & Conditions*, *supra* note 229, at para. 13.

231. *2014 GM Terms and Conditions, supra* note 229, at para. 25.

232. Omri Ben-Shahar & James J. White, *supra* note 222, at 961-962.

233. *2014 GM Terms and Conditions*, *supra* note 228, at para. 25.

234. Omri Ben-Shahar & James J. White, *supra* note 222.

235. *2014 GM Terms and Conditions*, *supra* note 229, at para. 23.

OEMs typically retain broad IP rights to "foreground intellectual property" created by the supplier during the course of the supply agreement.[236]

Historically, these terms and conditions did not change very often.[237] As noted by professors Ben-Shahar and White, the OEM terms and conditions were typically drafted by in-house attorneys who retained their position and maintained significant institutional knowledge with the fixed terms.[238] Recently, however, there have been some instances where OEMs have responded to criticisms from the supplier community. For example, when GM revised its Terms and Conditions in 2013, it responded to concerns from its suppliers by revising those terms in 2014.[239]

In the past, most believed that several of these terms would cascade through the various tiers of supply agreements. Professors Ben Shahar and White noted that this was referred to as "contractual DNA," where certain provisions imposed by OEMs were necessarily imposed by Tier 1 suppliers on Tier 2 suppliers, and so on.[240]

3. Software Contracts Handled Differently

As software began to integrate into automobiles, the industry soon recognized that software supply agreements required a slightly different model. For example, Ben-Shahar and White recognized that IT suppliers were typically able to better protect their IP, which was a fundamental part of their ability to supply to all buyers.[241] Additionally those authors observed that IT suppliers were more successful at limiting and capping liability, and making fewer warranties.[242] Several industry members told the authors that because software is easier to fix, the OEMs are not as concerned about recall expenses.

4. The Existing Supplier Contract Model Will Evolve

It is possible that the above model may change significantly. New companies will likely enter the automotive supply chain. These companies will possess a different product development cycle and attitude towards risk allocation. As explained in a recent PWC report:

> Auto makers favor proprietary technology tightly linked to hardware, emphasizing reliability and regulatory compliance. Their development cycles are long and their closed systems don't interact well with outside technology. Technology firms are less concerned

236. *Id.* at para. 23(c).
237. Omri Ben-Shahar & James J. White, *supra* note 221, at 965.
238. *Id.* at 966.
239. *2014 GM Terms and Conditions*, *supra* note 229.
240. Omri Ben-Shahar & James J. White, *supra* note 222, at 969-970.
241. *Id.* at 962-963.
242. *Id.* at 978.

> with legacy systems. They value speed-to-market, versatility, rapid product development, and frequent iteration. Many operate on open platforms with standard protocols that can be used by a wide range of players. Their products show keen understanding of consumer needs, but can fall short in reliability and durability.[243]

Examples of these new relationships include Bosch partnering with TomTom, and a group of high-end auto manufacturers acquiring Nokia's mapping technology.[244]

These new players might also resist the customary supply chain contract model. As recognized by one group of automotive attorneys, "[m]any of the technologies needed to implement V2V will come from non-traditional suppliers unfamiliar with the rigors of OEM and tiered automotive supplier terms and conditions."[245] These commentators noted that these new technology suppliers likely will possess unique and untested technology, likely increasing the importance of intellectual property rights remaining with the supplier and the negotiation over risk allocation provisions.[246] Additionally, it is possible that for several of these technology suppliers, a single core technology will form the basis of their business model.[247]

Additionally, as the software supplied by technology companies becomes more integral to safety applications, it is likely that products liability will increase in priority in risk allocation considerations. For software involved in safety applications, failure may lead to vehicle accidents involving property damage or personal injury. On the other hand, software involved in other vehicle functions, such as environmental applications, failure is less likely to lead to property damage or personal injury. Accordingly, the risk of products liability related tort claims increases, as the software technology incorporated into automobiles becomes increasingly integrated into safety related functions. Additionally, as the likelihood of driver fault decreases, there will likely be a greater focus on products liability risk allocation throughout the supply chain.

These shifting dynamics in the supply chain might be particularly important given that NHTSA bases some of its liability analysis in its V2V Readiness Report on the OEM's ability to shift the products liability risk to suppliers through contractual risk allocation provisions:

---

243. Richard Viereckl et al., *Connected Car Study 2015*, PRICEWATERHOUSECOOPERS (Sept. 16, 2015), https://www.strategyand.pwc.com/reports/connected-car-2015-study.

244. *Id.*

245. Butzel Long, *OESA North American OEM Production P.O. Terms and Conditions Presentation Handouts*, ORIGINAL EQUIPMENT SUPPLIERS ASSOCIATION, at 116 (Oct. 2014), http://www.oesa.org/Doc-Vault/Presentations/2014/2014-09-18-Presentation-and-Handout.pdf.

246. *Id.*

247. *Id.*

> Under the existing product liability tort law framework, manufacturers have the ability to take steps to limit their legal liability stemming from such on-board systems through a variety of mechanisms (e.g., compliance with applicable safety standards, contractual indemnification by OBE suppliers, dispute resolution/arbitration clauses applicable to supplies and consumers).[248]

The historical methods of risk allocation, such as those employed in supply chain contracts mandated by OEM's may not be available in the new model of industry coordination and technology integration.

B. *The New Transportation Network Will Require Industry Coordination and Technology Integration*

1. Overview of a Connected Vehicle System

In 2014, NHTSA issued its Advanced Notice of Proposed Rulemaking ("ANPRM") concerning V2V connectivity.[249] With the ANPRM, NHTSA published its V2V Readiness Report describing various aspects of a proposed system of connected vehicles.[250] The V2V system would include on-board DSRC devices to transmit Basic Safety Messages ("BSMs") to other vehicles.[251] The Basic Safety Messages would be transmitted up to 10 times per second, and could contain information about a vehicle's speed, heading, brake status, and other data to other vehicles.[252] A vehicle would also receive BSMs from other vehicles.[253] According to NHTSA's research, this connected system would allow cars to gather information about vehicles at a greater distance than existing vehicle resident technologies, such as Lidar, radar, sensors, and cameras. Additionally, V2V technology would allow vehicles to gather information about other vehicles that are outside the vehicles' line-of-sight.[254]

Such a system only works if the messages transmitted to and from vehicles are trustworthy.[255] Accordingly, NHTSA has proposed a system of "security infrastructure to credential each message, as well as a communications

248. V2V Readiness Report, *supra* note 50, at 213.

249. *U.S. Department of Transportation Issues Advanced Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communications*, NHTSA (Aug. 18, 2014), https://www.nhtsa.gov/press-releases/us-department-transportation-issues-advance-notice-proposed-rulemaking-begin.

250. V2V Readiness Report, *supra* note 50.

251. *Id.* at 13.

252. *Id.* at xiv, 13.

253. *Id.* at xiv

254. *Id.*

255. *Id.* at xviii ("In order to function safely, a V2V system needs security and communications infrastructure to enable and ensure the trustworthiness of communication between vehicles. The source of reach message needs to be trusted and message content needs to be protected from outside interference.").

network to get security credentials and related information from vehicles to the entities providing system security (and vice versa)."[256] NHTSA refers to this system as a V2V Security Credential Management System ("SCMS").[257] The SCMS would employ asymmetric public key infrastructure ("PKI").[258] NHTSA envisions that the SCMS functions would be carried out by separate, legally distinct "certificate management entities," including an SCMS "Manager" that together would make up the SCMS organization.[259] The SCMS would use short-term digital certificates that would be used by a vehicle's V2V device to authenticate BSMs that it sends and receives.[260] A valid certificate would purport to ensure that the BSM had been transmitted by a certified device and was unaltered between its transmission and reception. On the other hand, the receiving device would ignore BSMs with invalid certificates.[261]

2. SCMS Management

A critical aspect of the proposed SCMS is that it would be managed by one or more entities, known as the SCMS Manager(s). NHTSA proposes that the SCMS Manager would:

> Provide the policy and technical standards for the entire V2V system. Just as any large-scale industry ensures consistency and standardization of technical specifications, standard operating procedures (SOPs), and other industry-wide practices such as auditing, the SCMS Manager would establish SOPs, including in such areas as interoperability, security, privacy and auditing, and manage the activities required for smooth and expected operation of the SCMS.[262]

While NHTSA has considered a public model and a public-private partnership model, initially NHTSA focused on a private model of SCMS governance.[263] In the private model of SCMS governance, the "certificate management entities" themselves would agree to self-governance by a central SCMS Manager pursuant to binding contracts.[264] NHTSA has anticipated that the OEMs would be heavily involved in SCMS management, explaining:

---

256. *Id.*
257. DOT, VEHICLE-TO-VEHICLE SECURITY CREDENTIAL MGMT SYS.; REQUEST FOR INFO at 1 (Oct. 2014), http://www.safercar.gov/v2v/pdf/V2V-SCMS-RFI-Oct-2014.pdf [hereinafter SCMS RFI].
258. *Id.* at 9.
259. *Id.* at 12-13.
260. *Id.* at 13.
261. *Id.* at 14.
262. *Id.* at 17.
263. V2V READINESS REPORT, *supra* note 50, at 214.
264. *Id.*

> Additionally, the automotive industry seems to have significant incentives to help stand up and operate several elements of the SCMS, as currently designed, including the RA and SCMS Manager. As the only outward facing component of the SCMS, the RA is critical to the ability of individual OEMs to maintain control over its customer relationships. As the entity charged with establishing and enforcing policies and procedures applicable to all CME entities making up the SCMS, the SCMS Manager presumably will promulgate policies directly implicating the financial interests of OEMs and other manufacturers, such as liability distribution and intra-CME fees (i.e., the costs to motor vehicle and device manufacturers of obtaining certificates and certificate-related services (e.g., device type certification and bootstrapping)).[265]

Accordingly, it is possible that the SCMS Manager would be comprised of a joint venture or some other consortium of OEMs or entities involved in the deployment of ACVs.

3. SCMS Participant Liability Risks

Private entities considering involvement in the SCMS are naturally concerned about liability related to SCMS management or operation. Various theories of liability related to connected vehicles are addressed in detail in the Risk Assessment Report (Vehicle Manufacturers) prepared by Dykema Gossett, PLLC on March 12, 2009 ("Dykema Risk Assessment") as part of the Vehicle Infrastructure Integration Consortium ("VIIC").[266] The Dykema Risk Assessment identifies a number of liability avoidance possibilities.[267] These include manufacturer-based defenses such as warnings and instructions, compliance with applicable safety standards, and contractual relief such as indemnification by suppliers.[268] The risk avoidance regimes also include government-related models, such as preemption of common law tort liability, statutorily-granted immunity, indemnification from the federal government, victims' compensation funds, the government contractor defense, and contract specifications defense.[269] The Dykema Risk Assessment concluded by stating:

> OEM liability related to VII OBE arguably can be addressed by existing statutory or common law tort principles. [ ] On the other hand, the interdependencies of OBE with components and systems

265. *Id.*
266. Dykema Gossett PLLC, *Risk Assessment Report (Vehicle Manufacturers): Policy Work Order Task 6, Deliverable* 1 (Mar. 12, 2009).
267. *Id.* at 34-38.
268. *Id.* at 34-38.
269. *Id.* at 38-71.

> external to the accident vehicle and beyond the effective control of the OEM raise issues different, more complex, and potentially less predictable than typically encountered with liability-related failures of vehicle components.[270]

In addressing these concerns about potential manufacturer liability from participating in a connected vehicle system, NHTSA points to several reasons why a manufacturer or other SCMS participants' liability would be limited (or no greater than what they currently experience).[271] However, as discussed in this Report, several of these reasons are mitigated, if not negated, by the rapidly evolving environment of ACVs.

First, the V2V Readiness Report points out that the "V2V technology currently under consideration results in safety warnings – not motor vehicle control." Therefore, the Readiness Report submits that the driver would remain responsible for failing to avoid a crash.[272] As NHTSA itself has recognized, however, the world of ACVs is rapidly changing.[273] Indeed, with the significant advances made in autonomous technology, it is possible that AVs might be deployed in parallel to the deployment of V2V technology. Given the perception that autonomous technologies will shift the liability from the driver to the manufacturer, it is less clear today that "the driver would remain responsible for failing to avoid a crash" in the event the V2V technology failed.[274]

Next, the V2V Readiness Report suggests that in the case of a lawsuit alleging a crash was caused by the communications infrastructure failing, the public or quasi-public entity that deployed the infrastructure would be liable.[275] As discussed in Section V, however, the business model involving the deployment of roadside infrastructure to support V2V or V2I connectivity is far from clear. Given the cost of deploying that infrastructure, it is possible that such infrastructure might not be deployed by public entities. Private entities involved in such infrastructure deployment might seek to mitigate their risk through any contractual relationship they have with SCMS participants.

The V2V Readiness Report also suggests that manufacturers or other SCMS participants can contractually allocate risk to their suppliers or other contractees. As discussed in Section III.A., above, however, it is possible that the automotive supplier contacting model is evolving. It is not clear that OEMs will maintain their historical leverage to allocate product liability risk to suppliers.

---

270. *Id. at* 72.
271. V2V Readiness Report, *supra* note 49, at 212-215.
272. *Id.* at 212-213.
273. 2016 Updated Policy Statement, *supra* note 26.
274. V2V Readiness Report, *supra* note 49, at 212.
275. *Id.* at 213.

The V2V Readiness Report also mentions the possibility that the SCMS Manager could establish minimum insurance requirements or negotiate on behalf of members for system-side insurance. This very well may be the best way to protect against liability in sufficient fashion to encourage manufacturers and others to invest in SCMS participation. However, as discussed in Section III.D., the automotive insurance model is likely to evolve. Additionally, as discussed in Section III.C. on cybersecurity, and Section V on new models of tort liability, the authors believe there are new liability risks facing manufacturers and others involved in deploying ACVs based on the new industry coordination and technology integration. These new risks will certainly be something that any new insurance model will consider in pricing its coverage (or even deciding whether to offer coverage).

4. SCMS Operational Issues

NHTSA's proposed SCMS raises several operational legal issues as well. One issue relates to how an entity with certificate authority can revoke certificates from vehicles. A critical element of any PKI system is that the entity that manages the certificates must be able to revoke certificates and publish a list of revoked certificates to the system. This list enables certified users to know to ignore the revoked certificates.[276]

Similarly, the SCMS system will initially allocate a limited number of certificates to V2V connected vehicles. For example, the vehicles might have 3 years worth of certificates.[277] Because the system only works as long as participating vehicles have valid certificates, it will be critical for vehicles to renew their certificates. Accordingly, the SCMS system must have a way of requiring participating vehicles to renew their certificates. From a technical perspective, vehicles would receive updated certificates through over-the-air updates or through manual distribution of flash or SD memory cards.[278]

Certificate revocation and renewals could be privately enforced, such as through contracts with the OEMs or a service provider. Or, other critical, service updates could be conditioned on the vehicle operator's renewal of certificates. It appears, however, that OEMs or service providers would be concerned with this approach. Consumers with revoked certificates (or in trouble for not renewing their certificates) would direct their anger at the OEMs or service providers. While NHTSA appears to contemplate that certificate revocation would be automatically performed through "machine-to-machine" performance ("[n]o human judgment is involved in creation, granting, or revocation of the digital certificates"),[279] the OEMs or service

276. *Id.* at 163.

277. *Id.* at 248 ("We assume that the initial vehicles will be sold with 3 years of certificates and they will not need updates until the end of year 3.").

278. *Id.* at 115-116.

279. *Id.* at 168.

providers would still be on the front-line of communicating with disgruntled vehicle operators or claims under state "lemon laws."[280]

Accordingly, OEMs would likely desire rules from the federal or state government requiring vehicle operator certificate compliance. However, NHTSA has little authority over individual vehicle operators, as discussed in Section V.B.2. While NHTSA could enforce requirements against OEMs, through its recall authority, the OEMs would be required to pass this requirement on to the vehicle operators contractually. This would subject the OEMs to the costs of enforcement and associated liability.

5. Connected Vehicle Aftermarket Devices

As proposed by NHTSA, FMVSS No. 150 would only apply to new vehicles. Therefore, there would be no requirement that existing vehicles contain in-vehicle V2V devices, such as DSRC units. However, in order to provide significant crash avoidance benefits, a connected vehicle system requires a critical mass of connected vehicles on the road.[281] Accordingly, it is likely that aftermarket onboard V2V devices would play an important role in the deployment of CV technology. Indeed, NHTSA contemplates aftermarket V2V devices in its V2V Readiness Report.[282]

Aftermarket devices may come in varying levels of vehicle integration and effectiveness in providing crash avoidance benefits.[283] In NHTSA's terminology, a "retrofit safety device," one that is connected directly to the vehicle's data bus would provide the greatest functionality.[284] Such a device would likely require a certified installer to install the device and correctly ensure antenna placement and security.[285] Accordingly, aftermarket device manufacturers and their certified installers will need to consider their tort liability, given their participation in the integrated connected vehicle system contemplated by V2V technology. Tort liability for aftermarket providers is addressed in Section IV.B.3.c. below.

---

280. "Lemon laws" generally refer to state laws providing consumers enforcement rights beyond basic warranty claims. *See, e.g.*, *Dieter v. Chrysler Corp.*, 610 N.W.2d 832 (2000) (allowing state lemon law claim for defect when the buyer was aware of defect prior to purchase).

281. Thilo Koslowski, *U.S. Government Must Clarify Its Terms to Boost V2V Technology Adoption*, GARTNER (Feb. 10, 2014) ("V2V communication benefits will not be fully realized for years, until vehicles that can communicate with each other attain critical mass on the roads. This makes a government mandate for automakers' compliance critical. If adoption is widespread, safety benefits will be apparent within eight years; in approximately 15 years, nearly all U.S. vehicles would include V2V technology.").

282. V2V READINESS REPORT, *supra* note 49, at 29-31.

283. *Id.* at 30-31.

284. *Id.* at 31.

285. *Id.*

6. Connected Vehicle System Interoperability

NHTSA has explained that a critical aspect of the SCMS would be interoperability. One aspect of this interoperability is the 75 MHz of wireless spectrum reserved for DSRC communications.[286] Several aspects of DSRC operation are standardized and the DOT has recognized that additional standards will need to be developed to ensure interoperability of equipment.[287] CAMP has been involved in developing some initial standards.[288] NHTSA recognizes that the deployment of V2V connectivity requires the development of standards:

> The V2V devices tested in the Model Deployment were originally developed based on existing communication protocols found in voluntary consensus standards from SAE and IEEE. NHTSA and others participating in the Model Deployment (e.g., its research partners and device suppliers) found that the standards did not contain enough detail and left too much room for interpretation. They therefore developed additional protocols that enabled interoperability between devices participating in the study. The valuable interoperability information learned during the execution of Model Deployment is planned to be included in future versions of voluntary consensus standards that would support a larger, widespread technology roll-out.[289]

This need for interoperability will require substantial industry coordination. In NHTSA's proposed system, this will likely require interaction with the SCMS Manager. In any event, this will likely require significant standard-setting. The tort liability of standard-setting is addressed in Section V below.

C. *The Increasingly High-Tech and Networked Vehicles Will Raise New Cybersecurity Risks.*

Even with current electronic systems, automakers have faced known cybersecurity risks for several years. A 2010 study showed that an attacker who can infiltrate just one of a vehicle's many electronic control units can circumvent safety-critical system and control functions such as disabling

---

286. DOT, STATUS OF THE DEDICATED SHORT-RANGE COMMUNICATIONS TECHNOLOGY AND APPLICATIONS REPORT TO CONGRESS, at 17 (2015) [hereinafter DSRC REPORT].

287. *Id.* at 54-55 ("Additional standards are required to ensure interoperability among various makes and models of devices and communications technologies, and to ensure that messages are of appropriate quality and are trusted and authenticable.").

288. *Id.* at 59 ("CAMP has developed standardized algorithms for detecting bandwidth limiting conditions that may develop in certain traffic congestion conditions, and subsequently implementing mitigation measures such as reducing transmission power and/or transmissions per second.").

289. V2V READINESS REPORT, *supra* note 49, at xv.

brakes, selectively braking individual wheels, and stopping the engine.[290] Bad actors can hack vehicles using existing Bluetooth and cellular connections.[291] The July 2015 hacking of a Jeep Cherokee by researchers Charlie Miller and Chris Valasek brought wide attention to vehicular cybersecurity threats.[292]

While existing technologies expose vehicles to significant cybersecurity risks, the emergence of ACVs appear to provide several new forms of cybersecurity risks. The enabling equipment behind autonomous and connected technologies will provide additional threat vectors for bad actors. AVs will include Lidar, sensor, and camera inputs that could even be manipulated without a bad actor hacking into the car's internal systems.[293] V2I technologies will require a plethora of roadside equipment communicating essential information to onboard equipment through DSRC technology.[294] V2V will require frequent transmissions of Basic Safety Messages between DSRC equipment installed in each connected vehicle.[295]

The following sections lay out the legal framework for cybersecurity enforcement and litigation.

1. Federal Trade Commission Enforcement

The Federal Trade Commission ("FTC") has positioned itself as the nation's primary consumer protection agency. The FTC has been active in po-

290. Karl Koscher et al., *Experimental Security Analysis of a Modern Automobile*, 2010 IEEE SYMPOSIUM ON SECURITY & PRIVACY (2010), http://www.autosec.org/pubs/cars-oakland2010.pdf.

291. *See* Cahen v. Toyota Motor Corp., 147 F.Supp.3d 955, 966 (N.D. Cal. 2015); John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, NY TIMES (Mar. 9, 2011), http://www.nytimes.com/2011/03/10/business/10hack.html; Andy Greenberg, *This Gadget Hacks GM Cars to Locate, Unlock, and Start Them*, WIRED (Jul. 30, 2015, 7:00 AM), http://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/; David Goldman, *Chrysler Recalls 1.4 Million Hackable Cars*, CNN MONEY (Jul. 24, 2015, 4:29 PM), http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/; Xavier Aaronson, *We Drove a Car While It Was Being Hacked*, MOTHERBOARD (May 29, 2014, 1:05 PM), http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked.

292. Bryan Johnson, *Remote Hack on Jeep Demoed on Highway, Senators React with SPY Car Act*, AUTO CONNECTED CAR NEWS (July 22, 2015), http://www.autoconnectedcar.com/2015/07/remote-hack-on-jeep-demoed-on-highway-senators-react-with-spy-car-act/.

293. Jonathan Petit & Steven Shladover, *Potential Cyberattacks on Automated Vehicles*, 16 IEEE TRANSACTIONS ON INTELLIGENT TRANSP. SYS. 546, 551 (2015) (citing GPS spoofing/jamming and machine vision blinding as possible cyber attacks with high feasibility and high probability of success); Alexis C. Madrigal, *When Cars Are as Hackable as Cell Phones*, ATLANTIC (Sep. 8, 2014), http://www.theatlantic.com/technology/archive/2014/09/when-cars-are-as-hackable-as-cell-phones/379734/; Dave Gershgorn, *Hackers Can Trick Driverless Cars With a Handheld Laser*, POPULAR SCI. (Sept. 8, 2015), http://www.popsci.com/hackers-can-trick-lidar-used-in-autonomous-cars-with-laser-pointer (explaining how the ability to manipulate an autonomous car is not limited to sophisticated actors or means because tools as simple as laser pointers may do the trick).

294. V2V READINESS REPORT, *supra* note 49, at 69.

295. *Id.* at 13.

licing data security practices,[296] which it does under Section 5 of the FTC Act, prohibiting "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[297] The FTC prosecutes data security practices under both the "unfairness" and "deceptive" prongs of Section 5.

a. "Unfair" Data Security Practices

The FTC Act provides that an act is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[298] Because the FTC has never promulgated regulations concerning the "unfairness" standard and most FTC actions settle,[299] there is little guidance on what constitutes "unfair" cybersecurity practices. FTC allegations and consent decrees provide some insight by showing that the FTC considers security measures to be unreasonable when they fail to:

- protect data from commonly known attacks when measures to prevent such attacks are inexpensive and publicly available;[300]
- protect against SQL injection attacks;[301]
- utilize unique or robust passwords in securing data;[302]
- limit access to sensitive data;[303]
- have reasonable measures to identify the source of attacks;[304]
- have proper incident response procedures;[305] and
- use readily available security measures such as firewalls.[306]

296. FTC, 2014 PRIVACY AND DATA SECURITY UPDATE (2014), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurity-update_2014.pdf ("the FTC has brought over 50 cases against companies that put consumers' personal data at unreasonable risk").

297. 15 U.S.C. § 45 (2017).

298. *Id.* at §45(n)

299. FTC has settled 53 suits for data security. Jenna Greene, *FTC Stakes Claim As Data Security Cop*, NAT'L L.J. (Jan. 23, 2015), http://www.nationallawjournal.com/id=1202715977568/FTC-Stakes-Claim-As-Data-Security-Cop.

300. *See* Complaint at 3, Guess?, Inc., No. C-4091, FTC No. 022 3260 (Aug. 5, 2003), https://www.ftc.gov/sites/default/files/documents/cases/2003/08/guesscomp.pdf (hereinafter "Guess Complaint") ("The risk of web-based application attacks is commonly known in the information technology industry, as are simple, public available measures to prevent such attacks.").

301. Brian J. Perreault, 1 DATA SEC. & PRIVACY LAW § 8:36 (2016).

302. *Id.*

303. *Id.*

304. FTC v. Wyndham Wordwide Corp., 799 F.3d 236, 241 (3d Cir. 2015).

305. *Id.*

306. *Id.*

Most FTC actions relate to a failure to protect personal information and therefore raise concerns for any entity retaining personal information on a network. Some FTC allegations, however, particularly relate to the possible operation of a system of networked vehicles. First, at least one FTC action involves a failure to adequately secure connected devices. The FTC alleged that TRENDnet violated the "unfairness" prong of Section 5 when a hacker accessed Internet Protocol cameras sold by TRENDnet and was able to access the live feeds from the system.[307] Second, the FTC has alleged that failing to adequately test software, including software provided by third parties, is unfair because of the risk of harm to consumers.[308]

ACV technology providers should also note that the high cost of better security will not, by itself, justify a security failure.[309]

b. "Deceptive" Data Security Practices

The FTC brings Section 5 actions under the "deceptive" prong when a company's practices diverge from the privacy or security policies it disseminates to its customers.[310] While misleading statements in a company's privacy policy serve as the basis of many FTC "deceptive" prong actions[311], statements made in marketing and advertisements can also lead to "deceptive" allegations by the FTC.[312] This might be relevant for ACV technology providers. Given the public awareness of privacy and cybersecurity issues related to these technologies, providers might be tempted to oversell their network security and thus should be careful to ensure alignment between their public statements and actual practices. Recent FTC actions also show that the FTC will find statements deceptive even when made to other businesses, rather than the general public.[313]

---

307. Complaint at 18, TRENDnet, Inc., No. C-4426, FTC No. 122 3090 (Feb. 7, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf (hereinafter "TRENDnet Complaint").

308. Complaint, HTC America, Inc., No. C-4406, FTC No. 122 3049 (July 2, 2013), http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf.

309. FTC Policy Statement on Unfairness, *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm ("[u]njustified consumer injury is the primary focus of the FTC Act" and that such an injury "[b]y itself . . . can be sufficient to warrant a finding of unfairness.").

310. *See* Guess Complaint, *supra* note 301, at 4 (the policy stated that data would be stored in an "unreadable, encrypted format at all times," and a cyber attacker subsequently gained access to data "in clear readable text.").

311. *See, e.g.,* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241 (3d Cir. 2015) (alleging violation of "deceptive" prong of Section 5 based on Wyndham's statements in its privacy policy overstating its actual cybersecurity).

312. Complaint, Henry Schein Practice Solutions, Inc., No. C-__, FTC No. 142 3161 (Jan. 5, 2015), https://www.ftc.gov/system/files/documents/cases/160105scheincmpt.pdf.

313. *Id.*

c. FTC Authority to Police Data Security Practices

Two recent cases have examined the FTC's authority to prosecute cybersecurity cases under Section 5. In the first, the FTC sued Wyndham Worldwide ("Wyndham") in federal court, alleging that Wyndham violated both the "unfair" and "deceptive" prongs of Section 5 after hackers successfully accessed Wyndham's computer systems. Wyndham moved under Rule 12(b)(6) to dismiss the unfair practice alleging the FTC lacked authority to regulate cybersecurity under the unfairness prong. The Third Circuit affirmed the district court's denial of that motion, finding that the FTC did indeed have authority to regulate cybersecurity practices under its unfairness prong.

In the second case, the FTC filed a complaint against LabMD, Inc., a medical testing laboratory, alleging that the company failed to reasonably protect the security of customer's personal data, therefore violating the "unfairness" prong of Section 5. The case was brought before the FTC commission. An administrative law judge recently found that the FTC's complaint failed to state a claim for "unfair" security practices. Specifically, the judge ruled that the FTC had failed to allege conduct that caused or was reasonably likely to cause "substantial injury to consumers" as required by the FTC Act's definition of "unfairness."[314] In particular, the FTC failed to allege that the limited exposure of the data resulted, or was likely to result, in identity theft-related harm. The judge also ruled that the alleged embarrassment or similar emotional harm did not constitute" substantial injury where there was no proof of other tangible injury. The FTC staff has appealed this decision to the Commission.[315]

Even if the LabMD ruling is upheld the FTC likely retains broad authority to enforce cybersecurity related claims. However, it will need to show "substantial injury" to consumers like it did in the Wyndham litigation where it showed the fraudulent transactions due to the stolen credit card information of consumers.

d. FTC Has Indicated It Will Be Focused on Automotive Industry

The FTC has indicated it intends to be highly involved in regulating the cybersecurity aspects of the automotive industry. At the Washington D.C. Auto Show in January 2016, FTC Commissioner Maureen Ohlhausen specifically addressed the need for connected car technology providers to monitor their cybersecurity practices. As explained by the commissioner, "if the company had failed to take reasonable precautions [ ] based on the technology available, the level of threat and the standard of the industry and physical harm would certainly be considered a substantial injury that would meet

314. 16 U.S.C. 45(n) (2017).

315. FTC, LabMD, Inc., (last updated Sept. 29, 2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

the kind of requirements for an enforcement action."[316] Commissioner Terrell McSweeney also recently gave a keynote address at the Connected Cars Conference in Washington D.C., highlighting the importance of cybersecurity issues for connected vehicles.[317]

The FTC has also indicated its focus on cybersecurity issues related to connected vehicles in its comments to NHTSA's proposed rulemaking related to V2V communications.[318] Indeed, the FTC's Bureau of Consumer Protection launched the Office of Technology Research and Investigation (OTRI) to research technology issues involving a variety of new technologies, including "connected cars."[319]

The FTC has expressed several specific concerns about potential steps made by the automotive industry to address cybersecurity. The FTC testified in October 2015 on a discussion draft for the Data Security and Breach Notification Act of 2015, stating several concerns with the draft.[320] First, it criticized the broad safe harbor provisions for vehicle manufacturers.[321] Second, it objected to the omission of hacking exceptions for researchers.[322] Third, it critiqued the proposed Automotive Cybersecurity Advisory Council, designed to establish cybersecurity best practices, because automobile manufacturer representatives would comprise a majority of the council.[323]

Further, multiple vehicle cybersecurity bills were introduced in congress in 2015 which would require NHTSA to consult with the FTC to develop cybersecurity best practices and standards.[324]

---

316. Adam Waks, *Baby You Can Drive My Car*, PRIVACY LAW BLOG (Jan. 26, 2016), http://privacylaw.proskauer.com/2016/01/articles/uncategorized/baby-you-can-drive-my-car/.

317. Terrell McSweeny, *Connected Cars USA 2016, Keynote Remarks of Commissioner Terrell McSweeny*, FTC (Feb. 4, 2016), https://www.ftc.gov/system/files/documents/public_statements/913813/mcsweeny_-_connected_cars_usa_2016_2-4-16.pdf.

318. FTC, Advance Notice of Proposed Rulemaking Regarding Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications Pursuant to Chapter 301 of the Department of Transportation, Motor Vehicles and Driver Programs, FTC No. NHTSA-2014-0022 (Oct. 20, 2014) (comment of the FTC), https://www.ftc.gov/system/files/documents/advocacy_documents/federal-trade-commission-comment-national-highway-traffic-safety-administration-regarding-nhtsa/141020nhtsa-2014-0022.pdf (hereinafter "FTC V2V Comment").

319. Ashkan Soltani, *Booting Up A New Research Office at the FTC*, FTC (Mar. 23, 2015, 11:00 AM), https://www.ftc.gov/news-events/blogs/techftc/2015/03/booting-new-research-office-ftc.

320. FTC, PREPARED STATEMENT ON EXAMINING WAYS TO IMPROVE VEHICLE AND ROADWAY SAFETY 1 (Oct. 21, 2015), https://www.ftc.gov/system/files/documents/public_statements/826551/151021vehiclesafetytestimony.pdf.

321. *Id.* at 4-7.

322. *Id.* at 5-6.

323. *Id.* at 6.

324. Christopher H. Grigorian, *2016 Outlook: NHTSA, Automotive Safety, and Cybersecurity*, DASHBOARD INSIGHTS (Jan. 20, 2016), https://www.autoindustrylawblog.com/2016/01/20/2016-outlook-nhtsa-automotive-safety-and-cybersecurity/ (The Security and Privacy in Your Car Act, or SPY Car Act, introduced in July 2015 in the Senate would require NHTSA, in consultation with the FTC to develop standards that prevent hacking in vehicle control systems and the SPY Car Study Act, introduced in the House in November 2016 would require

In short, the FTC is focused on ACV technologies, and may be heavily involved in regulating the cybersecurity aspects of those systems. However, the recent resignations of two out of five Commissioners leave the future direction of the Commission in some uncertainty.

2. Private Causes of Action Related to Cybersecurity

Providers of ACV technology might also face liability from private actions. It has long been established that the FTCA does not provide a private right of action,[325] so private plaintiffs often seek causes of action under negligence, breach of contract or warranty, fraud, or misrepresentation theories. These cases have typically arisen from loss of privacy due to data breaches, however, manufacturers might also face liability under products liability theories.[326]

Private plaintiffs have struggled in bringing causes of action related to data breach cybersecurity events. In particular, data breach cases brought by private plaintiffs are often barred or limited because the plaintiffs cannot allege an injury-in-fact and therefore lack standing, the economic loss doctrine limits tort claims in many states, contractual limitations of liability imposed by software vendors can limit or cap damages claims, state consumer laws (sometimes called "mini-FTC" acts)[327] are limited to injunctive relief or are interpreted by courts to hold plaintiffs to an extremely high standard, and courts have been hostile to products liability claims against software "services." It is worth questioning whether these limitations will apply in the context of a possible cybersecurity claim related to ACVs, and in particular one that results in property damage or personal injury.

Whereas with a data breach the loss is typically limited to the exposure of personal information, a potential loss in a cyber attack on ACVs could involve economic loss, property damage, or even personal injury. At least one cybersecurity service provider has noted that the "most common near-term consequence of vehicle hacking could be auto theft."[328] A 2015 Wired article explained the ease with which this could be accomplished using a $100 device (although that vulnerability has reportedly been fixed according to an updated version of the article).[329] A cybersecurity breach of a con-

---

NHTSA, in consultation with the FTC and other agencies, to conduct a study to determine appropriate standards for the federal regulation of vehicular cybersecurity.).

325. *See* Holloway v. Bristol-Myers Corporation*,* 485 F.2d 986, 997-98 (D.C. Cir. 1973); Carlson v. Coca-Cola Co., 483 F.2d 279, 280-81 (9th Cir. 1973).

326. *See* U.S. Hotel & Resort Mgmt., Inc. v. Onity, Inc., No. CIV. 13-1499 SRN/FLN, 2014 WL 3748639 (D. Minn. July 30, 2014), *appeal dismissed* (Jan. 27, 2015).

327. *See* Plath v. Schonrock*,* 64 P.3d 984, 989 (S. Ct. Montana Feb. 13, 2003).

328. Jeremy Henly, *Connected Cars: Security Risks on Wheels*, IDEXPERTS (Jan. 4, 2016), https://www2.idexpertscorp.com/blog/single/connected-cars-security-risks-on-wheels.

329. Andy Greenburg, *This Gadget Hacks GM Cars to Locate, Unlock, and Start Them (Updated),* WIRED (July 30, 2015), http://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/.

nected car system could involve a "nightmare scenario"of a hacker taking control of vehicles and causing a crash.[330] A breach could also lead to a hacker having access to a vehicle operator or passenger's personal and other information, such as location and habits, which could lead to burglary or extortion.[331] A commentator from the insurance and technology industry noted that a cybersecurity event involving connected vehicles could lead to injuries including: gaining a commercial advantage through disabling a rival auto-maker's vehicle; industrial espionage or misappropriation of software related intellectual property; harming an operator, passenger, pedestrian, or others on the road; infrastructure damage such as disabling a municipality's fleet of vehicles.[332] The following sections examine some of the historical limitations on private causes of action related to cybersecurity breaches and discusses whether those same limitations would apply in the context of a cyber attack on ACV involving tangible losses.

a. Standing

Many private causes of action relating to the exposure of personal information in cybersecurity breaches fail due to a lack of standing. The Supreme Court in *Clapper* held that speculative harms such as fear of possible government surveillance are insufficient to constitute "injury-in-fact" and therefore lack the requisite standing required for federal court plaintiffs.[333] Following *Clapper*, a majority of federal courts hold that data breach plaintiffs lack standing to sue when they cannot show that their data has been misused.[334] State courts have followed this reasoning, analyzing a standing defense outside the context of Article III.[335]

In the automotive context, the recent case of *Cahen v. Toyota Motor Corporation et al.,* demonstrates courts' application of the standing requirements of Article III to cybersecurity related claims.[336] There, plaintiffs sued Ford Motor Company, General Motors LLC, Toyota Motor Corporation and Toyota Motor Sales, U.S.A., Inc. alleging that they equipped their vehicles with computer technology that was susceptible to third party hacking.[337] The

330. Henly, *supra* note 328.

331. *Id.*

332. Tom Srail, *Connected Cars and Cyber-Security: A Growing Risk,* WILLIS TOWERS WATSON WIRE (October 28, 2015), http://blog.willis.com/2015/10/connected-cars-and-cyber-security-a-growing-risk/.

333. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1141 (2013).

334. *See U.S. Hotel & Resort Mgmt.*, 2014 WL 3748639 at *16 (citing Reilly v. Ceridian Corp., 646 F.3d 38, 43 (3rd Cir. 2011)) ("Most courts have held that such plaintiffs lack standing because the harm is too speculative. We agree with the holdings in those cases.")

335. Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 NO. 1 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 229, 234 (2015).

336. *Cahen*, 147 F.Supp.3d at 961.

337. *Id.* at 958.

court dismissed the complaint finding that plaintiffs lacked standing. In particular, the court ruled that the plaintiffs' allegations that their vehicles were susceptible to future hacking by third parties were too speculative to state injuries-in-fact.[338]

Some cybersecurity breaches involving ACVs may merely involve the loss of personal data, and therefore fall under the facts of the above cases finding a lack of standing. As discussed above, however, with a cyber attack on ACVs it is possible that the victims would suffer economic loss, property damage, or personal injury.[339] Where the injury is actual or even threatened physical injury, economic injury, or property damage, courts regularly find standing.[340] Accordingly, defendants in these cybersecurity cases, where actual economic or physical harm has occurred would likely not benefit from a private plaintiff's lack of standing to sue.

b. Economic Loss Doctrine

Other private causes of action related to cybersecurity breaches have failed due to the economic loss doctrine. The economic loss doctrine generally limits tort claims to those alleging injury to person or property.[341] The *In re Michaels Stores Pin Pad Litigation* plaintiffs alleged that Michaels was negligent and negligent per se because it failed to comply with various PIN pad security requirements.[342] The court dismissed the plaintiffs' tort claims under the economic loss doctrine for failing to allege personal injury or property damage.[343] Courts around the country have followed this reasoning in the context of data breach claims alleging economic loss and no further injuries.[344]

---

338. *Id.* at 961.

339. Quinn Emanuel, *Article: Legal Issues Raised by the Driverless Vehicle Revolution - Part 2*, http://www.quinnemanuel.com/the-firm/news-events/article-january-2016-legal-issues-raised-by-the-driverless-vehicle-revolution-part-2/ (last visited Feb. 24, 2017) ("[There is] little doubt that future lawsuits will include allegations that vehicle manufacturers are to blame for accidents . . . that result from hacking.")

340. City of New York v. Exxon Mobil Corp., 2009 U.S. Dist. LEXIS 59287, at *27–30 (S.D.N.Y. July 6, 2009) (finding standing where wells had been contaminated causing economic injury and where there existed a reasonable threat of future contamination); Cole v. General Motors Corp., 484 F.3d 717, 722–24 (5th Cir. 2007) (finding standing based on allegations that the defendants defectively designed side air bags led to loss in value of the vehicle); In re Zurn Pex Plumbing Prods. Liab. Litig., 644 F.3d 604, 616–617 (8th Cir. 2011) (standing exists even if property damage has not yet occurred but would occur immediately upon use); Carlough v. Amchem Prods., Inc., 834 F.Supp. 1437, 1454 (E.D. Pa. 1993) (standing existed based on actual exposure to toxic substance known to cause physical harm).

341. *In re* Michaels Stores Pin Pad Litig., 830 F. Supp.2d 518, 531 (N.D. Ill. 2011) (finding that the economic loss doctrine barred the plaintiff's tort claims in a data breach case because the plaintiff had not suffered personal or property damage).

342. *Id.* at 528.

343. *Id.* at 531.

344. *E.g.*, Dittman v. UPMC, 2015 WL 4945713 (Pa. Ct. Comm. Pl. May 28, 2015) (dismissing plaintiff's negligence cause of action based on defendant's data breach because of

As discussed above, because an ACV system creates exposures beyond economic loss, there are reasonably likely scenarios where an injured party's claims would not be limited by the economic loss doctrine.

c. Intervening Causes

Professor Michael Scott has explained that even where the economic loss doctrine does not limit negligence claims, there still can be difficulty proving negligence when the harm was caused by an intervening actor, such as a cyber attacker.[345] According to Scott, "[u]nder traditional negligence law, where damage is caused by a third party's criminal act, the potential liability of the negligent party generally is superseded by the criminal conduct unless it is determined to be "highly foreseeable."[346] Mere knowledge of the risk of a cyber attack may not render the attack foreseeable.[347] Scott notes a few reasons why this doctrine might not apply in some cyber attacks. First, Scott notes that the prevalence of websites reporting on security vulnerabilities makes it at least arguable that a software vendor knows, or should know, of both the flaws in its software and the injuries that might arise from a breach of those vulnerabilities.[348] Second, Scott notes that courts will find a duty on the part of a cyber attack negligence defendant unless "special circumstances" exist.[349] However, Scott notes that commentators have suggested that key infrastructure providers might fall under those "special circumstances."[350] Accordingly, participants and providers of a network of ACVs might consider whether they might be found to have a duty to

absence of duty of care concerning cybersecurity); In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498-99 (1st Cir. 2009); Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 175-78 (3d Cir. 2008); Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 455 Mass. 458, 918 N.E.2d 36, 46-47 (2009).

345. Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?,* 67 MD. L. REV. 425, 451-54 (2008).

346. *Id.* (citing Atkins v. Dist. Of Columbia, 526 A.2d 933, 935 (D.C. 1987)).

347. Brian E. Finch & Leslie H. Spiegel, *Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety Act*, 30 SANTA CLARA HIGH TECH L. J. 349, 356 (2014) (citing Order and Opinion Granting United's Motion for Summary Judgment That It Had No Duty for Flight 11, *In re* September 11 Litig., No. 21 MC 101 (AKH) (S.D.N.Y. Nov. 21 2012) (finding that harm from a terrorist attack was not reasonably foreseeable to an airline that assisted in security screening when the terrorists used another airline's planes in the attack and noting New York courts' "caution regarding the extension of liability to defendants for their failure to control the conduct of others in light of the potential for unfairness and potentially limitless liability.").

348. Scott, *supra* note 346, at 451.

349. *Id.* at 452-53.

350. *Id.* at 454 n.176 (citing Randal C. Picker, *Cybersecurity: Of Heterogeneity and Autarky, in The Law and Economics of Cybersecurity* 115, 130 (Mark F. Grady & Francesco Parisi eds., 2006) ("[K]ey infrastructure providers have been held liable even in the face of malicious acts by third parties who might naturally be understood to be the actual source of the harm.").

a party injured in a cyber attack based on the fact that the network might be considered key infrastructure. This is an unsettled area of the law.

d. Contractual Limitations of Liability

Most data breaches involve the breakdown of software-enabled technology. Software is typically distributed under a licensing agreement.[351] These agreements disclaim all warranties and exclude and cap liability.[352] Additionally, because many data breach cases involve consumer-facing software applications, the software license agreements are adhesion contracts.[353] These contractual limitations of liability are rarely negotiated, and courts have little trouble in upholding them.[354] Additionally, the contractual relationship between the software vendor and the customer can preclude the customer from making a tort claim against the vendor.[355] Scott notes that a majority of courts apply this contract preclusion principle to bar a negligence claim where a contract between a buyer and seller exists.[356]

The above contractual limitations on liability might apply to claims related to economic loss or damages related to exposure of personal information. However, as discussed above, the risk exists that a cyber attack on an ACV system could result in tangible losses, such as physical injury or property damage. In most states, courts will not apply contractual limitations of liability to claims for physical injury.[357] As explained in the Restatement (Third) of Torts:

> Disclaimers and limitations of remedies by product sellers or other distributors, waivers by product purchasers, and other similar contractual exculpations, oral or written, do not bar or reduce otherwise valid products-liability claims against sellers or other distributors of new products for harm to persons.[358]

---

351. David Polin, *Proof of Manufacturer's Liability for Defective Software*, 68 AM. JUR. PROOF OF FACTS 3D 333, 342 (2002).

352. Scott, *supra* note 346, at 437-40.

353. Daniel M. White, Note, *The Federal Information Security Management Act of 2002: A Potemkin Village*, 79 FORDHAM L. REV. 369, 372 (2010) ("Software manufacturers traditionally use adhesion contracts, making any remedy rooted in contract law significantly more difficutl to attain.").

354. Scott, *supra* note 346, at 438 ("Courts generally uphold implied warranty disclaimers unless they are found to be unconscionable.")

355. *Id.* at 456-7.

356. *Id.*

357. Polin, *supra* note 352, at 343.

358. RESTATEMENT (THIRD) OF TORTS: PRODUCT LIABILITY § 18 (1998); *see also* AMERICAN LAW OF PRODUCTS LIABILITY 3D § 10.15 (updated Feb. 2017) ("Generally, disclaimers and limitation of remedies by product sellers or other distributors, waivers by product purchasers, and other similar contractual exculpations, oral or written, do not bar or reduce otherwise valid products liability claims against sellers or other distributors of new products for harm to persons.").

Additionally, the contract preclusion rule barring negligence claims when a contract exists has an exception for the situation where the negligent conduct caused physical injury, property damage, or other tangible losses.[359]

It is also worth noting, that in NHTSA's current proposal for a connected vehicle system, it is presuming that participants would "not be required to enter into contracts with the security or communications service provider or other participants."[360]

Additionally, in an integrated connected vehicle system, such as the one proposed by NHTSA, incorporating the SCMS, contracts between providers and managers of that system would involve sophisticated parties who might resist the broad disclaimers and limitations of liability discussed above. These parties might in fact expressly apportion liability related to cyber attacks or require covenants related to cybersecurity performance.[361]

e. Expansion of Products Liability Theories to Software Defects

Most cybersecurity breaches involve products incorporating software. Therefore, causes of action related to cybersecurity breaches occurring due to an alleged shortcoming in a software product or service could be framed in terms of the potential liability of the software provider. As one commentator has recently stated, however, "[t[he law of software liability seems to be strangely undeveloped, considering the size of the software industry and the infiltration of software into virtually every aspect of our lives."[362] Indeed, courts have been historically reluctant to permit a strict products liability theory of recovery against software manufacturers.[363] Recent scholarship, however, has suggested a products liability approach to regulating cybersecurity.[364] Indeed, the American Law Institute's Principles of the Law of Software Contracts imposed a duty on the part of software developers to disclose known defects to customers and prohibit the developer from dis-

359. Scott, *supra* note 346, at 457 (citing Heidtman Steel Prods., Inc. v. Compuware Corp., No. 3:97CV7389, 2000 WL 621144, at *12 (N.D. Ohio Feb. 15, 2000)).

360. V2V Readiness Report, *supra* note 49, at 209.

361. Music Grp. Mac. Commercial Offshore Ltd. v. David Foote, 2015 WL 3882448, *10-11 (N.D. Cal. June 22, 2015) (in post cyber attack lawshit, denying defendant's motion for summary judgement because triable issues of fact existed as to whether terms of agreement required defendant to imiplement cyber security measurs).

362. Polin, supra note 352, at 340.

363. Farhah Abdullah, *Strict Versus Negligence Software Product Liability*, 2 Computer & Info. Sci. 81, 86 (2009).

364. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 Nw. U. L. Rev. 1503, 1533 (2013) (noting that the problem of private investment in cyber-security closely resembles the perspectives of design defect product liability); Scott, *supra* note 346, at 457-59; Kevin R. Pinkney, *Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 Alb. L.J. Sci. & Tech. 43 (2002); White, supra note 354, at 389 ("Commentators believe that many of the barriers strict products liability was designed to overcome are pervasive in the software industry, and this lends support to extending strict products liability to software manufacturers.").

claiming this duty.[365] Accordingly, the reluctance of courts to look at software through a products liability lens may be tenuous.

3. Legislative or Governmental Protections Against Liability

a. Liability Protection Under the SAFETY Act

The Support Anti-Terrorism by Fostering Effective Technologies Act ("SAFETY Act") of 2002[366] might provide liability protection for some ACV technologies. Enacted as part of the Homeland Security Act of 2002, the purpose of the SAFETY Act is to ensure "that the threat of liability does not deter potential manufacturers or sellers of effective anti-terrorism technologies from developing and commercializing technologies that could save lives."[367]

The Act provides liability protection against acts of terrorism for two classifications of products: (1) designated products; and (2) certified products. The Secretary of Homeland Security awards the classifications, and once classified, a product is considered a "Qualified Anti-Terrorism Technology." A "designated" product receives limited liability, a prohibition on joint and several liability, and complete relief from punitive damages.[368] A "certified" product receives the same benefits as a "designated" product and additionally entitles sellers of the product to a rebuttable presumption that the "government contractor defense" covers them. The "government contractor defense" immunizes a seller from design defect claims and failure to warn claims. The presumption may be rebutted with evidence of fraudulent or willful misconduct.[369]

The SAFETY Act would presumably cover many acts of hacking into a network controlling ACVs. The Act's regulations broadly define "act of terrorism" as an act that "(i) is unlawful; (ii) causes harm to a person, property, or entity, in the United States. . . and (iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States."[370] Indeed, the Department of Homeland Security has recently qualified multiple cybersecurity companies.[371]

---

365. Michael L. Rustad, *Torts as Public Wrongs*, 38 PEPP. L. REV. 433, 549 (2001) (citing PRINCIPLES OF THE LAW OF SOFTWARE CONTRACTS § 3.05 (Proposed Final Draft 2009)).

366. 7 U.S.C. §§ 441-444 (2012).

367. *The Office of SAFETY Act Implementation*, DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/science-and-technology/safety-act (last visited Mar. 2, 2017).

368. Regulations Implementing the SAFETY Act, 71 Fed. Reg. 33,147, 33,148 (June 8, 2006) (to be codified at 6 C.F.R. pt. 25).

369. *Id*.

370. *Id.* at 33, 149.

371. Ashley Carman, *FireEye First Cybersecurity Firm Awarded DHS SAFETY Act Certification*, SC MAGAZINE (May 1, 2015), http://www.scmagazine.com/dhs-certifies-fireeye-products-under-safety-act/article/412563/.

Accordingly, the SAFETY Act may provide one of the best protections against cybersecurity liability for entities deploying ACVs or involved in operating a networked system, such as the SCMS.

b. The NIST Cybersecurity Framework

President Obama issued Executive Order 13636 titled "Improving Critical Infrastructure Cybersecurity" on February 12, 2013. The Order seeks to improve the protection of the nation's "critical infrastructure" against mounting "cyber threats." The Order seeks to incentivize and facilitate cybersecurity information sharing between government and private sector entities.[372] Perhaps most importantly, the Order directed the National Institute of Standards and Technology ("NIST") to "lead the development of a framework to reduce cyber risk to critical infrastructure (the "Cybersecurity Framework").

i. Cybersecurity Framework

A year later, NIST released version 1.0 of its Cybersecurity Framework.[373] The Framework is intended to serve as a set of industry standards and best practices that will aid organizations in managing their cybersecurity risks.[374] The Cybersecurity Framework resulted from an extensive public and private sector collaboration, and included voluntary standards borrowed from a variety of existing industry security standards.[375]

ii. Incentives for Adoption of Framework

Although the Framework's suggested actions are voluntary, the Executive Order called for the Department of Homeland Security to perform an "Incentives Study" to explore incentives to encourage private entities to adopt the Cybersecurity Framework.[376] The incentives explored in the Incentives Study include: cybersecurity insurance, grants, process preference for government service programs, liability limitation, streamline regulations, public recognition, rate recovery for price regulated industries, and cyber

372. Exec. Order No. 13636, 78 C.F.R. §11739 (2013).

373. Nat'l Inst. Of Standards & Tech., *NIST Releases Cybersecurity Framework Version 1.*0 (Feb. 12, 2014), https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10.

374. Eric G. Orlinsky, Katherine L. Hickey & David T. Shafer, *Cybersecurity: A Legal Perspective*, 47 Md. B.J. 32, 37 (2014).

375. *Id.*

376. Dep't of Homeland Security, Executive Order 13636: Improving Critical Infrastructure Cybersecurity Incentives Study (2013), https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf;
Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, White House Blog (Aug. 6, 2013), https://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

security research.[377] DHS announced in early 2015 that it believes market forces provide the most effective incentives for industry to adopt the Cybersecurity Framework.[378] To encourage adoption of the Framework, DHS announced it would focus on reducing regulatory burden, further funding cybersecurity research and development, and improving the federal procurement processes in order to encourage cybersecurity investment.[379] DHS has also offered technical assistance through the C3 Voluntary Program US-CERT Gateway.[380]

iii. De facto Standard

While the government has adopted few of the formal incentives discussed in its Incentives Study, it is possible that the Framework could become a *de facto* standard. As noted by a pair of cybersecurity attorneys, in preparing mandatory annual reports, government agencies will make inquiries to private sector entities regarding their degree of Framework adoption.[381] Due to concerns over increased regulatory scrutiny, companies receiving these inquiries might not view Framework adoption as voluntary.[382] These inquiries could be passed on to industry partners and suppliers, thus spreading the incentive for adoption.[383] In the absence of particular industry best practices, companies, and potentially courts, may view the Framework as the minimum standards required for cybersecurity.[384] In fact, counsel for Wyndham cited the Framework in the *FTC v. Wyndham* suit.[385] Commentators have noted that the Framework is being used by cyber insurance companies in informing underwriting and in the finance sector in re-

---

377. EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY INCENTIVES STUDY, at 9; *see also* John W. Burd, *Cybersecurity Developments: Does the NIST "Voluntary" Framework Portend New Requirements for Contractors?*, WILEY REIN NEWS & INSIGHTS NEWSL. (Fall 2013), http://www.wileyrein.com/newsroom-newsletters-item-4789.html.

378. Michael Daniel, *Strengthening Cyber Risk Management*, WHITE HOUSE BLOG (Feb. 2, 2015), https://obamawhitehouse.archives.gov/blog/2015/02/02/strengthening-cyber-risk-management.

379. *Id.*

380. Dep't of Homeland Security, *Using the Cybersecurity Framework*, DHS.GOV (Oct. 14, 2015), https://www.dhs.gov/using-cybersecurity-framework.

381. Kimberly Peretti & Lou Dennig, *Top Ten Things You Should Know About NIST's Preliminary Cybersecurity Framework*, ASS'N OF CORP. COUNS. LEGAL RESOURCES (Jan. 7, 2014), http://www.acc.com/legalresources/publications/topten/ttnistpcf.cfm.

382. *Id.*

383. *Id.*

384. Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 341 (2015)("The NIST Framework could have a particularly significant impact on shaping a reasonable standard of cybersecurity care in common law negligence claims.").

385. Lei Shen, *The NIST Cybersecurity Framework: Overview and Potential Impacts*, 10 THE SCITECH LAWYER 16, 19 (Summer 2014).

sponding to inquiries from counterparties.[386] Additionally, NHTSA has cited the Framework in its work on improving automotive cybersecurity best practices.[387]

4. Joint Liability Cybersecurity Risks

The new model of industry coordination and integrated technology evolving around the deployment of ACVs will likely present new joint liability risks related to cybersecurity. Section IV.E below lays out the framework for joint tort liability generally. This section analyzes a few specific joint liability risks that may arise related to cybersecurity risks. NHTSA has noted the enhanced unique joint liability risks arising from a system of networked ACVs, in citing the position taken by the Vehicle Infrastructure Integration Consortium:

> VIIC's position has been that "the design, development of ultimate deployment of DSRC-based V2X communications systems creates unique risk allocation concerns among the wide range of partisans (both public and private sector)'" and the risk allocation is "further complicated by the introduction of aftermarket devices, the potential for system tampering/hacking, and the risk of unauthorized access to networks and to sensitive data."[388]

Indeed, given the new ways that ACV technology providers will be interacting, and the integrated nature of the ACV technology, it may be difficult for industry participants to entirely shield themselves from cybersecurity liability risks created by others.

a. *Wyndham* Confirms Joint Liability for FTC Section 5 Enforcement

The FTC's enforcement action in the *Wyndham* litigation discussed earlier in Section III.C.1.c is notable for reasons other than the 3rd Circuit's confirmation of the FTC's authority to regulate cybersecurity practices. FTC brought its action against multiple defendants, including Wyndham Worldwide Corporation, Wyndham Hotel Group, LLC, Wyndham Hotels and Resorts, LLC, and Wyndham Hotel Management, Inc.[389] The FTC's complaint alleged that multiple of the defendants had collected and maintained the per-

386. Bruce McConnell, *Update on Implementation of Executive Order 13636: A Year In, How Successful Has it Been in Improving Critical Infrastructure Cybersecurity*, CYBERSECURITY LAW CONFERENCE (2015).

387. *Id.*

388. V2V READINESS REPORT, *supra* note 50, at 209 (citing DOT, *White Paper on Risk Management Issues*, Vehicle Infrastructure Integration Program, VIIC Deployment Analysis and Policy Work Order #4, Task 13 General Policy Support, at 2, (Apr. 18, 2012)).

389. FTC v. Wyndham Worldwide Corp., No. 13-1887, 2014 WL 2812049, at *1 (D.N.J. June 23, 2014).

sonal information of customers.[390] The FTC went on to allege that all defendants engaged in practices that, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[391] Several of the entities moved to dismiss the action arguing that the FTC did not adequately allege direct liability against any of the moving defendants individually and the moving defendants could not be derivatively liable for the actions of a single defendant, Wyndham Hotels and Resorts, LLC.[392]

The district court denied the motion to dismiss, finding that the FTC had sufficiently pled a common enterprise theory of joint liability.[393] In particular, the FTC had alleged that the defendants had shared resources, including office space, performed business functions on each other's behalf, and functioned as an interrelated network of companies having common ownership.[394] Under such a theory, each defendant might be jointly and severally liable.[395]

While the Wyndham entities might have functioned in a more interrelated fashion than would be likely for companies deploying ACV technology, *FTC v. Wyndham* still demonstrates that the FTC is willing to look beyond the actions of a single entity in bringing §5 enforcement actions.

b. Fiduciary Duties Related to Cybersecurity

Additionally, there has also been recent discussion about how fiduciary duties of corporate officers and directors may involve duties related to cybersecurity.[396] Indeed, in the litigation following the Target data breach, a shareholder derivative suit alleges that the company's directors failed "to institute adequate procedures at Target" and therefore committed a "bad faith breach of their fiduciary duties."[397] As previously discussed, entities involved in deploying ACVs might pursue joint ventures, such as in establishing the SCMS management entity.[398] Accordingly, from a corporate law perspective, the participating entities should consider what fiduciary duties

390. *Id.* at *2.
391. *Id.*
392. *Id.* at *1.
393. *Id.* at *8.
394. *Id.* at *6.
395. *Id*. at *23 (citing FTC v. Wash. Data Res., 856 F.Supp.2d 1247, 1272 (M.D. Fla. 2012) ("[A]n act by one entity constitutes an act by each entity comprising the 'common enterprise.'").
396. Shackelford et al., *supra* note 385, at 318 ("In addition to suits for negligence, corporate officers and directors also may have liability stemming from their fiduciary duties to shareholders in the aftermath of a cyber attack.").
397. Davis v. Steinhafel, Nos. 14-cv-00203-PAM-JJK, 14-cv-00261 (PAM/JJK), 14-cv-00266 (PAM/JJK), 14-cv-00551 (PAM/JJK)), 2014 WL 3853976, at ? 140 (D. Minn. July 18, 2014) (consolidated complaint).
398. *See supra* Section III.B.2.

attach to their role in any such venture and how that might expose them to additional cybersecurity risk.

c. Proof Difficulties from Integrated Software

Additionally, even if it is the case that a single entity is directly at fault for a cybersecurity related event involving ACV technology, it might be difficult for other potentially liable parties to prove that another party was the sole cause of the harm. This is because of the highly integrated nature of the technology involved in ACVs. As several parties mentioned to the authors, it is much more difficult, as a matter of proof, to determine fault when the evidence is comprised of lines of code compared to when the evidence involves broken mechanical parts. As NHTSA recognized "[i]t may be difficult to determine who is liable for a V2V system failing to perform as the driver expected, due to the complexity of the system and the number of parties involved."[399] Accordingly, parties involved in deploying ACV technology might incur more joint liability simply due to the difficulty in proving a lack of any liability.

D. *Evolving Insurance Models*

The transition from driver-controlled automobiles to AVs may result in a significant change in how the risks associated with auto-related accidents are insured. The nature and magnitude of the effect will depend on how the frequency, severity, and nature of auto accidents change and how the law adapts to the new technology. The most likely outcome is that premiums for driver liability coverage, as well as first-party health and lost-income coverage (sometimes called Personal Injury Protection or "PIP" coverage), will decline, while the effect on collision and comprehensive coverage is less clear. We may also see products liability premiums charged to AV manufacturers rise. This section addresses these possibilities.

Presently, the bulk of auto-related accident costs for both personal injuries and vehicle repairs are paid for by insurance companies that sell auto-insurance policies directly to vehicle owners, providing collision, comprehensive, and liability coverage. A commonly cited statistic is that 90 percent of auto accidents are the result of driver error, and only 2 percent are the result solely of a defective automobile.[400] One implication of these facts is that, with respect to the vast majority of auto accidents, the loss will be borne by one of the drivers and that driver's auto insurer; those losses will not be shifted to the vehicle manufacturer.

---

399. V2V Readiness Report, *supra* note 49, at 209.

400. Nat'l Highway Traffic Safety Admin., *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey* (Feb. 2015), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115.

In states that have fault-based auto-insurance regimes, some auto-accident losses are shifted through tort suits to the at-fault driver and that driver's insurer, while some of the losses remain with the party who suffered the loss and that party's insurer, depending on the relative fault of the two drivers. In states that have adopted an auto-no-fault regime, by contrast, auto-accident losses are primarily insured through each driver's own first-party insurance coverage in their auto policy (collision, comprehensive, and PIP if they have it), with only a very limited role for state tort law.

In the very small percentage of accidents in which the losses are attributable solely or primarily to a defective vehicle, state tort law—usually state products liability law—can be used to shift the losses from the driver and her first-party auto insurer to the vehicle's manufacturer. If the vehicle manufacturer has no products liability insurance coverage for such losses (but instead self-insures), most of those auto-accident costs will eventually be shifted to and spread over car buyers through increases in auto prices. If, however, the vehicle manufacturer does have products liability insurance coverage for auto-defect claims, some of the auto-accident losses can then be shifted to the manufacturer's insurer. Of course, over time, as auto products liability insurance premiums increase, those costs will be shifted back to auto makers, who will (again) shift most of those costs back to auto consumers through higher auto prices.

That is how the costs of auto accidents are currently insured.[401] As the automobile market moves towards more automated vehicles, the picture may change in a number of ways.

First, many have predicted that the shift to ACVs will dramatically decrease the overall number of auto accidents. That would mean fewer overall claims. Whether such a change would also mean lower overall auto-related repair costs depends on the extent to which the reduction in the number of accidents would be offset potentially by the increase in the magnitude of repair costs per accident. (It seems likely that the cost to repair a crash-damaged ACV is likely to be significantly greater than the cost to repair a non-automated vehicle.) The shift to ACVs, however, should produce a substantial reduction in total personal injury costs associated with auto-accidents, including medical expenses, lost income, and of course lost lives. That shift too can be expected to have an effect on the amount of insurance payouts.

Second, the greater the degree to which cars actually drive themselves, the larger will be the share of auto-accident losses borne by the ACV industry and its insurers as compared with the share that is borne by the auto-

401. Some auto-accident costs, of course, are presently not insured at all, but rest on the party who suffers the loss. This can happen because first-party auto insurance—collision, comprehensive, PIP—in most states is not mandatory; and the amount of liability coverage that is mandatory in most states is often smaller than the amount of the loss.

owners' insurance market, whether through the operation of existing tort law or through any new ACV compensation scheme. The cause of this effect is obvious: to the extent more of the task of driving the vehicle is taken over by the vehicle itself, the number of accidents attributable to human error will decrease. This conclusion does not necessarily imply that there will be more products liability suits overall against auto-industry defendants or that there will be a higher percentage of successful products liability suits. Rather, the point is merely that, relative to the current situation, a greater *percentage* of accidents are likely to be the responsibility of the automotive industry. This is part of what ACV means.

And the products liability landscape would likely be different. For example, to the extent ACVs eventually reach the point of "platooning" on the highways, the ACV industry would face a risk of tort liability for large-scale, multiple-car accidents that is beyond the existing risk of auto product liability claims. This is the sort of risk that liability insurers (and reinsurers) may find difficult to price at least in the short run. In the long run, however, the new products liability risks associated with the shift to ACVs seem entirely insurable, given the size of reinsurance markets and given their ability to handle substantially larger risks. Put differently, there does not seem to be any need for federal or state subsidies for the ACV product liability insurance market, as there are for some other types of risks, such as terrorism risk or earthquake risk.

This conclusion would likely apply even if a completely different type of compensation regime were adopted for ACV-related accidents. Even if the existing patchwork of state tort law regimes were eventually supplanted by a comprehensive compensation regime—analogous to workers' compensation regimes for work-related losses or the National Vaccine Compensation program for vaccine-related losses—such liability risks should be insurable through private markets. After all, employers are able to purchase workers' compensation insurance coverage even though such loss payouts are much larger than any conceivable AV-related payouts; and there is no state or federal workers' compensation reinsurance program.

Perhaps the most difficult aspect of ACV-related crash risks for insurers to price is the possibility of hacker-caused crashes. Such intentionally caused losses, as with terrorism-related risks, are especially difficult for insurers to predict. But another part of the problem is the uncertain nature of the ACV industry's legal responsibility for such losses if they do occur. As discussed in Section III.C.2.c, historically courts in tort cases under current law often decline to hold liable a non-criminal third party for the losses caused by criminals, even if the non-criminal third party could reasonably have foreseen and prevented such losses. The rationale is that, in such cases, the non-criminal third party, even if they were negligent (or even if their product was defective), is not the *cause* of the harm in question; rather, the "superseding"

cause of the harm was the criminal, and only the criminal should be held responsible.

If courts were to apply this line of cases to the cyber-hacker-caused ACV crash scenario, the losses under current law would not be shifted to the ACV industry and therefore would not be shifted to the ACV industry liability insurers. Rather, those losses would remain with the accident victims and with their first-party auto insurers. If, however, courts were to go the other way, holding ACV manufacturers responsible for leaving ACVs vulnerable to such hacking, those risks may in fact get shifted: from ACV owners and accident victims (and their first-party insurers) to ACV makers (and their liability insurers). In any event, the uncertainty as to how such cyber-hacker risk will be allocated may be making it harder for insurers to price both auto first-party coverage and for ACV products liability coverage.

IV. Tort Liability

A. *Products Liability Generally*

One of the issues of greatest concern to parties involved in the production and use of ACVs is how the risks of automobile accidents will be allocated. In Section III.D., we discussed the possibility of various alternative compensation regimes that might be used at some future point, when ACV technology has been fully deployed. For example, it is possible that some combination of auto-manufacturers, auto-parts suppliers, ACV infrastructure suppliers (such as sensor makers), and even software providers may someday all agree contractually to assume responsibility for the costs of all ACV-related accidents. It is also possible that a legal regime will be adopted that will impose such liability, something akin to a workers' compensation regime. Under such a regime, some portion of the ACV accident risks born by the ACV providers might in turn be reallocated through liability insurance contracts to insurance companies, just as workers' compensation risks are now shifted from employers to workers' compensation insurers.

Such a workers-compensation-style liability regime, however, seems unlikely to be adopted anytime soon. Rather, in the short and medium term, the risks of personal injury and property damage from ACV-related accidents will initially be allocated under existing regimes of insurance and tort law. To the extent ACV-related accidents are attributable to defects in the ACVs themselves, in the ACV infrastructure, or the algorithms or software programs that run the ACVs, existing state tort and warranty law will be relevant.

This Section addresses several specific aspects of how state tort law (especially state products liability law) might be applied to losses caused by ACV-related crashes. The types of tort claims that can be brought against automotive defendants (manufacturers, distributors, part suppliers, etc.) generally include negligence claims and product liability claims. Under negli-

gence law, if an automotive defendant breached a duty of reasonable care owed to the plaintiff (that is, the defendant was negligent), and that negligence caused the plaintiff's injuries, the plaintiff can recover from the defendant for those damages. Although plaintiffs can and sometimes do still allege negligence in their suits against automotive defendants, those theories largely overlap with, and in a sense have been supplanted by, product liability theories, which are the focus of the remainder of this Section.[402]

Modern products liability began as a "distinct branch of tort law" with the famous California case of *Greenman v. Yuba Power Products Inc.*, in 1963.[403] That was the first judicial decision adopting the concept of "strict liability" for sellers of "defective products." This concept was soon thereafter adopted by the American Law Institute as Section 402A of the *Restatement (Second) of the Law of Torts*.[404] Today, all but a few jurisdictions have some version of products liability law. As explained further below, some jurisdictions continue to follow the products liability rules as articulated in the *Restatement (Second),* while some follow ALI's more recent articulation in the *Restatement (Third) of Torts: Products Liability*.[405]

Although there is some variation across jurisdictions, in general to establish a products liability claim against an automobile manufacturer (or against any "seller" of an automobile), a plaintiff must establish three elements. First, the plaintiff must prove that the automobile, or some aspect of the automobile, was "defective." A car or some part of the car can be defective with respect to how it is manufactured, how it is designed, and/or whether there are adequate warnings or instructions regarding particular risks. On the "design defect" question, most courts apply a standard that focuses on whether "the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of *a reasonable alternative design*."[406] This design-defect standard is similar to the negligence standard of reasonable care as applied by some courts.

---

402. Products liability has largely supplanted negligence liability in cases against auto manufacturers, part suppliers, etc., in the following sense: In practice, if plaintiffs are not successful on their products liability claims against a defendant, they also typically are not successful on their negligence claims. Moreover, it is rare for a plaintiff to succeed on a negligence theory without also succeeding on a products liability theory. In addition, the judicial opinions in auto maker liability cases focus primarily on the products liability analysis, and when they do discuss negligence law the analysis is almost identical to the products liability analysis. Some auto products liability cases also still involve a breach-of-warranty claim, but those claims also have largely been supplanted by the products liability analysis.

403. John C. Goldberg, Anthony J. Sebok & Benjamin C. Zipursky, TORT LAW: RESPONSIBILITIES AND REDRESS 887 (3d ed. 2012).

404. RESTATEMENT (SECOND) OF TORTS § 402A (1965).

405. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. (2000).

406. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (2000). This test is a version of the "risk-utility" test. Some jurisdictions apply a "consumer expectations" test for determining whether a products design is defective. Other jurisdictions apply a combination of the two approaches.

The second element in a products liability claim against an automobile seller is that the defect in the automobile caused the plaintiff's losses. This showing of causation includes both a showing that the automotive defect was the "but for" cause of the losses (*but for* the defect, the loss would not have happened) and a showing that the defect was the "proximate" cause of the losses (that the harm was a reasonably foreseeable result of the defect). Plaintiffs can attempt to show that the defect caused the accident—the crash—or that it caused the vehicle to be insufficiently "crashworthy," resulting in harms that would not otherwise have happened.

Finally, plaintiffs must prove the nature and extent of the harms they suffered as a result of the automotive defect. Damages that can be recovered include compensatory damages and, in most jurisdictions, punitive damages. Compensatory damages, which are intended to make the victim whole, include economic losses (such as medical expenses, the cost of property repairs or replacement, and lost income) and noneconomic losses (sometimes referred to as "pain and suffering" damages). Punitive damages are awarded, in the jurisdictions in which they are available, only if the plaintiff can prove the existence of aggravating circumstances, such as recklessness or even intentional wrongdoing on the part of the defendant.

Even if the plaintiff is able to establish the preceding elements of a products liability claim against an automotive defendant, the defendant can raise various "affirmative defenses" to liability, including the argument that the driver's negligence contributed to the accident or to the harm that was caused. In most jurisdictions, a showing of driver contributory fault results in a reduction in the damages owed by the automotive defendant. In only a few jurisdictions, such a showing can result in the defendant being excused from liability entirely.

In the context of an ACV crash, depending of course on the law of the particular jurisdiction, a products liability claim might be brought against a variety of potential automotive defendants, including manufacturers, parts suppliers, and potentially to providers of the software or algorithms that run the ACVs.[407] The following sections address several specific products-liability-related questions.

407. The principles underlying tort liability of auto manufacturers and other product sellers would seem to apply equally strongly to the makers of the software that runs ACVs. However, there is very little case law applying tort principles to hold software developers liable in tort for personal physical injury or for damage to physical property. What cases there are tend to involve purely commercial contexts involving only economic harms where courts have been willing to enforce contractual waivers of all liability. Section III.C further analyzes some legal theories concerning software and cybersecurity liability and how they might apply in the context of ACVs.

B. *Component Part Supplier Liability*

1. Background

ACVs, like all automobiles, are made up of a comprehensive, complex network of component parts. Unlike traditional cars, however, ACVs contain certain technologies that depend on specialized components and enable it to drive without real-time input from a human driver. One commentator groups these ACV-specific parts into five categories of technology:

> (1) human-driver interface; (2) sensors that provide data about operation of vehicle and its parts; (3) sensors that provide data about the external roadway environment, including Connected Vehicle or other real-time sources of dynamic data about the area around a vehicle; (4) automated controls over vehicle operations and functions; and (5) artificial intelligence that integrates in-vehicle operational data with external roadway data and uses it to activate automated vehicle controls.[408]

This web of technologies at work in an ACV means there is a web of potential defendants in a lawsuit regarding an ACV's alleged defect. Traditional automotive suppliers like Bosch, Continental, and Magna have been developing, manufacturing, and selling systems that build autonomy into brakes, acceleration, and steering—category (4) above.[409] Tech companies like Velodyne Lidar, Quanergy, and Mobileye compete in category (3), building Lidar sensors and high-tech cameras that allow an AV to "see" its surroundings.[410] Chipmakers such as Qualcomm, Samsung, and Nvidia have moved into the automotive industry to provide AVs with the "brains"—category (5)—to process external and internal data from categories (2) and (3) and decide how and when to activate systems in category (4).[411]

2. General Approaches to Component Supplier Liability

Products liability law has long treated component parts—and the responsibilities of their sellers—as a special subcategory within its broader doctrines. The rationale for such treatment has consistently been that component parts enjoy some or all of these qualities that differentiate them from ordinary consumer products:

---

408. Dorothy J. Glancy, *Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J. L. SCI. & TECH. 619, 634 (2015).

409. Mark Bergen, *Meet the Companies Building Self-Driving Cars for Google and Tesla (and Maybe Apple)*, RECODE (Oct. 27, 2015, 3:30 AM), http://recode.net/2015/10/27/meet-the-companies-building-self-driving-cars-for-google-and-tesla-and-maybe-apple.

410. *See id.*

411. *See id.*

(1) Component parts often do not reach the ultimate consumer in a form substantially unchanged and do not deserve strict products liability treatment;

(2) The component supplier may in fact have sold a duly safe and perfectly merchantable product that only thereafter, by dint of design, formulation, application, warnings or other initiatives taken by others, became a part of a defective end product;

(3) The component seller often has no practical or efficient means of overseeing the use of its product by a large population of buyers, and thus cannot reasonably be expected to foresee all potential risks inhering in various finished products, nor take steps to remedy those flaws;

(4) Even without recourse against the component supplier, the injured party may proceed against the manufacturer of the finished product; and

(5) It is the downstream manufacturer whom we want to encourage to pursue risk reducing manufacturing decisions, and who can most readily and inexpensively detect and remedy avoidable product risks.[412]

Usually, the liability issue turns on whether the injury-causing product's dangerously defective condition can be linked to the component itself or whether the defect results from the manner in which the final product manufacturer integrates the component into the product.[413] In the former case, the supplier of a defective component is subject to liability for harm proximately caused by defects in the components at the time they are sold. This is a largely uncontroversial result that rests on the same principles as products liability writ large.

In the latter case, the component supplier usually is not responsible for harm resulting from the defective final product, and courts will therefore grant summary judgment to the component supplier. To the extent that the supplier actually had control, however, over the design, end-use testing, or manufacture of the final product with respect to the integration of its component part, this rule may not apply.

a. Restatement (Third) of Torts: Product Liability

The American Law Institute (ALI), in Section 5 of the *Restatement (Third) of Torts,* in an effort to summarize the existing common law on this

412. *See* M. Stuart Madden, *Component Parts and Raw Materials Sellers: From the Titanic to the New Restatement*, 26 N. KY. L. REV. 535, 539–40 (1999).

413. *See, e.g.*, White v. ABCO Eng'g Corp., 221 F.3d 293, 303–04 (2d Cir. 2000) (applying N.J. law) (citing Zaza v. Marquess & Nell, Inc., 675 A.2d 620, 629–30 (N.J. 1996)).

issue, directly addresses component supplier liability. That Section states the rule in the following terms:

> One engaged in the business of selling or otherwise distributing product components who sells or distributes a component is subject to liability for harm to persons or property caused by a product into which the component is integrated if: (a) the component is defective in itself, as defined in [Sections 2 and 3 of the Restatement] and the defect causes the harm; or (b) (1) the seller or distributor of the component substantially participates in the integration of the component into the design of the product; and (2) the integration of the component causes the product to be defective, as defined in [Sections 2 and 3 of the *Restatement*]; and (3) the defect in the product causes the harm.[414]

This Section's statement of the rule is consistent with what was "overwhelmingly the law before" across jurisdictions.[415] In the comments to this Section, the ALI Reporters provide the reasoning for this rule, stating that it would be unfair to require a component supplier to scrutinize a product that

---

414. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 5 (2000). Section 2, in turn, defines when a "component is defective in itself":

> A product is defective when, at the time of sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instructions or warnings. A product: (a) contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product; (b) is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe; (c) is defective because of inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe. *Id.* at § 2.

Section 3 provides additionally that a product's defective condition may be inferred without proof of a specific defect if the injury-causing incident "(a) was of a kind that ordinarily occurs as a result of product defect; and (b) was not, in the particular case, solely the result of causes other than the product defect existing at the time of sale or distribution." *Id.* at § 3. Courts and scholars alike often call this rule the "malfunction doctrine." *See, e.g.*, White v. Mazada Motor of Am., Inc., 99 A.3d 1079, 1096, 1100, (Conn. 2014) (Eveleigh, J., dissenting) (arguing that plaintiff introduced sufficient circumstantial evidence to create a genuine issue of material fact under the malfunction doctrine); *see also* Henderson v. Sunbeam Corp., 46 F.3d 1151 (10th Cir. 1995) (applying Oklahoma law) (holding that plaintiff may prove case against product manufacturer with circumstantial evidence without identifying a particular defective component).

415. Hildy Bowbeer, *Component Suppliers: Drawing Common Sense Boundaries For Liability*, 10 KAN. J. L. & PUB. POL'Y 110, 110 (2000).

the supplier had no role in developing, and that it would be inefficient for the supplier to hire its own experts and second-guess the product manufacturer, who almost undoubtedly has more expertise regarding the safe design of its own product. This rationale extends to the duty to warn and instruct as well: the component supplier is under no duty to warn of risks associated with the use of its component where the buyer is sophisticated and integrates it into another product, unless the supplier knows that the component purchaser has a significant lack of expertise and ignorance of those risks.

The two bases for liability articulated in Section 5 of the *Restatement (Third)* make a distinction between defective components (clause (a)) and components that become dangerous only as a result of their integration into the final product (clause (b)). As noted above, liability for components defective in and of themselves is a self-evident application of basic products liability principles.

As to liability based on clause (b), comment *e* offers additional guidance as to possible situations implicating the "substantial participation" rule. The easy cases are where the component supplier jointly participates in the design of the final product designs (on its own) a component especially for use in the integrated product, or assists in modifying the component or modifying the integrated product to accept the component. In those cases, the component supplier is shares in liability with the manufacturer. Other less obvious scenarios possibly implicating this basis for liability are where the component supplier offers substantial participation to the assembler-manufacturer in selecting the correct component for use in the product—based on the manufacturer's general purpose for the part and request for help in development or selection of an appropriate part—or any other situation involving more than the manufacturer providing specifications for the part to meet. In any case of "substantial participation," of course, liability depends additionally on whether the integration causes the plaintiff's injury.

b. Restatement (Second) of Torts

In specifically addressing the products liability principles affecting component part suppliers, the *Restatement (Third)* explicitly filled a void left by the ALI's articulation of products liability in *Restatement (Second).* Because courts for decades framed their analysis of component supplier liability against it, however, it is useful to consider Section 402A of *Restatement (Second) of Torts*, which provides as follows:

> (1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if (a) the seller is engaged in the business of selling such a product, and (b) it is expected

> to and does reach the user or consumer without substantial change in the condition in which it is sold.
>
> (2) The rule stated in Subsection (1) applies although (a) the seller has exercised all possible care in the preparation and sale of his product, and (b) the user or consumer has not bought the product from or entered into any contractual relation with the seller.[416]

The reporters of Section 402A also added three caveats, the third of which expressly disclaims taking any position as to whether component part sellers should be subject to its rule.

The comments to Section 402A clarify several additional points worth noting. First, the rule extends beyond products for intimate bodily use and applies to more complex machinery, including automobiles.[417] Second, under the rule of Section 402A the seller of a product is not liable if he delivers the product in a safe condition; in order to recover, plaintiff has the burden to prove that the defect existed at the time that it left the seller's hands.[418] Some jurisdictions have accepted the bulk of the rule of Section 402A, only omitting the phrase "unreasonably dangerous" because it confusingly introduces language sounding in negligence into a strict liability determination.[419]

This rule—by focusing on the moment when the component supplier transfers control of its part to the assembler-manufacturer—precludes recovery in the case where the component is not inherently defective, even if the finished product is defective as a result of the component's integration into the whole.

c. The *Verge* Test

In addition to rules prescribed in the Restatements, another influential approach to component supplier products liability has developed out of a case, *Verge v. Ford Motor Co.*[420] In that case, Ford manufactured a truck chassis that was subsequently modified by Leach and made into a garbage truck. Plaintiff was injured when the truck backed into him and sued both Ford and Leach, claiming that the absence of a back-up alarm rendered the truck defective.[421] The Third Circuit ruled in part as follows:

> Where . . . the finished product is the result of substantial work by more than one party, we must determine responsibility for the ab-

416. RESTATEMENT (SECOND) OF TORTS § 402A (1965).
417. *Id.* at § 402A cmt. d.
418. *Id.* at § 402A cmt. g.
419. Union Supply Co. v. Pust, 583 P.2d 276, 282 n.5 (Colo. 1978).
420. Verge v. Ford Motor Co., 581 F.2d 384 (3d Cir. 1978).
421. *Id.* at 385–86.

> sence of a safety device by looking primarily to at least three factors:
>
> 1. Trade Custom—at what stage is that device generally installed. . . .
> 2. Relative expertise—which party is best acquainted with the design problems and safety techniques in question. . . .
> 3. Practicality—at which stage is installation of device most feasible. . . .[422]

The court absolved Ford from liability on the grounds that it was not feasible for Ford to install a back-up alarm in a multi-use product, where such an alarm was not required for all uses, and where Leach had more expertise than Ford in producing garbage trucks.[423]

The *Verge* test gained traction with other courts, being applied in cases that largely involved similar circumstances, where one company manufactures an unfinished product (like a cab-and-chassis) and the other finishes it (like with whatever truck outfitting suits its business).[424] A number of commentators likewise favor the *Verge* test because its factors of trade custom, expertise, and practicality relate to both of tort laws goals: efficiency and fairness.[425]

The *Verge* test may be especially relevant in the context of ACVs, depending on the manufacturing arrangement. If one manufacturer—say, a traditional automaker—supplies an unfinished vehicle to another—say, a tech company—who outfits the vehicle with ACV technology and other finishing touches, then application of the Verge test may make perfect sense. Of course, the two manufacturers may allocate the risk of liability *ex ante* via an indemnification agreement.

3. Applying the Rules to Three Specific Factual Contexts

a. "Design to Spec"

Manufacturers of component parts made to the final product maker's specifications are liable for injuries caused by the final product only if the

422. *Id.* at 386–87 (citations omitted).

423. *Id.* at 388–89.

424. Cross v. Cummins Engine Co., 993 F.2d 112 (5th Cir. 1993) (applying Tennessee law); Pietluck v. Danella Companies, Inc., Prod. Liab. Rep. (CCH) ¶13572, 1993 WL 57194 (E.D. Pa. 1993) (applying Pennsylvania law); Richter v. ITW Ransburg Electrostatic Sys. Grp., No. 03-6083, 2005 WL 1214610, at *3–4 (D. Minn. May 20, 2005) (applying Minnesota law); Mayberry v. Akron Rubber Mach. Corp., 483 F. Supp. 407, 412–13 (N.D. Okla. 1979) (applying Oklahoma law); Williams v. Gen. Motors Corp., No. E-83-48, 1984 WL 7838, at *3 (Ohio Ct. App. Apr. 13, 1984); Ford v. Int'l Harvester Co., 430 So. 2d 912 (Fla. Ct. App. 1983); Elliott v. Century Chevrolet Co., 597 S.W.2d 563 (Tex. Ct. App. 1980); Mott v. Callahan AMS Mach. Co., 416 A.2d 57, 60–61 (N.J. Ct. App. 1980).

425. *See, e.g.*, David A. Fischer, *Product Liability: A Commentary on the Liability of Suppliers of Component Parts and Raw Materials*, 53 S.C. L. Rev. 1137, 1146–47 (2002).

component part was defective when it left the supplier's control or if the specifications obviously showed that the part would become dangerous when integrated into the final product, such that it would not be reasonable for the defendant to follow the specifications.[426] In other words, the component supplier will be liable (for defective design, failure to warn, or negligence) if it has actual knowledge that the final product design is excessively dangerous with respect to its integration of the component part.[427]

Of course, for suppliers to take advantage of this rule, components that are "designed to spec" must actually be "to spec." That is, a component may itself become unreasonably dangerous solely by virtue of its non-compliance with design specifications.[428] Heightened design specifications can therefore place a component supplier on notice that ordinary quality will not suffice.[429] On the other hand, a component supplier may be considered involved in the design of the component system when it writes the system specification or is actively involved in the specification's development.[430]

In the automotive context, the typical arrangement is that vehicle manufacturers—called "original equipment manufacturers" (OEMs)—for competitive reasons, compartmentalize the design and manufacture tasks of various component part suppliers such that the suppliers know only enough

426. Crossfield v. Quality Control Equip., 1 F.3d 701, 704 (8th Cir. 1993) (applying Missouri law); Carey v. Hy-Temp Mfg., Inc., 929 F.2d 1229, 1234 (7th Cir. 1991) (applying Illinois law); Childress v. Gresen, Inc., 888 F.2d 45, 49 (6th Cir. 1989) (applying Michigan law); Koonce v. Quaker Safety Prods. & Mfg., 798 F.2d 700, 715 (5th Cir. 1986) (applying Texas law); Spangler v. Kranco, Inc., 481 F.2d 373, 375 (4th Cir. 1973) (applying Virginia law); Littlehale v. E. I. du Pont, etc. & Co., 268 F. Supp. 791, 802 n. 16, (S.D.N.Y. 1966) (applying New York law), aff'd 380 F.2d 274 (2d Cir. 1967); Searls v. Doe, 505 N.E.2d 287, 290 (Ohio Ct. App. 1986); Munger v. Heider Mfg. Corp., 456 N.Y.S.2d 271, 273 (Sup. Ct. 1982).

427. *See* Orion Ins. Co., Ltd. v. United Technologies Corp., 502 F. Supp. 173, 176 (E.D. Pa. 1980) (applying Pennsylvania law); *see also* Zager v. Johnson Controls, 18 N.E.3d 533, 541 (Ohio Ct. App. 2014) (finding no liability on part of automotive component manufacturer where defect alleged related to cargo retention of rear seatback, and component supplier did not participate in design of cargo retention system; vehicle manufacturer could have delegated such task to component manufacturer but did not). At least one jurisdiction, however, applies this rule for component parts designed to purchaser specifications only to claims based on theories of negligence; for claims under a theory of strict liability, a non-designing manufacturer can still be held liable for design defects it did not cause. See Hendricks v. Comerio Ercole, 763 F.Supp. 505, 512–13 (D. Kan. 1991) (applying Kansas law) (citing Lenherr v. NRM Corp., 504 F.Supp. 165 (D. Kan. 1980)).

428. *See* Thorndike v. DaimlerChrysler Corp., No. 00-198-B, 2003 WL 21212591, at *5 n.8 (D. Me. May 21, 2003), *report and recommendation adopted*, 288 F. Supp. 2d 50 (D. Me. 2003) (applying Maine law); cf. Fink v. Chrysler Motors Corp., Inc., 308 N.E.2d 838, 841 (Ill. Ct. App. 1974) (holding that a question of fact was properly presented to the jury as to whether defendant's failure to meet *its own* design specifications constituted a defective condition).

429. *See* Thorndike, 2003 WL 21212591, at *5 n.8.

430. LEWIS BASS & THOMAS PARKER REDICK, PRODUCTS LIABILITY: DESIGN AND MANUFACTURING DEFECTS § 2:29 (2015).

information to complete those tasks.[431] According to vehicle seat design expert William Tighe, "All car companies reserve all the safety decision making, all the safety methods to themselves. It's too important and can only be done at the vehicle level."[432]

In some jurisdictions, the specific nature of a component part is enough to preclude the application of the component parts doctrine, which is reserved for "generic" or "off-the-shelf" parts.[433] Component parts that are designed to the buyer's specifications are likely to always be non-generic, designed as a "separate product with a specific purpose and use."[434] In those situations, so the reasoning goes, the component supplier has sufficient knowledge of the suitability of the application and the risks associated with integrating the component according to the final product manufacturer's design. On the other hand, other jurisdictions apply the component parts doctrine even in the design-to-spec cases, following the *Restatement (Third)* rule requiring either a defect in the component itself or substantial participation of the component supplier in the final product's design.[435]

b. Supplier's Design

Cases in which an automotive supplier has designed on its own a component part for integration into a vehicle's final design are virtually unheard-of. As described in Section IV.B.3.a above, OEMs typically make safety design decisions and enlist component suppliers to produce parts that meet the specifications in accordance with that overall design. This makes sense, given (i) the law's tendency to hold the party responsible for manufacturing the final product liable when an end-user is injured by the product and (ii) the difficulty of isolating a specific component as being the sole proximate cause of injury. In most instances where the component supplier and the designer are identical—such as where Ford designs the engine blocks and cylinder heads to be used in its vehicles—there is no separation of supplier

431. *See* Zager, 18 N.E.3d at 543.

432. *Id.* In *Romans v. Texas Instruments*, No. CA2013-04-012, 2013 WL 6094299 (Ohio Ct. App. 2013), the court upheld summary judgment granted to the supplier of a speed control deactivation switch (SCDS) where the OEM made integration decisions—to keep SCDS powered on, orientation of it, and brake system vacuum—and where the plaintiff presented no evidence creating a genuine issue of material fact as to whether SCDS could ignite on its own. The CEO of Delphi Automotive, the supplier to General Motors of the defective ignition switch that caused at least 13 deaths, employed a similar defense in his testimony in front of Congress. Ben Klayman, *Delphi CEO Says the Bad Ignition Switch Was GM's Responsibility*, REUTERS (Jul. 17, 2014), http://www.reuters.com/article/2014/07/17/us-gm-recall-delphi-idUSKBN0FM1OS20140717 ("GM knowingly approved a final design that included less torque than the original target. . . . In our view, that approval established the final specification").

433. California is one such jurisdiction. *See* Romine v. Johnson Controls, Inc., 169 Cal Rptr. 3d 208, 221–22 (Ct. App. 2014); Tellez-Cordova v. Campbell-Hausfeld/Scott Fetzger Co., 28 Cal Rptr. 3d 744, 747 (Ct. App. 2004).

434. *Id.*

435. *See, e.g.*, *supra* note 428.

and OEM liability, making this Section IV.B.3.b largely moot. For discussion of component supplier's liability to the extent of its participation in the integration of its part into the final product or in the setting of design specifications, see Section IV.B.3.a above.

It is worth noting also that strict liability is not extended to the provider of pure services (e.g., an engineering firm who simply designs a product) unless a product is also supplied in the course of the transaction.[436] This is a simple application of the principle that in order to be liable in products liability, a defendant must actually place the defective product into the stream of commerce.[437]

c. Aftermarket Parts

Aftermarket parts that modify or replace those initially supplied at the time of the product's purchase present an interesting case in the broader scheme of component supplier liability. Unfortunately, however, the case law in which those more general liability principles are applied to aftermarket suppliers is scant. The reason for the limited case law on aftermarket part makers is that defendants in these cases are more likely than OEMs to be judgment proof. This could be true despite the fact that they presumably have liability insurance coverage for such claims.

One thing the case law is certain about: the manufacturer of a final product is generally not liable for damages caused by defective component parts added to a vehicle subsequent to distribution.[438]

---

436. *See* Abdul-Warith v. Arthur G. McKee & Co., 488 F. Supp. 306 (E.D. Pa. 1980), aff'd, 642 F.2d 440 (3d Cir. 1981); *Romine*, 169 Cal. Rptr. 3d at 222–23.

437. To the extent that a product designer breaches its duty of care to, say, follow professional standards in designing the product, such a defendant might be found liable for negligence. *See* Romine, 169 Cal. Rptr. 3d at 223.

438. Braswell v. Cincinnati, Inc., 731 F.3d 1081, 1091–92 (10th Cir. 2013) (applying Oklahoma law) ("[A]n otherwise safe product is not made unreasonably dangerous if the manufacturer fails to prevent the replacement of a part with a substandard aftermarket part."); Westchem Agric. Chemicals, Inc. v. Ford Motor Co., 990 F.2d 426, 430 (8th Cir. 1993) (applying North Dakota law) (holding that OEM has no duty to design to protect against or warn against harm resulting from improperly installed aftermarket equipment); Baughman v. Gen. Motors Corp., 780 F.2d 1131, 1133 (4th Cir. 1986) (applying South Carolina law) ("While a manufacturer can be fairly charged with testing and warning of dangers associated with components it decides to incorporate into its own product, it cannot be charged with testing and warning against any of a myriad of replacement parts supplied by any number of manufacturers."); Gonzalez v. Thomas Built Buses, Inc., 934 F. Supp. 2d 747, 754–56 (M.D. Pa. 2013) (applying Pennsylvania law) (holding that issues of substantial change and foreseeability—such that facts amounted to superseding cause—were questions for the jury where mechanic attempted to repair broken electrical terminal with an aftermarket part); Braaten v. Saberhagen Holdings, 198 P.3d 493, 495–500 (Wash. 2008) (holding that manufacturer had no duty to warn about danger of asbestos-containing replacement parts manufactured by third party); Cousineau v. Ford Motor Co., 363 N.W.2d 721, 727–28 (Mich. Ct. App. 1985) (holding that manufacturer could not be held liable for damages caused by defective component parts added to a vehicle subsequent to distribution).

There is far less case law implicating the actual manufacturer of the aftermarket parts, even in those cases cited above where the OEM is being sued for failure to warn against dangerous replacement parts. For example, in *Baughman v. General Motors*, a tire mechanic injured by an exploding aftermarket replacement wheel rim assembly brought a products liability action against the vehicle manufacturer—not the aftermarket part maker.[439] The Fourth Circuit affirmed the district court's grant of summary judgment on the ground that the defendant did not design, manufacture, or place the wheel rim into the stream of commerce.[440] With respect to the claim that the defendant failed to warn of the dangers associated with that type of wheel rim, the court noted in dictum: "The duty to warn must properly fall upon the manufacturer of the replacement component part."[441]

For the assertion just quoted, the *Baughman* court cited to *Spencer v. Ford Motor Co.*, a case based on similar facts.[442] There, however, the injured tire mechanic sued the replacement component manufacturer (Firestone) in addition to the OEM (Ford).[443] As to Firestone, the plaintiff alleged only that it had a duty to warn of the danger of the multi-piece tire rim.[444] In reversing the trial court's denial of Firestone's motion for summary judgment, the Michigan Court of Appeals found that there was no evidence of a causal connection between Firestone's failure to warn and plaintiff's injury.[445] Rather, plaintiff testified that he knew of the danger and would not have altered his behavior in working on the wheel rim assembly, such that Firestone's warning would not have made a difference.[446]

While these cases do not comprehensively analyze the liability principles affecting aftermarket component manufacturers, they do indicate that such manufacturers generally receive treatment similar to that of OEMs. Downstream manufacturers do not integrate aftermarket components into the final assembly before the product reaches the consumer—otherwise the parts wouldn't be "aftermarket." Rather, they are sold to and installed by third-party vehicle specialists[447] or consumers themselves. On the other hand, if the component supplier doctrine—that manufacturers of generic, off-the-shelf components are shielded from liability, at least in some jurisdic-

439. *Baughman*, 780 F.2d at 1131.
440. *Id.* at 1133.
441. *Id.*
442. 368 N.W.2d 393, 395 (Mich. Ct. App. 1985)
443. *Id.* at 393.
444. *Id.* at 396.
445. *Id.*
446. *Id.*; *see also* Lake v. Firestone Tire & Rubber Co., 936 F.2d 573 (6th Cir. 1991) (applying Michigan law) (holding, on similar facts, that defendant Firestone could not be held liable for failure to warn where plaintiff tire mechanic was aware of the dangers of the replacement wheel rim, and that Firestone could not be held liable for defective design where plaintiff presented no evidence of the reasonableness of an alternative design).
447. See cases cited supra Section IV.B.3.c.

tions[448]—applies to aftermarket parts that are compatible for integration into a wide range of finished products, then aftermarket suppliers need not have the same liability concerns as an OEM.

Recognizing the importance of third-party installation specialists as gatekeepers to protect consumers from harm, the law imposes products liability on such parties just as it does on manufacturers. That principle is espoused in the *Restatement (Second)* as follows: "One who as an independent contractor negligently makes, rebuilds, or repairs a chattel for another is subject to the same liability as that imposed upon negligent manufacturers of chattels."[449] Case law supports that proposition.[450]

C. *Liability of Standard-Setting Organizations*

1. Introduction to Standard-Setting Organizations

Less obvious defendants in an automotive product liability lawsuit than the respective manufacturers of the vehicle and its allegedly defective component parts are private standard setting organizations (SSOs). The private sector develops standards for products, materials, systems, and practices that fall into three broad categories: (1) "proprietary standards," developed by a single firm for its own products; (2) "consensus standards," arising out of a consensus shaped by the impact of market forces, the passage of time, and the participation of a wide variety of interested parties; and (3) "industry standards," created by trade associations and standards development organizations for their members.[451] This section focuses on the liability arising from the latter category, but recognizes that the lines between the groups are not always clear: many consensus standards begin as proprietary or industry standards, and industry standards may enjoy near-consensus levels of stakeholder approval.

Courts and commentators have identified a number of benefits provided by standard-setting organizations, including the following: (i) they lower search costs, decreasing information asymmetry and easing entry into the industry, which in turn fosters competition; (ii) they facilitate the interchangeability of parts (especially replacement parts); (iii) they help market participants identify possible goals the product can serve; (iv) they can elim-

448. *See supra* section IV.B.3.a.

449. RESTATEMENT (SECOND) OF TORTS § 404 (1965).

450. *See* Hoyt v. Wood/Chuck Chipper Corp., 651 So.2d 1344, 1349–50 (La. Ct. App. 1995) (holding that installer of aftermarket modification that rendered product unreasonably dangerous could be held liable where installer's employee knew that the modification was unsafe); *but see* Winans v. Rockwell Int'l Co., 705 F.2d 1449, 1453 (5th Cir. 1983) (applying Louisiana law) (holding that repairer must exercise reasonable care, but that strict liability does not apply to such defendant).

451. *See* Robert W. Hamilton, *The Role of Nongovernmental Standards in the Development of Mandatory Federal Standards Affecting Safety or Health*, 56 TEX. L. REV. 1329, 1336–37 (1978).

inate the need for more burdensome governmental regulation; (v) they facilitate benchmarking, by which superior-performing industry participants are studied and mimicked, thereby increasing competitors' efficiency; (vi) they sponsor industry-wide educational activities; (vii) they assist the industry in marketing and public relations; and (ix) they maintain governmental relations.[452] SSOs serve a particularly important role in the fields of communications and information technology, where networking and interoperability are essential to the commercialization of new innovations.[453]

Despite their detachment from the actual development and manufacture of specific products on the market, SSOs do have potential tort liability for injuries caused by products subject to their standards and certifications. The remainder of this section outlines the contours of legal framework of that potential liability.

2. Negligence

The most successful theory used by injured consumers to seek recovery from SSOs is some form of negligence: negligent misrepresentation, negligent testing or inspection of the product, negligent promulgation of standards, or negligent failure to warn. Negligence liability of an SSO derives most commonly from one of the Restatements or the voluntary rescue doctrine.

Sections of both the *Restatement (Second) of Torts* and the *Restatement (Third) of Torts: Liability for Physical or Emotional Harm*—324A and 43, respectively—provide that one who undertakes to render to another a service is reasonably expected to protect a third party. One has a duty of reasonable care to the third party if (a) the failure to exercise reasonable care *increases the risk* of harm, (b) the actor has undertaken to *perform a duty* owed by the other to the third party, or (c) the beneficiary of the services, the third party, or another *relies* on the actor's exercise of reasonable care in the undertaking.[454]

---

452. *See* Meyers v. Donnatacci, 531 A.2d 398, 404 (N.J. Super. Ct. Law Div. 1987); STANDARDS AND CERTIFICATION, 43 Fed. Reg. 57269 (proposed Dec. 7, 1978) (to be codified at 16 C.F.R. pt. 457); Robert H. Heidt, *Damned for Their Judgment: The Tort Liability of Standards Development Organizations*, 45 WAKE FOREST L. REV. 1227, 1228 (2010).

453. *Id.* at 1229 (citing Jonathan L. Rubin, *Patents, Antitrust, and Rivalry in Standard-Setting*, 38 RUTGERS L. J. 509, 509 (2007); David J. Teece, *Information Sharing, Innovation, and Antitrust*, 62 ANTITRUST L. J. 465, 477–78 (1994)).

454. The black-letter language of the two Restatements is largely identical. Section 324A of the Second Restatement provides:

> One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of a third person or his things, is subject to liability to the third person for physical harm resulting from his failure to exercise reasonable care to protect his undertaking, if
>
> (a) his failure to exercise reasonable care increases the risk of such harm, or
>
> (b) he has undertaken to perform a duty owed by the other to the third person, or

It is important to note that these two Restatement versions of the same "good Samaritan"[455] rule pertain only to the existence of the SSO's duty of care to plaintiffs. As we will see below, the element of proximate causation can be difficult for plaintiffs to prove in these cases.[456] If a finding that the SSO has a duty takes place at an earlier stage in the litigation than the ultimate determination of causation and thus liability, however, that finding might increase the likelihood of the defendant offering a more favorable settlement.

To the extent that a court interprets an SSO's promulgation or suggestion of product standards as an undertaking to render services to a product designer or manufacturer, it may find a duty owed to the ultimate consumers under any one of the three bases in the Restatements, depending on the facts. Officially sanctioned specifications that turn out to cause harm could be viewed in hindsight to have increased the risk of harm pursuant to (a), while the performance of testing or product safety research normally conducted by the manufacturer will constitute the undertaking of a duty pursuant to (b). Subsection (c), however, becomes an especially fertile ground for possible imposition of a duty in light of comment e to Section 43, which provides that the provision of services "may create an appearance of safety," while the manner in which the reliance causes harm and the identity of the person relying on the SSO's undertaking are wholly irrelevant.[457]

(c) the harm is suffered because of reliance of the other or the third person upon the undertaking.

RESTATEMENT (SECOND) OF TORTS § 324A (1965). The Third Restatement left the substance of this provision unmodified, changing only its wording:

> An actor who undertakes to render services to another and who knows or should know that the services will reduce the risk of physical harm to which a third person is exposed has a duty of reasonable care to the third person in conducting the undertaking if:
>
> (a) the failure to exercise reasonable care increases the risk of harm beyond that which existed without the undertaking,
>
> (b) the actor has undertaken to perform a duty owed by the other to the third person, or
>
> (c) the person to whom the services are rendered, the third party, or another relies on the actor's exercising reasonable care in the undertaking.

RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM § 43 (2012).

455. Sizemore v. Georgia-Pacific Corp., Nos. 6:94–2894 3, 6:94–2895 3, 6:94–2896 3, 1996 WL 498410, at *6 (D.S.C. Mar. 8, 1996).

456. *But see* Meneely v. S.R. Smith, Inc., 5 P.3d 49, 58–59 (Wash. Ct. App. 2000) (holding that the jury's finding of proximate cause was supported by evidence and reasonable inferences therefrom where the SSO both formulated a safety standard that permitted the product specifications under which the injury arose and did not warn consumers when its research revealed a risk of injury years before).

457. RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM § 43 cmt. e (2012).

One prominent example of an SSO being found liable for injuries caused by a product conforming to its promulgated standards is the National Spa and Pool Institute (NSPI). The NSPI was a private, nonprofit trade association and SSO that developed suggested minimum standards for pools, through consensus surveys of its members and other methods.[458] In some cases, courts granted NSPI summary judgment, refusing to find that a duty of care arose out of the mere development of standards for pool construction and design. In *Howard v. Poseidon Pools, Inc.*, 506 N.Y.S.2d 523, 527–28 (Sup. Ct. 1986), the court based its dismissal on the lack of duty or authority of NSPI to control the product manufacturers. In *Meyers v. Donnatacci*, 531 A.2d 398, 404, 406–07 (N.J. Super. Ct. Law Div. 1987), the court conducted analysis under each of the subsections of Section 324A, finding that (a) NSPI did not increase the inherent risk of diving head-first into shallow water, but at most permitted its continuation; (b) NSPI had no authority, nor made any effort, to mandate compliance with its standards; and (c) to the extent that the manufacturer and installer relied on NSPI to promulgate safety standards, such reliance was unjustified, because the manufacturer and installer knew such standards were voluntary and pertained only to the construction and design (and not the ownership, use, or maintenance) of the swimming pool.

Other courts, however, found that, under different circumstances, NSPI's conduct constituted an undertaking that created a duty of care owed to users of swimming pools complying with its standards. In *King v. Nat'l Spa & Pool Inst., Inc.*, 570 So. 2d 612 (Ala. 1990), the Alabama Supreme Court considered these prior decisions from other jurisdictions and found that the lack of control over manufacturers or the voluntary nature of the standards does not absolve the SSO of a duty of care.[459] Rather, the court—in overturning the lower court's grant of summary judgment—held that NSPI assumed a duty to the consumer, stating in relevant part:

> The trade association's voluntary undertaking to promulgate minimum safety design standards for safe diving from diving boards installed in residential swimming pools (such standards being based on studies of the "needs of the consumer" and founded on a consideration of "safety" involved in the design and construction of such swimming pools) and to disseminate those standards to its members for the purpose of influencing their design and construction practices, made it foreseeable that harm might result to the consumer if it did not exercise due care.[460]

458. Heidt, *supra* note 452, at 1227.
459. *King*, 570 So. 2d at 617.
460. *Id.* at 616.

The court distinguished *Meyers* on the basis that the plaintiff in that case alleged that NSPI was negligent in failing to prevent pool users from diving from the side of the pool into shallow water, whereas the plaintiff in *King* alleged that NSPI was negligent in the very promulgation of design and construction standards relating to diving boards.[461] The reporters of *Restatement (Third)* notably cited *King* favorably in the reporters' notes to comments c, e, and h of Section 43, which indicates that the Alabama Supreme Court's decision is not an aberration.[462]

Ten years after *King*, and on similar facts, the Washington Court of Appeals upheld a jury verdict against NSPI for negligence in suggesting standards and upheld the damages award of $11 million against multiple defendants, $6.6 million of which was assessed against NSPI.[463] The court noted that "the foreseeability of the harm" was the keystone of the determination of whether NSPI had a duty under the voluntary rescue doctrine or Section 324A.[464] Importantly, the court based its holding in large part on the fact that NSPI had ignored and failed to warn consumers of a report, which it had commissioned, indicating that construction of the pool and diving board combination under NSPI standards was unsafe.[465] The judgment ultimately drove NSPI into bankruptcy.[466]

In addition to purely private SSOs like NSPI, quasi-governmental organizations also face potential tort liability for their development of standards. Most prominently, recipients of blood transfusions of HIV-contaminated blood sued the American Association of Blood Banks (AABB), claiming that AABB was negligent in setting standards for screening blood donors and thus liable for the plaintiffs' HIV infections.[467] In most of these cases, the courts imposed a duty on AABB, rejecting any claim of a qualified privilege stemming from its quasi-governmental nature, and affirmed the judgments against it.[468]

---

461. *Id.*

462. RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM § 43 reporters' notes to cmts. c, e, h (2012).

463. Meneely v. S.R. Smith, Inc., 5 P.3d 49, 60 (Wash. Ct. App. 2000).

464. *Id.* at 57.

465. *Id.* at 60 n.5.

466. Heidt, *supra* note 453, at 1231 n.15.

467. In some cases, plaintiffs claimed AABB's negligence was in failing to adopt a standard calling on blood banks to surrogate test blood donors. *E.g.*, Snyder v. Am. Ass'n of Blood Banks, 676 A.2d 1036, 1038 (N.J. 1996). In other cases, the plaintiffs' theory of negligence was based on AABB's alleged failure to impose a standard that would call on blood banks to offer directed donations to transfusion patients or its alleged failure to impose a standard that would call on blood banks to undertake direct questioning of donors. *E.g.*, N.N.V. v. Am. Ass'n of Blood Banks, 89 Cal. Rptr. 2d 885, 889, 893 (Ct. App. 2000).

468. *See, e.g.*, Douglass v. Alton Ochsner Med. Found., 696 So. 2d 136, 140 (La. Ct. App. 1997) (reversing summary judgment in favor of AABB); Snyder, 676 A.2d at 1055 (affirming a jury verdict against AABB for a plaintiff transfused with HIV-infected blood); Weigand v. Univ. Hosp. of N.Y. Univ. Med. Ctr., 659 N.Y.S.2d 395, 400 (Sup. Ct. 1997)

The court in one of the prominent AABB cases adopted four required criteria by which "considerations of fairness and policy" could converge to impose a duty when the defendant was a professional association lacking privity or some special relationship to the plaintiff.[469] First, the harm posed by the defendant's conduct must be reasonably foreseeable. Second, the defendant SSO's influence within the industry must be so dominant that the industry participants have little discretion in choosing whether to join or to adopt its standards. Third, the association must actively seek to become the arbiter of its industry's standards. Finally, the association must have a financial interest in maintaining its position as the arbiter of its industry's standards.[470]

Even though SSOs generally aim their standards primarily at product designers and manufacturers, they often offer them to the public at large. This broad dissemination of standards creates an unlimited pool of people who might "rely" on the standards for purposes of subsection (c) of Section 324A or Section 43. The reporters of the *Third Restatement* apparently recognized the fear of open-ended or insufficiently limited liability—a fear no doubt induced when standard developers are at risk of being liable to any injured user of a complying product. Comment b to Section 43 reads, "Even though an affirmative duty might exist pursuant to this Section, a court may decide, based on special problems of principle or policy, that no duty or a duty other than reasonable care exists." Indeed, some courts have declined to impose a duty on an SSO, citing this fear of overwhelming tort liability.[471]

(imposing a duty on the AABB to a plaintiff transfused with HIV-infected blood); *cf.* Doe v. Am. Nat'l Red Cross, 848 F. Supp. 1228, 1234 (S.D. W. Va. 1994) (finding that a reasonable jury could find the American Red Cross dilatory in its standards relating to blood transfusions); United Blood Servs., Div. of Blood Sys., Inc., v. Quintana, 827 P.2d 509, 525 (Colo. 1992) (en banc) (observing that blood-banking standards were insufficient and that blood center's compliance was "not conclusive proof" of reasonable care); Gilmore v. Mem'l Sloan Kettering Cancer Ctr., 607 N.Y.S.2d 546, 550 (Sup. Ct. 1993) (same); Doe v. Univ. Hosp. of the N.Y. Univ. Med. Ctr., 561 N.Y.S.2d 326, 328 (Sup. Ct. 1990) (imposing a duty on a hospital to a plaintiff transfused with HIV-infected blood). *But see* Hoemke v. N.Y. Blood Ctr., 912 F.2d 550, 551 (2d Cir. 1990) (affirming summary judgment for a hospital in a suit by a plaintiff transfused with HIV-infected blood); N.N.V., 89 Cal. Rptr. 2d at 889, 909 (finding no duty imposed on AABB to a plaintiff transfused with HIV-infected blood); Osborn v. Irwin Mem'l Blood Bank, 7 Cal. Rptr. 2d 101, 104 (Ct. App. 1992) (finding a blood bank not negligent for failing to screen blood donors adequately when the court observed that the blood bank was "doing as much if not more in the areas of testing and screening than any other blood bank in the country.").

469. *See* Snyder, 676 A.2d at 1048–49, 1053.

470. *Id.* at 1052.

471. *See, e.g.*, Commerce & Indus. Ins. Co. v. Grinnell Corp., Nos. 97–803, 97–775, 1999 WL 508357, at *3 (E.D. La. July 15, 1999) ("Here policy considerations weigh against holding the [National Fire Protection Association], a voluntary membership association, liable . . . . Promoting public safety by developing safety standards is an important, imperfect, and evolving process. The imposition of liability on a nonprofit, standards developer who exercises no control over the voluntary implementation of its standards . . . could expose the

It is important to distinguish the promulgation of standards from the certification of a particular unit or model design. (IAPMO in, e.g., *FNS Mortgage*; *Hanberry v. Hearst*). A certifier's approval of an existing specimen is not subject to the same fear of unlimited liability, is more likely to cause the designer or manufacturer to discontinue its own safety efforts, and establishes a clearer and closer relationship between the injured product user and the defendant certifier.[472] Though courts in these cases often similarly ground their decisions on Section 324A or Section 43, they are more likely to find that certifiers' owe a duty to product users than they are to find that standards developers do.[473]

In sum, a SSO that does not manufacture or design products may be held liable for injuries caused by products subject to its standards only if the court finds a legal duty under Section 324A, Section 43, or the voluntary rescue doctrine. That finding of duty, in turn, seems to depend mainly on two factors distilled from case law: the foreseeability of the risk of harm, and the connection between the SSO and the designer or manufacturers (including the SSO's control over the designer's or manufacturer's actions vis-à-vis the standards, and the procedure or input used in developing the standards). Those factors go to the heart of whether the SSO performed a duty normally performed by the designer or manufacturer (pursuant to subsection (b) of Section 324A or Section 43) and whether the designer, manufacturer, or consumer (justifiably) relied on the SSO's undertaking to develop standards. The more foreseeable the harm, or the more closely the SSO and the designer or manufacturer are connected, the more likely the SSO will be liable in tort for negligence.

3. Strict Products Liability

SSOs are, as a general rule, not liable to plaintiffs injured by defective products under the theory of strict product liability. Courts, nearly universally, have held that such a theory is not available to consumers seeking recovery from a party who expresses approval of a product on the ground

association to overwhelming tort liability to parties with whom its relationship is nonexistent and could hinder the advancement of public safety").

472. *Heidt*, *supra* note 453, at 1253.

473. *Id.*; Hempstead v. Gen. Fire Extinguisher Corp., 269 F. Supp. 109, 117–18 (D. Del. 1967) (imposing liability on a testing company that approved a particular model of fire extinguisher that exploded and injured the plaintiff); FNS Mortg. Serv. Corp. v. Pac. Gen. Grp., Inc., 29 Cal. Rptr. 916, 921-23, 24 Cal.App.4th. 1564, 1572-73 (1994) (imposing a duty on the International Association of Plumbing Mechanical Officials because it certified that certain injury-causing piping complied with its Uniform Plumbing Code); *see also* Hanberry v. Hearst Corp., 81 Cal. Rptr. 519, 521–24 (Ct. App. 1969) (imposing a duty on Good Housekeeping Magazine because it placed its "Consumers' Guaranty Seal" on a pair of shoes that caused plaintiff's injury); *see also* Toman v. Underwriters Labs., Inc., 707 F.2d 620, 620–21 (1st Cir. 1983) (discussing the liability of Underwriters Laboratories when it certified the particular product injuring the plaintiff).

that such a party is not involved in the manufacturing or supplying process.[474]

4. Breach of Warranty

As with strict products liability claims, claims based on a theory of breach of warranty may be brought only against parties responsible for placing the product into the stream of commerce.[475] Most courts accordingly dismiss claims for breach of warranty against SSOs or other parties who express approval of a product on the ground that such a party is not directly involved in manufacturing or supplying the allegedly defective product.[476]

Unlike claims based on a theory of strict products liability, breach of warranty claims arise out of contract. In some states, therefore, privity of contract between the consumer and the seller of the product remains a prerequisite to recovery under a theory of breach of warranty.[477] Since SSOs do not enter into contractual relationships with consumers of the products meeting their standards, they cannot be liable for breach of warranty in those jurisdictions.[478]

---

474. *See, e.g.*, Swartzbauer v. Lead Industries Ass'n, Inc., 794 F.Supp. 142, 144 (E.D. Pa. 1992) (applying RESTATEMENT (SECOND) OF TORTS §402A pursuant to Pennsylvania law) (holding that a trade association cannot be held liable for harm caused by an allegedly defective product because it is not a seller or supplier); Harmon v. Nat'l Automotive Parts Ass'n, 720 F.Supp. 79 (N.D. Miss. 1989) (APPLYING RESTATEMENT (SECOND) OF TORTS §402A pursuant to Mississippi law) (holding that strict products liability could not be extended to a trade association, which allegedly endorsed the product by licensing its trade name to the manufacturer, but did not manufacture, market, test, inspect, distribute, or warehouse products); Howard v. Poseidon Pools, 506 N.Y.S.2d 523, 526-27 (Sup. Ct. 1986) (holding that strict liability could not be extended to the manufacturer-hired trade association that certified the product, where the trade association placed into the stream of commerce only publications, which did not cause the plaintiff's injury). *See also* 2 OWEN & DAVIS ON PROD. LIAB. § 16:31 (4th ed.); AM. L. PROD. LIAB. 3D § 5:40.

475. *E.g.*, Perez v. Brown & Williamson Tobacco Corp., 967 F.Supp. 920, 929 (S.D. Tex. 1997) (applying Texas law) (holding that only actual sellers are liable for breach of warranty, even where another party has promoted a product and made promises regarding it).

476. *See, e.g.*, Klein v. Council of Chemical Ass'ns, 587 F.Supp. 213 (E.D. Pa. 1984) (applying Pennsylvania law) (holding that a worker injured by long-term exposure to unidentified chemicals in his workplace could not bring a breach of warranty claim against a trade association or an industry research institute because neither one placed any chemical product into the stream of commerce).

477. AM. L. PROD. LIAB. 3d § 21:1 (providing an overview of the body of law arising from the UCC provision that maintains a requirement of privity of contract between seller and injured party).

478. *See, e.g.*, Albin v. Illinois Crop Improvement Ass'n, 174 N.E.2d 697, 699 (Ill. App. Ct. 1961) (applying Illinois law) (holding that no action for breach of express or implied warranty could be maintained against an organization that issues product certifications to the manufacturer but makes no representation to the plaintiff), *rev'd on other grounds by* Rozny v. Marnul, 250 N.E.2d 656 (1969).

5. Tort Liability of SSOs: In the Automotive Industry

The automotive industry, like many manufacturing industries, features plenty of SSOs that develop standards for designers and manufacturers to follow in their production of vehicles and their component parts. At the time of this writing, however, the case law on SSO liability includes only one example of an SSO as a defendant in a lawsuit stemming from injury-causing automotive product. (Perhaps SSOs are likely to be sued or impleaded only where the product maker has relatively "shallow pockets," which is less common in the auto industry than in, say, the swimming pool industry.)

In the relevant case—*Beasock v. Dioguardi Enterprises, Inc.*[479] — the plaintiff sought relief from the Tire and Rim Association (TRA) after her husband died as a result of injuries sustained in an explosion after attempting to inflate a 16-inch truck tire mistakenly mounted on a 16.5-inch rim.[480] TRA's primary function was to disseminate dimensional standards within the automotive industry so as to allow interchangeability among the various manufacturers tires and rims.[481] The court found that because the relationship between TRA and any manufacturer was insufficient to afford TRA control over the design or manufacture of any tires or rims, TRA had neither a duty to control the production of tires so as to conform to its standards, nor a duty to warn product users of the dangers associated with their use.[482]

Though the *Beasock* court did not cite the Restatement, Sections 324A and 43 remain relevant to the analysis of the tort liability of automotive SSOs. With respect to subsection (a), it is highly unlikely that a court would find the mere promulgation of standards to increase the risk of an injury-causing car accident that exists without such standards. Subsection (b) has relevance in the automotive context only to the extent that an SSO performs the manufacturer's duties to warn and design a reasonably safe product, and an SSO generally does not design or manufacture vehicles or component parts on a carmaker's behalf.

Most relevant is subsection (c) pertaining to reliance. As comment e to Section 43 notes, a duty of care may attach if the SSO's conduct "may create an appearance of safety or make alternative arrangements appear unnecessary," regardless of the manner in which the reliance causes harm or of the identity of the person relying.[483] In fact, as described below, some SSOs may be created for the very purpose of allowing manufacturers (and, by extension, their consumers) to rely on the standards as a marker of a product's proper performance.

---

479. Beasock v. Dioguardi Enterprises, Inc., 494 N.Y.S.2d 974 (Sup. Ct. 1985).
480. *Id.* at 975.
481. *Id.* at 976.
482. *Id.* at 979.
483. RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM § 43 cmt. e (2012).

6. Possible SSOs for the ACV Industry

In the specific context of the production and deployment of ACVs, some SSOs in particular might find themselves exposed to tort liability under the principles expressed earlier in this section. The three identified below are not intended to be an exhaustive list, and this memorandum leaves unresolved the viability of such SSOs as "deep pockets" defendants in a hypothetical ACV product liability lawsuit.

SAE International, initially established in 1904 as the Society of Automotive Engineers, coordinates the development of technical standards based on best practices identified and described by SAE committees and task forces.[484] SAE publishes recommended standards for nearly all aspects of motor vehicle design, including self-driving features like blind spot monitoring systems.[485] Notably, however, SAE grants membership to individuals and maintains no affiliations with individual manufacturers or manufacturer groups. No known product liability lawsuit has implicated SAE throughout its 112 years of operation.

Consumer Electronics for Automotive (CE4A) is a working group of car manufacturers—Audi, BMW, Daimler, Porsche, and VW—that promotes an active standardization of mobile device interfaces.[486] CE4A is organized into six expert groups and coordinates common activities through steering committees.[487] Unlike SAE, CE4A is comprised of several large automakers and has a close affiliation with others. To the authors' knowledge, CE4A has not been subject to any U.S. litigation since its inception in 2007.

The Automotive Electronics Council (AEC) was originally established by Chrysler, Ford, and General Motors for the purpose of setting common part-qualification and quality system standards.[488] The Component Technical Committee is AEC's standardization body, and any components meeting its specifications "are suitable for use in the harsh automotive environment without additional component-level qualification testing."[489] AEC's members include many of the world's top auto suppliers, including Denso, Magna, Continental, Lear, TRW, and Delphi.[490] To date, AEC has not been a defendant in any product liability litigation. Its own admission that manufacturers and others can rely on the suitability of products meeting its standards,

---

484. *See About SAE International*, SAE Int'l, http://www.sae.org/about/board/vision.htm (last visited Feb. 25, 2017).

485. *See* SAE Safety & Hum. Factors Standards Steering Comm., *SAE Standards J 2802* (June 4, 2015), http://standards.sae.org/j2802_201506.

486. Consumer Electronics for Automotive, https://ce4a.de (last visited Feb. 25, 2017).

487. *Id.*

488. Automotive Electronics Council, http://www.aecouncil.com (last visited Feb. 25, 2017).

489. *Id.*

490. *Id.*

however, would seem to implicate application of subsection (c) of the Restatements Sections 324A and 43.

D. *Product Liability Implications of Automated Warning Devices*

One necessary feature of all ACVs that fall short of complete (Level-4) autonomous driving capability is an automated warning system and interface that prompt the operator to take (or retake) control of the vehicle. The adequacy of the automated warning device and the user's interaction with it are issues that will likely arise in product liability litigation stemming from an ACV crash. This section addresses the law that would govern in such a scenario.

1. The Duty to Warn and the Effect of User's Failure to Heed Warnings

No matter how well a product is designed and manufactured, it may nevertheless cause injury due to dangers not immediately evident to the user. A product seller therefore has a general duty to warn users of the product's hazards. The seller will be found liable for failure to warn or instruct if (1) reasonably foreseeable use of the product creates an unreasonable risk of harm, (2) either the likelihood of the harm or its severity should it occur is not apparent to the user, *and* (3) the product carries inadequate warnings of the risk or instructions on how to use the product in a duly safe manner.[491] The inquiry in warning defect cases is more limited than in design defect cases, focusing on the foreseeability of the risk and the adequacy and effectiveness of any warning given.[492]

Two primary policy justifications underpin the duty to warn: (1) risk reduction and reduction of avoidable accident costs, and (2) informed consent.[493] The first rationale relates to tort law's broader goal of efficiency; the product seller is presumably in the best position to identify the risks associated with using the product and take steps to avoid those risks at the lowest relative cost. The second rationale relates to the goal of fairness, reflecting the notion that a consumer is entitled to make his own choice as to whether the product's benefits are worth the underlying risks, and to do so must have adequate basis for evaluating those benefits and risks.

---

491. 1 OWEN & DAVIS ON PROD. LIAB. § 9:1 (4th ed.); *see* RESTATEMENT (SECOND) OF TORTS § 388 (1965) ("One who supplies directly or through a third person a chattel for another to use is subject to liability to those whom the supplier should expect to use the chattel with the consent of the other or to be endangered by its probable use, for physical harm caused by the use of the chattel in the manner for which and by a person for whose use it is supplied, if the supplier (a) knows or has reason to know that the chattel is or is likely to be dangerous for the use for which it is supplied, and (b) has no reason to believe that those for whose use the chattel is supplied will realize its dangerous condition, and (c) fails to exercise reasonable care to inform them of its dangerous condition or of the facts which make it likely to be dangerous").

492. Liriano v. Hobart Corp., 700 N.E.2d 303, 306 (N.Y. 1998).

493. 1 OWEN & DAVIS ON PROD. LIAB. § 9:1 (4th ed.).

A plaintiff's failure to heed a seller's warnings of dangers or instructions on safe use is a form of "misuse"[494] that normally bars a product liability claim where (1) the danger of failing to comply with the warning is evident, (2) the noncompliance causes the injury, and (3) there is no simple way or apparent reason for the manufacturer to design the danger out of the product.[495] Statutes and case law alike protect the seller by generally presuming that product users will read and follow its warnings and instructions and barring recovery where the plaintiff disregarded such admonitions.[496] Most courts, however, because of the foreseeability that users will disregard warnings, hold that manufacturers have an independent duty to design away a product's dangers, if doing so would be reasonable.[497] To benefit from the liability shield of misuse, however, the seller's warning must itself be adequate.[498]

2. The Effect of User's Disabling of Warning Device

Given the relative rarity of automated warning devices in the history of product design, cases involving a determination of whether a user's disabling of such device constitutes misuse are likewise rare. The few cases that have arisen, however, provide some basis for reasoning by analogy. For example, a driver who disables his ACV's warning of upcoming danger, or who fails to react properly to the that warning, can be analogized to the situation of the aircraft pilot. In *McLennan v. American Eurocopter Corp.*, 245 F.3d 403 (5th Cir. 2001), a helicopter crashed after running out of fuel. The pilot sued the helicopter manufacturer, alleging that the fuel gauge had malfunctioned, failing to warn the pilot that the fuel was almost exhausted, and that the manufacturer had failed to warn that the fuel gauge might be inaccurate.[499] However, the Fifth Circuit held that, because the evidence revealed that the pilot had disregarded the many warnings that the manufacturer and helicopter had in fact provided, there was no proof he would have

494. *See infra* notes misuse is also a defense to claims of design defect, as illustrated in the case discussed.

495. 2 OWEN & DAVIS ON PROD. LIAB. §13:25 (4th ed.).

496. *See* RESTATEMENT (SECOND) OF TORTS § 402A cmt. j (1965) ("Where warning is given, the seller may reasonably assume that it will be read and heeded; and a product bearing such a warning, which is safe for use if it is followed, is not in a defective condition, nor is it unreasonably dangerous"); *see, e.g.*, MICH. COMP. LAWS §§ 600.2945(e), 600.2947(2) (defining misuse to include uses contrary to warnings and instructions and providing immunity for unforeseeable misuse); *See, e.g.,* Alsip v. Louisville Ladder, Inc., No. L-09-1987, 2010 WL 2560031, at *2 (D. Md. June 21, 2010) ("Misuse includes a failure to heed a manufacturer's warning").

497. 2 OWEN & DAVIS ON PROD. LIAB. §13:25 (4th ed.).

498. *See, e.g.*, Harless v. Boyle-Midway Division, Am. Home Prods., 594 F.2d 1051, 1055 (5th Cir. 1979) (applying Florida law) ("It seems both confusing and internally inconsistent to ask a jury who has previously concluded that the label was *inadequate* to consider the defense of failure to read an *adequate* label") (emphasis in original).

499. *Id.* at 413–14.

heeded any additional warnings.[500] The court concluded the causal connection was too remote.

In *American Eurocopter Corp. v. CJ Systems Aviation Group*, 407 S.W.3d 274 (Tex. Ct. App. 2013), a helicopter crashed after the main rotor gearbox failed. During one flight, the oil-pressure warning light for the gearbox illuminated, but the oil-temperature warning light did not.[501] The pilot landed the helicopter safely. The on-duty mechanic found no evidence of an oil leak or unusual behavior of the main rotor and—after partial troubleshooting—concluded, along with the pilot, that the problem was a faulty oil-pressure switch and not low oil pressure.[502] After deciding to fly the helicopter back to its origin to complete the troubleshooting steps suggested in the manufacturer-issued manual, the pilot asked the mechanic to leave the oil-*pressure* warning light disconnected so he would not be distracted from seeing the oil-*temperature* warning light if it came on.[503] During the return flight, the main rotor gearbox suffered a catastrophic failure, the helicopter crashed, and the pilot was killed.[504] As it turned out, the gearbox had failed airworthiness tests, but the manufacturer had certified it for installation.[505] A jury implicitly found that the disabling of the warning light did not cause the crash, and that the actions in making the second flight were foreseeable in light of the manual's troubleshooting guidance and the reasonable judgment of the pilot and mechanic regarding the aircraft's airworthiness; the appeals court held that such a determination was not so contrary to the evidence as to be clearly wrong and unjust.[506] One wonders whether the outcome would have been the same had it not been for the "bad fact" of the manufacturer's certification of airworthiness in the face of failed tests.

Two other cases involving different factual or legal circumstances also merit review. The first is failure to warn case in the industrial machine context. In *Besser Co. v. Hansen*, 415 S.E.2d 138 (Va. 1992), the plaintiff suffered crushing injuries when he stepped between two electrically powered transfer cars to uncouple the racks of cement blocks they were towing. Plaintiff had failed to disconnect the power to the cars before stepping between them, disregarding warning lights indicating the car was still in automatic mode; as a result, he was pinned between a rack and the steel pressure chamber that was its ultimate destination.[507] The court found that the car manufacturer "had no reason to know or foresee that an operator would put himself

500. *Id.* at 433–34.
501. *Am. Eurocopter*, 407 S.W.3d at 278.
502. *Id.* at 279.
503. *Id.*
504. *Id.*
505. *Id.*
506. *Id.* at 286.
507. *Besser*, 415 S.E.2d at 141–42.

in the path of the racks without seeing that he had the switch turned to 'off.' "[508] Moreover, the defendant manufacturer had no reason "to know or foresee that an operator would not realize that danger and heed the warnings on the panel."[509]

The second implicates a product design's accommodation of natural human reactions. In *McAdams v. Pak-Mor Mfg. Co.*, 602 S.W.2d 374 (Tex. Ct. App. 1980), the plaintiff's hand was injured when it was caught between the loading door and the moving compactor blade of a garbage truck. The plaintiff brought design defect claims against the manufacturer of the garbage truck, alleging the compactor was unreasonably dangerous without a hydraulic or interlocking system whereby the door would be closed before the compactor blade passing the pinch point.[510] The jury found that the truck was defectively designed, but that the plaintiff voluntarily assumed the risk of injury.[511] The court held that the latter finding was against the great weight and preponderance of the evidence, and it remanded the action for a new trial.[512] The court noted testimony by a "human factors expert" that if at the time of injury the plaintiff was attempting to push spilling trash back into the truck when the blade was crossing the loading door opening, then the plaintiff's action was an involuntary response or a reflex action; that the truck design caused a "trap" in that when a person sees trash falling out he automatically tries to push it back in; that because of the speed of the reactor blade if one makes such an involuntary reaction after the cycle has started he probably will not be able to realize the danger and pull his hand back; and that the act of this plaintiff was an unintentional act because of the situation.[513] The court stated that evidence of the plaintiff's familiarity with the danger, and his usual precautions against injury, militated against the assumption that the plaintiff freely and intentionally chose to risk the danger, but more strongly supported a showing that the plaintiff's action was instinctive or inadvertent.[514]

An ACV user could interact with the vehicle's automated warning devices in a number of ways that could prove relevant in product liability litigation: (1) by ignoring pre-trip warnings against using the vehicle because of some condition, whether due to weather, traffic, or lack of sufficient mapping data or software update; (2) by tampering with the warning system so as not to warn against unsafe conditions for autonomous mode; (3) by failing

508. *Id.* at 144.
509. *Id.*
510. *McAdams*, 602 S.W.2d at 375.
511. *Id.*
512. *Id.* at 381, 383.
513. *Id.* at 380–81.
514. *Id.* at 382; *see also* Coty v. U.S. Slicing Mach., 373 N.E.2d 1371 (Ill. Ct. App. 1978) (holding as a matter of law that plaintiff did not assume the risk created by the absence of a safety device because of her impulsively reaching into an area of a meat-slicing machine from which a safety device would have excluded her).

to react quickly enough to an unexpected user override alert; (4) by "over-reacting" to an unexpected user override alert.

As to (1) and (2), a court would have to determine whether the user's ignorance or disabling of a pre-trip warning was a foreseeable risk that the ACV manufacturer could have designed out, say, by making it impossible for the vehicle to drive itself under the unsafe condition. *McLennan*, *American Eurocopter* and *Besser* demonstrate that such an inquiry is highly fact-specific and largely subject to the whims of a jury. Thanks to legislation requiring the ACV manufacturer to store user-related data recorded in the moments before a crash,[515] there would likely be digital forensic proof as to interactions (3) and (4). A jury would likely hear expert testimony, as in *McAdams*, from a "human factors expert," and decide whether the user's conduct was a foreseeable risk that the defendant could have prevented with a better design—perhaps some guard against a human driver's natural instinct to "overcorrect"—or an adequate warning.

3. The Absence of an Automated Warning Device as Product Defect

In addition to failure to warn claims, the issue of automated warning devices comes up when product liability plaintiffs allege that the *absence* of such features constitutes a design or warning defect in the product. In the helicopter context, manufacturers have sometimes been held liable for failing to install such a device, and other times not. The determinations of which standards to apply and whether the design is defective are separate, as are whether the plaintiff misused the product or assumed the risk.

In *Haas v. United Technologies Corp.*, 450 A.2d 1173 (Del. 1982) (applying Maryland law), the court affirmed judgment in favor of the plaintiffs in a wrongful death action arising from the crash of a military helicopter manufactured by the defendant that occurred when a rotor blade depressurized and fractured. The question whether the absence of a cockpit in-flight warning device in the helicopter constituted a design defect that rendered the defendant liable for the deaths was a question for the jury.[516] The plaintiff had introduced evidence showing that an in-cockpit warning device for blade pressure was a necessary component of a helicopter designed for long-range flights and such a system was available for use in certain other helicopter models.[517] The defendant countered with evidence that such systems were unreliable and dangerous because a false warning of loss of blade pressure might cause a pilot to bail out or attempt to land his aircraft in rough terrain unnecessarily damaging or destroying the aircraft in the process and that defendant's repeated recommendation to install cockpit sys-

515. *E.g.*, CAL. VEH. CODE § 38750(c)(1)(G) (2014).
516. *Haas*, 450 A.2d at 1177.
517. *Id.* at 1176.

tems in the helicopters (after it learned they were being used for long-range flights exceeding two hours) went unheeded by military authorities.[518]

In *Carmical v. Bell Helicopter Textron, Inc.*, 117 F.3d 490 (11th Cir. 1997) (applying Georgia law), a helicopter crashed when the spur adapter gearshaft of the engine's compressor unit failed because it did not receive proper lubrication from the oil delivery piccolo tube, which was missing an inlet screen filter and contained metal chips in the exit end. The court affirmed the grant of summary judgment to the manufacturer, dismissing a claim that the helicopter should have been equipped with a warning light system that would alert the pilot of a reduction in the oil flow to the spur adapter gearshaft.[519] The court noted that the pilot's expert did not know whether a warning light capable of detecting a reduction of the oil flow to the spur adapter gearshaft would have been feasible or appropriate, because that was not within his area of expertise, and that the plaintiff presented no other evidence that the installation of such a warning light was feasible or appropriate.[520]

In *Kay v. Cessna Aircraft Co.*, 548 F.2d 1370 (9th Cir. 1977) (applying California law), the court held that the absence of a warning light alerting the pilot to the fact of the rear engine's failure did not constitute a warning defect, because compliance with pre-takeoff procedures in the owner's manual would have alerted the pilot of that danger. The court also held that failure to follow instructions before and during takeoff was not a foreseeable misuse for which the manufacturer could be held liable.[521]

It is expected that—at least until level-4 AVs are deployed—all AVs will feature some kind of automated warning system (along with detailed instructions for their users),[522] so that the sheer absence of such a device is an unlikely scenario. An injured plaintiff nevertheless might feasibly bring claims that the automated warning system design was defective or inadequate: by failing to recognize a warning-triggering condition, by failing to include a given driving condition as a warning trigger, by alerting the user too slowly, or some other failing.

---

518. *Id.*

519. *Carmical*, 117 F.3d at 495.

520. *Id.*; *see also* Wilson v. Boeing Co., 655 F.Supp. 766 (E.D. Pa. 1987) (applying federal law) (granting the helicopter engine manufacturer summary judgment despite the alleged defective design due to the lack of a warning indicator as to lubrication problems, where no factual information showed that the defendant learned of the alleged defect after the government's approval of the design, and where the government had over 15 years operating and maintaining 600 such engines).

521. *Kay*, 548 F.2d at 1373.

522. Regulations providing for the deployment of AVs may require such a system. *See* CA DMV, Deployment of Autonomous Vehicles for Public Operation (proposed Dec. 16, 2015) (to be codified at 13 Cal. Code Reg. § 227.56(b)) (requiring manufacturer to submit with its application for deployment certification of a "functional safety plan" and a copy of the owner's manual that provides information on an "easily accessible" mechanism to disengage the autonomous technology).

E. *Joint Tort Liability Risks for the ACV Industry*

1. Joint Tort Liability Background

Given the number of potential defendants in a product liability or other tort claim arising out of an ACV-related accident, it becomes important to examine the rules governing joint liability of multiple tort defendants. The apportionment of tort liability among multiple parties responsible for an injury has long been an issue of contention in American Jurisprudence.[523] This issue intensified as the doctrines of products liability and comparative responsibility emerged and courts began holding product manufacturers strictly liable for injuries resulting from defective products and multiple tortfeasors responsible only for their share of an accident.[524] Attempts at resolving the problem posed by the application of traditional multiple tortfeasor liability methods in the relatively new arena of strict products liability while using the newly developed doctrine of comparative responsibility has resulted in varying methodologies of liability apportionment across American courts.

Where an injury caused by multiple parties is indivisible (which is often the case in auto accident scenarios), courts vary on which is the appropriate methodology of apportioning liability.[525] According to the *Restatement (Third) of Torts*, most states have now adopted some variation on a comparative responsibility system that is applied even in cases of strict products liability.[526]

Although the final determination of responsibility for each person is made by the factfinder, certain factors have been laid out in order to aid a factfinder in making such a determination. Those factors include the nature of the party's conduct, such as their awareness or indifference with respect to risks created and any intent with respect to injuries resulting from the conduct, and the strength of the causal connection between the party's conduct and the resulting injury or injuries.[527] It is important to note that the percentages assigned by the factfinder are not representative of fault, negligence, or causation; the term responsibility is specifically used as a general and neutral term so as to not reflect any of those misconceptions.[528] As applied to strict products liability, comparative responsibility allows a defen-

523. Timothy Patton, *Comparative Causation, Indemnity, and the Allocation of Losses Between Joint Tortfeasors in Products Liability Cases,* 10 ST. MARY'S L.J. 587, 587 (1978–79).

524. *Id.*

525. RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIAB. § 17 cmt. a (AM. LAW INST. 2000).

526. *Id.*

527. *Id.* § 8.

528. *Id.* § 8 cmt. a.

dant to introduce evidence related to its absence of fault in order to reduce its percentage of responsibility.[529]

As pertaining to a conjunction of ACV part manufacturers, the upshot of this trend in tort law is that the liability of the manufacturers would likely depend on a factfinder's distribution of responsibility among the parties. However, as aforementioned, many jurisdictions differ on how to use the factfinder's distributed responsibility to apportion liability when determining damages. The next section discusses the prominent variations of allocation.

2. Parties Acting in Concert

Although the *Restatement (Third) of Torts: Apportionment of Liab.* declines to take a position on which theory of apportionment is to be preferred, it does state that parties acting in concert are always to be held jointly and severally liable for resulting damages.[530] This rule is applied regardless of the rule of a specific jurisdiction regarding multiple independent tortfeasor liability. Acts deemed to qualify a party as acting in concert with another include when a party: commits a tortious act in concert with the other pursuant to a common design; knows that the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other so to engage in such conduct; or gives substantial assistance to the other in accomplishing a tortious result and her own conduct, separately considered, constitutes a breach of duty to the third person.[531]

Historically, courts have rejected the concerted action theory in products liability cases with an indeterminate defendant because proof of concerted tortious activity is highly speculative.[532] Concerted action liability requires an agreement between parties to conceal product risk, and mere parallel activity is insufficient to impost joint and several liability on manufacturers.[533] Further, holding component manufacturers to have acted in concert would have unequitable consequences; a defendant manufacturer that could prove that it had not supplied the part that actually caused the harm could still be held liable for the entirety of the resulting damages.[534] Thus, under the current law, ACV manufacturers are unlikely to be held jointly and severally liable under a concerted action theory.

---

529. *Id.* § 8; *see* Pittsburg Coca-Cola Bottling Works v. Ponder, 443 S.W.2d 546, 548-49 (Tex.1969).

530. RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIAB. § 15 (AM. LAW INST. 2000).

531. *Id.* reporters' note cmt. a.

532. Rebecca J. Greenberg, *The Indeterminate Defendant in Products Liaiblity Litigation and a Suggested Approach for Ohio*, 39 CLEV. ST. L. REV. 207, 214 (1991).

533. Patton, *supra* note 524 at 589-90.

534. Greenberg, *supra* note 533, at 215.

3. Pure Joint and Several Liability

Pure joint and several liability was long the tradition for multiple tortfeasor liability in tort law before the aforementioned tort reforms of the late 20th century; until that time, this theory of apportionment had gained wide acceptance in American courts.[535] Courts applied this theory in situations where multiple parties caused a truly indivisible injury to a plaintiff or problems of proof precluded the injury from being divided.[536] The main premise of pure joint and several liability is that each party responsible for causing an indivisible injury can be held jointly and severally liable for the recoverable damages. The upshot of this is that a plaintiff may sue and recover all damages from any defendant found liable, thus shifting the burden of joining and asserting a contribution claim against other responsible parties on the defendant.[537] Further, the risk of insolvency of any one liable party will be borne by any other liable parties.[538]

Upon a jury finding that multiple parties were the legal cause of an indivisible injury, a jurisdiction that employs a joint and several liability method would then submit the parties to a factfinder for assignment of a percentage of comparative responsibility.[539] This effectively shifts the burden of identifying and suing other liable parties onto the shoulders of the defendants. However, a jury will not be allowed to assign responsibility to an immune party. But in a situation where one defendant's liability is limited by a statutory cap, immunity, or insolvency, the latter defendants are liable for the full amount of recoverable damages.[540] Defendants held jointly and severally liable for an indivisible injury are able to collect from other liable defendants in a suit for contribution for their respective shares of responsibility, discussed below.

The adoption of the comparative fault method has nearly foreclosed the use of pure joint and several liability as the primary liability apportionment method in American jurisdictions.[541] The *Restatement (Third) of Torts: Apportionment of Liab.* § 10 indicates that this method remains only in the few jurisdictions that have not adopted comparative responsibility.[542]

4. Several Liability

Historically, several liability was only used in situations where an injury was divisible by causation. Yet many jurisdictions adopted several liability

535. RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIAB. § A18 reporter's note on cmt. a. (AM. LAW INST. 2000).
536. *Id.*
537. Id.
538. Id.
539. *Id.* § A20.
540. *Id.* cmt. e.
541. *Id.* § 10 cmt. a.
542. *Id.*

to relieve the plaintiff of the difficulties of proving divisibility by causation. Several liability thus uses defendants' comparative percentage of responsibility to determine their respective shares of liability for an indivisible injury.[543] Here, a defendant is only liable for that portion of the plaintiff's damages that reflect the percentage of comparative responsibility to that defendant.[544] In essence, the method of several liability reverses the effects of joint and several liability.

In a several liability regime, the risk of insolvency of one or more parties legally responsible for an injury is placed on the plaintiff.[545] In addition, the burden of locating and suing all potentially responsible parties is placed on the plaintiff. Again, the factfinder bears the responsibility of assigning each party a percentage of comparative responsibility. However, unlike a joint and several liability allocation method, here the percentage of responsibility assigned to a person immune to judgment does not fall on other liable parties. Likewise, unidentified tortfeasors are not to be submitted for an assignment of responsibility.[546]

Justifying the use of a pure several liability method of allocation is difficult for the same reasons as justifying a joint and several liability method: it systematically disadvantages one party with the risk of insolvency.[547] Other concerns that have pushed jurisdictions away from the use of a several liability method of allocation include procedural rules that make the joinder of responsible parties difficult and the risks of an un-joined liable party's responsibility being borne by a joined defendant.[548] Thus, many jurisdictions have turned to a hybrid version of joint and several liability with several liability to account for the shortcomings of the two traditional allocation methods in their pure forms.

5. Joint and Several Liability with Reallocation

Concerns about the burden of an insolvent or immune party liable for an indivisible injury have influenced courts to modify existing allocation rules. One such modification is the method of reallocation in joint and several liability jurisdictions.[549] In jurisdictions that have adopted this modification, the main premises of the joint and several liability rule hold true, save for the allocation of an insolvent or immune party's responsibility.[550] Here, where a defendant can establish that a judgment for contribution cannot fully be collected from another defendant, the court will reallocate the portion that is not

543. *Id.* § 11 cmt. a.
544. *See id.* § 11.
545. *Id.* cmt. a.
546. *Id.* § B19 cmt. c.
547. *Id.* § 10 cmt. a.
548. *Id.* § B19 reporters' note on cmt. c.
549. *See id.* § C19.
550. *See id.* §§ C18-21.

able to be collected among all other parties in proportion to the percentages of comparative responsibility.[551] This reallocation is not available for any defendant subject to joint and several liability pursuant to rules on intentional tortfeasors or persons acting in concert.[552]

The rationale behind adopting such a modification lies in the implementation of comparative responsibility. Burdening one defendant with the full insolvency of another is no longer compelling where a jury has allocated responsibility among the parties.[553] This rule still creates an incentive for defendants to identify other responsible parties, but no longer categorically disadvantages them with the full burden of an insolvent defendant.

6. Hybrid Liability Based on Threshold Percentage of Comparative Responsibility

A hybrid liability based on threshold of comparative responsibility has been adopted as an alternative to the traditional allocation methods in a handful of American jurisdictions. In these jurisdictions, a threshold of comparative responsibility is required to be met by a defendant in order to hold that defendant jointly and severally liable.[554] Any defendant that does not meet the threshold is held severally liable for only their share of comparative responsibility.[555] The rationale behind the threshold is based largely in fairness principles; a minimally responsible tortfeasor should not be required to pay all of an injured party's responsible damages.[556] Because there appears to be no logical or policy argument that might justify a certain threshold percentage, the jurisdictions that use this method vary on threshold percentages and have implemented them anywhere from 10% to 60%.[557]

Unlike pure joint and several or pure several liability regimes, this hybrid method allows for the burden of insolvency to be shared by both the plaintiff and defendants. However, this method is not without criticism. Implementation of this method creates certain tactical incentives the *Restatement (Third) of Torts: Apportionment of Liab*. § D18 deems as "unfortunate."[558] Plaintiffs are forced to decide whether to maximize the number of joined parties so as to shrink their own comparative responsibility or to minimize the number of joined parties in order to increase the chance

551. *Id.* § C21.
552. *Id.*
553. *Id.* § C21 cmt. a.
554. *Id.* § D18.
555. Id.
556. *Id.* reporters' note cmt. b; *see* Walt Disney World Co. v. Wood, 515 So. 2d 198 (Fla. 1987).
557. RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIAB. § D18 reporters' note cmt. g (AM. L. INST. 2000).
558. *Id.* cmt. c.

of full recovery in hopes that one or more will be held jointly and severally liable by meeting the threshold requirement.[559]

7. Hybrid Liability Based on Type of Damages

One of the main critiques of the tort regime in general is that it awards large damages for noneconomic injuries.[560] Some jurisdictions, in order to address both this concern and the concerns arising from traditional allocation methods have implemented an allocation system that differentiates allocation methods among multiple tortfeasors based upon the type of damages resulting.[561] In these jurisdictions, defendants are held jointly and severally liable for the economic-damages potion of the recoverable damages and severally liable for each defendant's comparative share of the noneconomic damages.[562] This method addresses the risk of insolvency by allocating such risk on plaintiff for noneconomic damages and on defendants for economic damages. The rationale for this method is that it is more important to provide a damaged plaintiff with replacement for economic damages than it is to provide a damaged plaintiff full recovery of noneconomic damages.[563]

Critics of this method argue that it is ignorant of the deterrent effects of tort law. While pecuniary losses may be erratic, they do represent real injuries and compensating for those injuries is one of the main facets of tort law.[564] An additional critique is that this method favors high income plaintiffs; those plaintiffs will bear a smaller proportion of the risk of insolvency than their low income counterparts because lost income makes up for a significant portion of economic damages.[565]

8. Other Joint Liability Considerations

a. Contribution Among Multiple Tortfeasors

When multiple parties are held liable, and—either through settlement, discharge of judgment, or other means—one party discharges the liability of another, that party is entitled to recover contribution from the other.[566] A

559. *Id*.

560. *See* Am. Tort Reform Ass'n, *Mission*, http://www.atra.org/about/mission (last visited Feb. 23, 2016).

561. Restatement (Third) of Torts: Apportionment of Liab. § E18 (Am. L. Inst. 2000).

562. Id. cmt. h.

563. Id. cmt. d.

564. *Id.* § E18 reporter's note on cmt. d; *see* Kwasny v. United States, 823 F.2d 194 (7th Cir. 1987).

565. Restatement (Third) of Torts: Apportionment of Liab. § E18 reporter's note cmt. d (Am. L. Inst. 2000); *see* M. Stuart Madden, *Selected Federal Tort Reform and Restatement Proposals Through the Lenses of Corrective Justice and Efficiency*, 32 Ga. L. Rev. 1017, 1074-75 (1998).

566. Restatement (Third) of Torts: Apportionment of Liab. § 23.A (Am. L. Inst. 2000).

party entitled to contribution may recover only so much as they paid to the plaintiff in excess of its own comparative share of responsibility.[567] This entitlement allows the entitled party to assert a claim for contribution and obtain a contingent judgment in an action in which the person seeking contribution is being sued by the plaintiff, regardless of whether the party against whom contribution is sought has extinguished its liability.[568]

Not to be confused with indemnity, entitlement to contribution arises largely in jurisdictions that use a joint and several liability method of allocation. In these jurisdictions, any party held jointly and severally liable for an indivisible injury is entitled to bring an action against an additional party for any amount paid to plaintiff in excess of a jury's finding of comparative responsibility.[569] Where a party is not held jointly and severally liable, it cannot normally recover contribution.[570]

b. Effect of Settlement on Multiple Tortfeasors

The *Restatement (Third) of Torts: Apportionment of Liab.* § 23 indicates that a majority of jurisdictions also allow for a settling party to obtain contribution where the settlement extinguishes the liability of another tortfeasor.[571] Additionally, where a party makes a good-faith settlement, that party is protected from contribution suits brought against them. A contrary rule would essentially void the incentive for settlement.[572] Conversely, fairness in loss allocation requires that nonsettling tortfeasors receive a credit equal to the percentage share of a plaintiff's damages assigned to the settling tortfeasor.[573] This rule relieves nonsettling parties from liability a plaintiff has discharged while concurrently preventing plaintiff from receiving a windfall by recovering "double damages." In circumstances where the factfinder assigns no responsibility to the settling party, the nonsettling parties are not to receive any credit for the settlement.[574]

Although the *Restatement* § 23 indicates the above described method as preferred, there is variance among jurisdictions as to the apportionment of liability among a settling tortfeasor and a nonsettling tortfeasor.[575] Three basic methods exist; they are a *pro tanto* credit, where the nonsettling tortfeasor receives a credit against the judgment equal to the amount of the settlement; a *pro rata* credit, where the nonsettling tortfeasor receives a

567. *Id.* § 23.B.
568. *Id.* § 23 cmt. b.
569. *Id.* § 23 cmt. f.
570. *Id.* (indicating that there are limited circumstances in which a party held severally liable may be liable for the same indivisible injury caused by another severally liable party and thus would be entitled to contribution.)
571. *Id.* § 23 cmt. h.
572. *Id.* § 23 reporter's note cmt. i.
573. *Id.* § 16 cmt. c.
574. *Id.* § 16 cmt. f.
575. *Id*. § 16 cmt. c.

credit against the judgment equal to the settling tortfeasor's share of the damages, determined by dividing the total number of liable parties into the recoverable damages; and a percentage or comparative share credit, as described in the outset of this section.[576]

c. Indemnity in Cases with Multiple Tortfeasors

Similar to contribution in some fashions, tort rules of indemnity allow for the recovery of the amount paid to the plaintiff as well as reasonable legal expenses when one party discharges the liability of the other in whole or in part under certain circumstances.[577] The *Restatement (Third) of Torts: Apportionment of Liab.* § 22 indicates that for a party to recovery indemnity, the indemnitor must have agreed by contract to indemnify the indemnitee; or the indemnitee must not have been liable except vicariously for the tort of the indemnitor or was not liable except as a seller of a product supplied by the indemnitor and the indemnitee was not independently culpable.[578] The right to indemnity pursuant to contract is not contingent on whether the party against whom indemnity is sought is liable to the plaintiff.[579]

Issues of indemnity often arise where one party suffers judgment, yet, for some reason, another party was completely or mostly at fault. While contractual indemnity is determined by the terms of the contract, specific circumstances allow for the recovery of indemnity regardless of a contract. In such cases, an indemnitee must extinguish the liability of the indemnitor to collect indemnity, either through settlement or satisfaction of judgment.[580] The rationale behind this rule is grounded in fairness; no person should be required to pay non-contractual indemnity while remaining liable to the plaintiff.[581] Further, a person seeking indemnity must prove that the indemnitor would have been liable to the plaintiff in order to allow the indemnitor "his day in court."[582] However, most issues of indemnity are those of contractual indemnity. And a majority of American jurisdictions enforce contracts for indemnity where the contract contains clear and unequivocal language.[583]

9. Notable State Laws

This section addresses the substantive joint liability (allocation and apportionment) laws in the jurisdictions of California, Michigan, and New York, respectively.

---

576. *Id.* § 16 reporter's note on cmt. c.
577. *Id.* § 22.
578. *Id.*
579. *Id.* § 22 cmt. f.
580. *Id.* § 22 cmt. b.
581. *Id.* § 22 reporter's note on cmt. b.
582. *Id.* § 22 reporter's note on cmt. c.
583. *Id.* § 22 reporter's note on cmt. f.

a. California

The allocation and apportionment methods applied by the courts of California are crucial to the widespread implementation of ACVs not only because it is the heart of the tech industry in America, but because Google, one of the leaders in ACV technology development, is headquartered in California; Google carries out much of its testing on its campus located 35 miles south of San Francisco.[584] California courts—the forums responsible for creation of the contemporary doctrine of strict products liability—have primarily implemented a hybrid system of liability for multiple tortfeasors responsible for an indivisible injury based on the type of damages resulting—discussed in section III.E of this memorandum.[585]

California courts, however, do not apply this relaxed method of pure joint and several liability in traditional strict products liability actions; there, the common law tradition of joint and several liability remains.[586] The rationale for this decision is that, as a matter of public policy, liability is imposed under the California strict products liability doctrine irrespective of fault.[587] However, the law of California does entitle tortfeasors responsible for an indivisible injury to an apportionment of liability based on their respective comparative fault, a term referred to in those jurisdictions as comparative equitable indemnity.[588]

Lastly, in products liability actions with multiple tortfeasors responsible for an indivisible injury, California courts recognize that indemnity agreements created between the parties or by the statute may govern apportionment of liability.[589] An example specifically concerning motor vehicles can be found in Cal. Veh. Code § 3064(a); the statute requires that every new franchisor must inform franchisees of their preparation obligations, and the performance of those obligations will determine the liability between the franchisor and franchisee.[590] A recent amendment to a piece of California legislation concerning the regulation of ACVs struck previous language that indicated current law shall control issues of liability arising from the operation of ACVs. However no affirmative legislation on the topic has resulted.[591] A more in depth discussion of California's various motor vehicle manufacturing regulations relevant to ACV production is necessary in un-

584. John Markoff, *Google Cars Drive Themselves, in Traffic*, N.Y. TIMES (Oct. 9, 2010), http://www.nytimes.com/2010/10/10/science/10google.html.

585. CAL. CIV. PRAC. TORTS § 4:5 (WEST 2015).

586. *Id.* §§ 4, 4:5

587. *Id.* § 4:5.

588. *Id.* § 24:6.

589. *Id.*

590. *Id.* § 24:6; CAL. VEH., *supra* note 123, at § 3064(a).

591. Gabriel Weiner & Bryant Walker Smith, *Automated Driving: Legislative and Regulatory Action*, CTR. FOR INTERNET & SOC'Y, http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action#Federal_Regulatory_Guidance.

derstanding the challenges ACV manufacturers face, but it is outside the scope of this memorandum.

b. Michigan

The State of Michigan, the global center of automotive research and development, contrasts with California in its allocation and apportionment of multiple tortfeasor liability.[592] The courts of Michigan largely implement a pure several liability method of liability allocation, and a liable party in a Michigan state court is not required to pay damages in an amount greater than its percentage of fault, based on the fault of all parties responsible for the injury, save for in cases of medical malpractice.[593] In medical malpractice cases, Michigan law calls for a joint and several liability method with reallocation as described in section III.C. of this memorandum.

In the realm of products liability, Michigan is somewhat of an anomaly; Michigan is the only state that does not recognize strict liability in products liability actions.[594] In 2009, this long held belief was affirmed by the Michigan Court of Appeals in *Curry v. Meijer, Inc.*, 780 N.W.2d 603 (Mich. Ct. App. 2009). There, the court held that a plaintiff in a products liability suit against a non-manufacturing seller must prove negligence on the part of the seller to prevail.[595] As to multiple tortfeasors in products liability cases, Michigan's pure several liability allocation method generally applies.[596] Additionally Michigan caps products liability for noneconomic damages at $280,000, except where the product defect causes death or permanent loss of a vital bodily function, in which case the cap is set at $500,000.[597]

In direct response to the development and manufacturing of ACVs in the state, the Michigan legislature has enacted various policies on the subject. Specifically, the legislature enacted legislation that shields an auto manufacturer from liability resulting from another party's attempted conversion of a non-AVs into AVs.[598] Michigan, the American center of auto manufacturing, is a state rich with legislation and regulation that will undoubtedly affect the manufacturing of AVs, but an examination of this material is outside of the scope of this memorandum.

---

592. MICH. ECON. DEV. CORP., *Michigan's Automotive Industry*, http://www.michiganbusiness.org/cm/Files/Brochures/1283Auto%20brochure.pdf; RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIAB. § 17 reporter's note on cmt. a (AM. LAW INST. 2000).

593. MICH. CIV. JURIS. TORTS § 24:16 (WEST 2016); MICH. COMP. LAWS ANN. § 600.6304 (WEST 1996).

594. MICH. CIV., *supra* note 594 § 9:1; Phillips v. J. L. Hudson Co., 79 Mich. App. 425 (1977).

595. Curry v. Meijer, Inc., 780 N.W.2d 603, 610 (Mich. Ct. App. 2009).

596. MICH. CIV., *supra* note 594; MICH. COMP., *supra* note 594.

597. MICH. CIV. JURIS. PROD. LIAB. § 15 (WEST 2016).

598. CTR. FOR INTERNET & SOC'Y, *Automated Driving: Legislative and Regulatory Action*, https://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action#Enacted. (last visted Feb. 23, 2016, 3:23 PM).

c. New York

The laws of New York are crucial to understand in this context, because historically they have been on the forefront in terms of allocation and apportionment and because much of the value associated with the implementation of ACVs is increasing safety in areas of high traffic congestion; New York City is one of the most traffic-congested areas in the nation.[599] New York courts employ a hybrid liability for multiple tortfeasors responsible for an indivisible injury that is based on a threshold percentage of comparative responsibility, as described above.[600] New York defendants are held jointly and severally liable for noneconomic damages when a defendant's comparative responsibility is greater than 50%, the threshold percentage.[601] Where the damages are economic, defendants are held jointly and severally liable, regardless of comparative responsibility percentage.[602]

In New York products liability cases, however, defendants are always subject to joint and several liability.[603] In such cases, the liability of more than one defendant may result in the more responsible defendant being required to indemnify the less responsible defendant.[604] The New York legislature currently has legislation concerning AVs in committee as of January 6, 2016.

V. Incentivizing Innovative Networks

This Section addresses incentives to promote the necessary private and/or public investment in ACV technologies. ACVs present classic issues related to network effects. That is, the safety benefits of ACVs will be exponentially realized the more ACVs are deployed. In addition, ACVs present several instances of network externalities. That is, the full societal benefits from the deployment of a certain ACV technologies will not be enjoyed if private entities are left to make decisions based on their own individual cost/benefit analysis. Section V.A. addresses the societal benefits of ACVs. Section V.B. addresses the extent to which the National Highway Safety Administration (NHTSA) can require certain investments by OEMs, individuals, or municipalities in bringing ACVs to market. Section V.C. ad-

599. Restatement (Third) of Torts: Apportionment of Liab. § 17 reporter's note on cmt. a (Am. Law Inst. 2000); Stephen Shankland, *Platooning: The Future of Freeways is Lining Up*, CNET (Sept. 3, 2013, 8:44 AM), http://www.cnet.com/news/platooning-the-future-of-freeways-is-lining-up/; Alexander E.M. Hess & Samuel Weigley, *Ten Cities with the Worst Traffic*, USA Today (May 4, 2013, 11 AM), http://www.usatoday.com/story/money/cars/2013/05/04/worst-traffic-cities/2127661/.

600. Apportionment of Liab. § 17 reporter's note on cmt. a.

601. *Id.*

602. 103 N.Y. Jur. 2d Torts § 33 (2017).

603. Apportionment of Liab. § 17 reporter's note on cmt. a; 103 N.Y. Jur. 2d Torts § 39 (2017).

604. 103 N.Y. Jur. 2d Torts § 34 (2017).

dresses the framework for government liability in light of the fact that state and local governments will likely be involved in promoting, if not deploying, aspects of ACV infrastructure. Lastly, section V.D. discusses particular incentives that could be used to foster certain aspects of ACV deployment.

A. *Societal Benefits of ACVs*

1. The Benefits of ACVs

Dean Garfield, President and CEO of Information Technology Industry Counsel, which represents 62 technology companies, including: Toyota, Qualcomm, Google, Apple, and IBM, testified in November 2015 to the U.S. House of Representatives Committee on Oversight and Government Reform subcommittee.[605] Garfield identified some of the externalities imposed by automobiles, including:

- the World Health Organization estimated there were 1.24 million deaths on the world's roadways in 2010;
- according to the U.S. Census Bureau, there were 10.8 million accidents on U.S. roadways in 2009;
- annual costs from automobile accident injuries amount to $365 billion, and costs from fatalities amount to $260 billion[606]

With ACVs reportedly capable of preventing 90 percent of accidents, according to Garfield, the positive economic impact from accident avoidance alone would be $563 billion annually.[607] Garfield continued to point out that ACVs present potential benefits beyond crash avoidance, such as increased productivity, decreased congestion, fuel savings, car sharing, and increased mobility for those currently incapable of driving. Garfield cited a study estimating the total positive benefits of ACVs (including crash avoidance and other, non-safety related benefits) to be over a trillion dollars annually.[608]

The RAND Report thoroughly analyzed the social costs of automobiles and the benefits of ACVs. According to that report, the social costs of traditional automobiles amount to 13 cents per mile driven.[609] The RAND Report noted that this is almost equal to the 14 cents per mile we pay for fuel

605. *Internet of Cars: Hearing Before the H Comm. on Oversight and Gov't Reform Subcomm. on Info. Tech. and Subcomm. on Transp. and Pub. Assets*, 114th Cong. (2015) (statement of Dean C. Garfield, President and CEO of the Information Technology Industry Council), https://oversight.house.gov/wp-content/uploads/2015/11/11-18-2015-Joint-Subcommittee-Hearing-on-Internet-of-Cars-Garfield-ITI-Testimony.pdf.

606. *Id.*

607. *Id.*

608. *Id.*

609. RAND Report, *supra* note 69, at 11.

when gasoline costs $3.50;[610] and with the current price per gas we spend significantly less on gas per mile than the social costs we impose per mile.[611]

The RAND report went on to describe the benefits provided by ACVs beyond safety:

- NHTSA Level 4, driverless cars, are capable of expanding mobility and access to the disabled, older citizens, and children under the age of 16.[612]
- ACVs could decrease traffic congestion costs by reducing vehicle miles traveled per capita, increasing vehicle throughput on existing roads, and reducing crash-related delays.[613]
- ACVs could reduce the need for parking space in urban cores areas.[614]
- ACVs could increase passenger productivity.[615]
- ACVs could drastically reduce fuel consumption through: enabling the widespread adoption of smaller safer cars; decreasing traffic congestion; enabling platooning; implementing automated efficient driving practices; and enabling alternative fuels due to reduced vehicle weights, autonomous battery-charging or hydrogen refueling capabilities, and vehicle-to-grid enabled battery-charging.[616]

To be fair, the RAND Report notes there might be some negative consequences from ACVs. These include, an increase in vehicle miles traveled due to the increased access to and the decreased cost of transportation. ACVs might distract from public transit investment, and will likely result in the loss of jobs for drivers and/or manufacturers.[617]

2. Network Effects

Many have recognized that ACVs present a classic case of "network effects."[618] "Network effects" have been described as situations where the

610. *Id.*

611. GASBUDDY.COM, *US Average Gas Prices by State* (2016), http://www.gasbuddy.com/USA.

612. RAND, *supra* note 69, at 17.

613. *Id.* at 17-25.

614. *Id.* at 26.

615. *Id.* at 25-26.

616. *Id.* at 26-38.

617. *Id.* at 38-40.

618. J.C. Sullivan, *What Will Drive The Future of Self-Driving Cars?* 10 (AM. ENTER. INST., May 2015), http://www.aei.org/wp-content/uploads/2015/05/Future-of-driverless-cars.pdf (describing the network effects of both autonomous and connected vehicles); *Top Misconceptions of Autonomous Cars and Self-Driving Vehicles*, DRIVERLESS CAR MARKET WATCH, (July 1, 2015), http://www.driverless-future.com/?page_id=774.

value of a particular activity increases the more other people engage in the activity.[619] Examples of network effects include fax machines and social networking; the value to a potential consumer depends on how many others use the same technology.[620] AVs exhibit network effects because many of the societal benefits are increased as more AVs are adopted. It does no good if one's vehicle is fully autonomous if a vehicle in close proximity is driven by a reckless or distracted driver. Similarly, the traffic synchronization benefits from AVs come from a critical mass of vehicles being AVs.[621] Similarly, the benefits of a CV system, only arise from a substantial number of vehicles on the road having interoperable CV technology.

Due to these network effects, many of the societal benefits from ACVs reflect "positive externalities." As described by David Easley and Jon Kleinberg:

> An *externality* is any situation in which the welfare of an individual is affected by the actions of other individuals, without a mutually agreed-upon compensation. For example, the benefit to you from a social networking site is directly related to the total number of people who use the site. When someone else joins the site, they have increased your welfare even though no explicit compensation accounts for this. This is an *externality*, and it is *positive* in the sense that your welfare increases.[622]

As is the case often with positive externalities, such as the societal benefits of ACVs, an individual market participant may not internalize these benefits.[623] In other words, especially in the early stages, prior to the realization of the network effects of ACVs, an individual entity may not invest in ACV deployment if basing the decision solely on its own benefits. Accordingly, it is important to consider what incentives might be needed to cause individual actors to invest in ACV deployment.

B. *NHTSA's Authority to Mandate ACV Deployment*

This section analyzes the extent to which NHTSA can require entities such as OEMs, vehicle operators, or municipalities to invest in developing ACV technology.

---

619. David Easley & Jon Kleinberg, Networks, Crowds, and Markets: Reasoning about a Highly Connected World 509 (2010).

620. *Id.*

621. Sullivan, *supra* note 619, at 10.

622. Easley and Kleinberg, *supra* note 620, at 509-10.

623. Brian Galle, *The Tragedy of the Carrots: Economics and Politics in the Choice of Price Instruments,* 64 Stan. L. Rev. 797, 831-832 (Apr. 2012).

1. NHTSA's Authority Generally

The federal agency now known as NHTSA was born from companion acts passed on September 9, 1966, the National Traffic and Motor Vehicle Safety Act[624] ("Motor Vehicle Safety Act") and the Highway Safety Act.[625] NHTSA is responsible for "reducing deaths, injuries and economic losses resulting from motor vehicle crashes."[626] One of NHTSA's primary tools in seeking to accomplish this goal is the ability to set and enforce safety performance standards for motor vehicles and motor vehicle equipment ("FMVSSs").[627] FMVSSs may govern "motor vehicles" or "motor vehicle equipment."[628] The Act defines a "motor vehicle" as "a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways."[629] The Act defines "motor vehicle equipment" as:

> (A) any system, part, or component of a motor vehicle as originally manufactured;
>
> (B) any similar part or component manufactured or sold for replacement or improvement of a system, part, or component, or as an accessory or addition to a motor vehicle; or
>
> (C) any device or an article or apparel, including a motorcycle helmet and excluding medicine or eyeglasses prescribed by a licensed practitioner, that –
>
> (i) is not a system, part, or component of a motor vehicle; and
>
> (ii) is manufactured, sold, delivered, or offered to be sold for use on public streets, roads, and highways with the apparent purpose of safeguarding the users of motor vehicles against risk of accident, injury, or death.[630]

Besides its authority to issue FMVSSs, NHTSA also has general authority to prescribe regulations to fulfill the duties of the DOT Secretary, including to

---

624. National Traffic and Motor Vehicle Safety Act, Pub. L. No. 89-563, 80 Stat. 718 (1966) (current version at 49 U.S.C. §§ 30101-30169 (2012)).

625. Pub. L. No. 89-564, 80 Stat. 735 (1966) (current version at 23 U.S.C. §§ 401-10 (2012)).

626. NHTSA, *Who We Are and What We Do*, http://www.nhtsa.gov/About+NHTSA/Who+We+Are+and+What+We‡o [https://web.archive.org/web/20161118163734/http://www.nhtsa.gov/About-NHTSA/Who-We-Are-and-What-We-Do]. (last updated Nov. 18, 2016).

627. 50 U.S.C. §§ 30111(a) (2012) ("The Secretary of Transportation shall prescribe motor vehicle safety standards. Each standard shall be practicable, meet the need for motor vehicle safety, and be stated in objective terms.").

628. *Id.* § 30102(a)(9) (defining "motor vehicle safety standard" as "a minimum standard for motor vehicle or motor vehicle equipment performance.").

629. *Id.* § 30102(a)(6).

630. *Id.* § 30102(a)(7).

reduce traffic accidents and deaths and injuries resulting from traffic accidents.[631]

2. NHTSA's Authority Related to FMVSS No. 150 for V2V Communications

NHTSA's proposed connected vehicle system provides a useful example of the numerous technological and operational aspects involved in bringing CV technologies to market. Accordingly, the following sections will focus on the connected vehicle system contemplated under NHTSA's proposed FMVSS No. 150. As discussed in Section II.A.2.a, on August 20, 2014, NHTSA issued an Advance Notice of Proposed Rulemaking ("ANPRM") concerning proposed FMVSS No. 150, requiring V2V communication capability for light vehicles.[632] Proposed FMVSS No. 150 raises unique questions about NHTSA's authority because FMVSS No. 150 proposes an entire architecture for a connected vehicle system, and not just particular in-vehicle equipment. Like other FMVSSs, NHTSA's proposed FMVSS 150 would require vehicle-based hardware such as DSRC radios, a GPS receiver with a process, an inertial measurement unit, and a driver-vehicle interface.[633] Beyond these in-vehicle hardware components, FMVSS No. 150 would also require non-vehicle based hardware such as roadside equipment including wireless communications infrastructure to support communication between the vehicle and the SCMS.[634] The proposed standard would also involve software that determines and transmits vehicle conditions and evaluates whether to issue warnings.[635] FMVSS No. 150, as proposed by NHTSA would involve a Security Credential Management System to govern and manage the cybersecurity aspects of the V2V system.[636] NHTSA has also proposed guidance on how aspects of the system architecture would address privacy concerns.[637]

In the V2V Readiness Report, NHTSA identifies why it believes certain aspects of the V2V system architecture fall within its authority. It is relatively clear that NHTSA can require that new vehicles include in-vehicle DSRC units.[638] Such units would constitute "motor vehicle equipment" because they are a "system, part, or component of a motor vehicle as originally manufactured."[639] NHTSA also opines that it can regulate aftermarket in-

631. *Id.* § 402(a).
632. Federal Motor Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 49270 (Aug. 20, 2014) (to be codified at 49 C.F.R. pt. 571).
633. V2V Readiness Report, *supra* note 49, at 67.
634. *Id.* at 69.
635. *Id.* at 70.
636. *Id.* at 162.
637. *Id.* at 144.
638. *Id.* at 45.
639. 50 U.S.C. § 30102(a)(7) (2012).

vehicle equipment.[640] Concerning the roadside equipment, NHTSA has stated that to the extent road side equipment transmits safety information to vehicles, the NHTSA has taken the position that such infrastructure is likely a device "manufactured. . . with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death" and therefore motor vehicle equipment under §30102(a)(7)(C) of the Safety Act.

On the other hand, there are multiple aspects of the V2V system architecture proposed by NHTSA that are not clearly within its existing legal authority. For example, NHTSA recognizes that its proposed V2V system would require communications and security components that it cannot mandate under its existing authority.[641] While NHTSA may be able to indirectly regulate through its ability to enter into agreements or contracts under the "necessary expense doctrine,"[642] its enforcement mechanisms for such regulators are not as strong as for FMVSSs.

a. Roadside Equipment

Concerning roadside infrastructure, NHTSA's ANPRM and associated documents indicate no plans for NHTSA to mandate such equipment.[643] Indeed, NHTSA has stated that roadside equipment that merely receives data from a vehicle, but does not transmit information to a vehicle, likely does not constitute "motor vehicle equipment."[644] Further, at least one commenter to NHTSA's ANPRM has questioned whether NHTSA has authority over roadside equipment even when it directly facilitates V2V communica-

640. V2V READINESS REPORT, *supra* note 49, at 39. To the extent a device is provided, with a "substantial portion of its expected use [ ] in conjunction with motor vehicles" then NHTSA believes such a device would fall under its regulatory authority. *Id.* at 39. NHTSA has previously also taken the position that it has authority over a smartphone application enabling the smartphone to transmit and receive BSMs and alert drivers of a potential crash. *Id.* at 39-40. Accordingly to NHTSA, this application would constitute a motor vehicle "accessory" because of its use with the motor vehicle. *Id.* The application would also constitute a "device or article manufactured or sold with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death." *Id.*

641. *Id.* at 61 ("The discussion in this section has focused so far on what it would take to establish FMVSSs to facilitate a V2V system, but a V2V system is not complete without communications and security components that NHTSA cannot mandate fully under its Safety Act authority.")

642. *See Use of Appropriated Funds to Purchase Kitchen Appliances,* 2004 WL 1853469 (June 25, 2004) ("The general rule is that where an appropriation is not specifically available for a particular item, its purchase may be authorized as a necessary expense if there is a reasonable relationship between the object of the expenditure and the general purpose for which the funds were appropriated, so long as the expenditure is not otherwise prohibited by law.") (citing 66 COMP. GEN. 356 (1987)).

643. FHA, *2015 FHWA Vehicle to Infrastructure Deployment Guidance and Products: V2I Guidance Draft* (Sept. 29, 2014) [hereinafter FHWA V2I GUIDANCE DRAFT] at 1.

644. *Id.* at 42.

tions.[645] Additionally, even if NHTSA did have authority to regulate the performance of such roadside equipment, it is doubtful that NHTSA could directly require municipalities to install roadside equipment. Accordingly, some incentive system would need to be in place to encourage municipalities or their private sector partners) to invest in the costly roadside infrastructure needed to support V2I.

Lastly, it is also questionable whether NHTSA is the only agency with authority related to roadside equipment. The Alliance of Automobile Manufacturers has also suggested "it is the FHWA [Federal Highway Authority] that ordinary has jurisdiction over road-side equipment."[646] The FHWA has indicated that deployment of V2I services will be strongly encouraged but will be voluntary.[647]

b. In-vehicle Equipment

Concerning in-vehicle equipment, it is doubtful that NHTSA could directly require existing vehicle owners to upgrade their vehicles with V2V technology. This is important because the significant crash avoidance benefits of V2V can only be achieved when a critical mass of vehicles are connected to the system.[648] While NHTSA contemplates aftermarket devices,[649] it does not indicate any plan to mandate existing vehicle operators to update their vehicles with such devices. Indeed, NHTSA likely lacks the authority "to require retrofitting of older vehicles with new safety equipment unless the vehicle is a commercial vehicle."[650] Additional incentives would need to be provided for vehicle operators to adopt such devices.

Further, as stated in Section III.B.4, because NHTSA's proposed SCMS would only provide vehicles with a limited set of security credentials, vehicles operators would need to occasionally update their security credentials. NHTSA does not clearly have the authority to require vehicle operators to update their credentials or other V2V software. Indeed, the Alliance of Automobile Manufacturers has taken the position that NHTSA's authority does not extend to the "relationship between the vehicle manufacturers and their

645. Alliance of Automobile Manufacturers, Comment Letter to Proposed Federal Motor Vehicle Safety Stanndard No. 150; Vehicle-to-Vehice (V2V) Communications (Oct. 20, 2014), [hereinafter ALLIANCE COMMENT LETTER] at 7.

646. *Id.* attachment A, p. 2.

647. FHWA V2I GUIDANCE DRAFT, *supra* note 644, at 3.

648. Thilo Koslowski, *U.S. Government Must Clarify Its Terms to Boost V2V Technology Adoption,* GARTNER (February 10, 2014) ("V2V communication benefits will not be fully realized for years, until vehicles that can communicate with each other attain critical mass on the roads. This makes a government mandate for automakers' compliance critical. If adoption is widespread, safety benefits will be apparent within eight years; in approximately 15 years, nearly all U.S. vehicles would include V2V technology.")

649. V2V READINESS REPORT, *supra* note 49, at 29-31.

650. Wood et al., *supra* note 30, at 1436.

customers (except as it relates to communicating about safety recalls).[651] NHTSA's attorneys have taken a similar position, stating that "[NHTSA] does not regulate the actions of vehicle owners [ ] or the maintenance and repair of vehicles-in-use."[652] Accordingly, concerning the actions of vehicle operators, additional laws would need to be passed requiring their maintenance of their vehicles to maintain up-to-date security credentials and software. Alternatively, some legal or contractual authority would need to be implemented to allow OEM's (or some other system operator) to "push" upgrades to the vehicle.

c. SCMS Management and Operation

Concerning security, as discussed in Section III.B.2, NHTSA proposes a Security Credential Management System ("SCMS") that imposes a public key infrastructure cryptography method. The SCMS would be governed by an entity or entities taking the role of SCMS Manager.[653] It is unclear how NHTSA authority would relate to the actions of entities managing the SCMS. Indeed, it appears NHTSA currently plans to indirectly regulate the SCMS entities via its ability to contract with outside parties.[654]

d. Privacy Aspects

Additionally, the proposed V2V system will only function properly if privacy and cybersecurity considerations are properly managed. Concerning privacy, NHTSA calls privacy considerations "critical" to the analysis of the proposed V2V system. NHTSA states that the "system will not collect or store any data on individuals or individual vehicles, nor will it enable the government to do so."[655] While some privacy considerations could fall under NHTSA's authority (e.g., the content of Basis Safety Messages transmitted from in-vehicle safety equipment), NHTSA likely does not have the authority to regulate all aspects of the proposed privacy framework for its V2V system. In particular, it is unclear that NHTSA would have the authority to impose the "organizational controls"[656] and "policy controls"[657] required to minimize privacy risks. Indeed, "[i]ndustry members . . . have suggested that the Federal Government should play a central role in protect-

651. *Id.*
652. *Id.* at 1435.
653. SCMS RFI, *supra* note 257, at 12-13.
654. V2V Readiness Report, *supra* note 49, at 43-44, 61.
655. *Id.* at 144.
656. *Id.* at 148.
657. *Id.* at 155 (describing "policy controls" as "laws or organizational policies that make unauthorized data collection, storage, or disclosure less likely by creating organizational and/or functional separation and imposing organizational or legal consequences against hackers or malfeasant insiders.").

ing individual privacy in the V2V context, through regulation or governance over the SCMS."[658]

3. Costs of V2V and V2I Deployment

The above limitations are not insignificant. NHTSA estimates that the total cost for the V2V system to be approximately $350 per consumer in 2020. This would include vehicle equipment costs, fuel economy impact, SCMS costs, and communication costs. The costs for V2I system infrastructure are more significant. While total cost estimates are unclear, a September 2015 Government Accountability Office report estimated that V2I technology may cost $51,650 per site in non-recurring costs (in addition to the recurring costs of SCMS management).[659] Furthermore, according to that same report, the decision to deploy V2I technologies will be up to the states and localities.[660] Accordingly, the extent to which state and local governments can fund the V2I deployment might greatly impact the speed of deployment. That report stated that many states and localities may lack resources for funding both V2I equipment and the personnel needed to install, operate, and maintain the technologies.[661] The FHWA has noted that some funds for V2I deployment may be available under various Federal-aid highway programs.[662]

4. AV Infrastructure Requirements

Questions related to NHTSA's ability to mandate deployment of transportation infrastructure are not unique to CV technologies. While AV technologies are less reliant on transmissions from sources external to the vehicle, there will likely need to be changes to the transportation infrastructure. For example:

- changes to construction warning signs and equipment to notify AVs of the presence of construction conditions (unlike a human driver, an AV will likely not be able to detect a construction worker's hand gestures);[663]
- changes to traffic lights so AV cameras can detect their color even when looking into the sun;[664]

---

658. *Id.* at 146.

659. U.S. Gov't Accountability Off., GAO-15-775, Intelligent Transportation Systems: Vehicle-to-Infrastructure Technologies Expected to Offer Benefits, but Deployment Challenges Exist 39 (2015).

660. *Id.* at 21.

661. *Id.* at 23.

662. FHWA V2I Guidance Draft, *supra* note 644, at 5.

663. Andrew Ng and Yuanqing Lin, *Self-driving Cars Won't Work Until We Change Our Roads – and Attitudes*, Wired (Mar. 15, 2016), http://www.wired.com/2016/03/self-driving-cars-wont-work-change-roads-attitudes/.

664. *Id.*

- new communication techniques for emergency service vehicles;[665]
- creating clear lane markings;[666]
- creating uniform road markings across states;[667]

Similar to the questions about for the V2V system roadside equipment, it is not clear that NHTSA's authority covers the above infrastructure. Further, it is unlikely that NHTSA, under its existing legal authority, could require state or local governments to invest in the above infrastructure.

5. Potential for Expanded Federal Agency Authority

For a variety of reasons, it appears DOT is examining the potential for new legislation and/or regulations related to ACVs. As discussed above in Section II.B.3.d, there is a growing consensus that uniform regulations are needed related to the deployment of ACVs on public roads. As discussed in Section II.A.2.d-e, NHTSA likely needs additional rulemaking to confirm its FMVSSs permit driverless cars. Additionally, as discussed in this Section V.B, DOT needs to consider what additional authorities are necessary to help deploy the infrastructure necessary to fully support ACVs. It is likely not prudent to mandate the immediate adoption all aspects of an integrated ACV system. Nonetheless, there may be particular aspects, such as the need for vehicle operators to maintain updated security credentials, that could be best supported by expanded federal or state laws. DOT has scheduled public meetings to explore what new regulatory tools and authorities might be required to meet NHTSA's safety mission in a world of ACVs.[668]

C. *Government Liability*

As explained above in section V.B., it is likely that state and local governments will play at least some role in deploying infrastructure to support ACVs. In addition to the questions about how these governments will fund this infrastructure, these governments will also have questions about their increased liability from deploying, operating, and maintaining aspects of a sophisticated transportation network. This section lays out the general framework for assessing government liability in the context of traffic control devices.

---

665. *Id.*

666. *Id.*

667. Daniel Vock, *States Fix Infrastructure to Prepare for Driverless, Connected Cars*, GOV'T TECH. (Mar. 7, 2016), http://www.govtech.com/fs/infrastructure/States-Fix-Infrastructure-to-Prepare-for-Driverless-Connected-Cars.html.

668. U.S. DEP'T OF TRANSP., U.S. DOT TO HOST PUBLIC MEETINGS ON SAFE OPERATION OF AUTOMATED VEHICLES, 2016 WL 922770.

1. Analysis of Tort Liability for Traffic Control Devices

In almost any form of deployment, ACV technologies will require state and local municipalities to be involved, directly or indirectly, in deploying, operating, and maintaining infrastructure to support ACVs. V2I technology would involve the infrastructure playing "a coordination role by gathering global or local information on traffic and road conditions and then suggesting or imposing certain behaviors onto a group of vehicles."[669] Essential to this function is the wireless exchange of data between a vehicle and infrastructure "that could, among other things: warn drivers of upcoming road conditions, such as work zones, or that they are approaching a curve at an unsafe speed; adjust traffic signal lights to provide priority to emergency vehicles or to address congestion; advise drivers about upcoming traffic and alternative routes; and provide driving advice to minimize stop-and-go driving."[670] Even with non-connected AVs, as discussed above in Section V.B.4, state and local governments would likely need to be involved in deploying infrastructure changes to support the AV's. Accordingly, transportation infrastructure will shift from providing human-readable information to a human driver to exchanging data with electronics devices.

This shift in the role of transportation infrastructure does not change the possibility that an inadequate function or defect of infrastructure could potentially lead to life threatening accidents. In some V2I related studies, experts have pointed out that an accident involving a vehicle utilizing V2I technology could make it more difficult "to determine whether fault . . . lies with one of the drivers, an automobile manufacturer of a device, or another party."[671] The United States Government Accountability Office has provided the following insight on the legal liability issue based on interviews with experts and government officials:

> According to DOT officials, it is unlikely that either V2I or V2V technologies will create significant liability exposure for the automotive industry, as DOT expects auto manufacturers will contractually limit their potential liability for integrated V2I and V2V applications and third-party services. However, according to DOT, V2I applications using data received from public infrastructure may create potential new liability risks to various infrastructure owners and operators—state and local governments, railroads, bridge owners, and roadway owners—because such cases often are brought

669. Luigi Glielmo, THE IMPACT OF CONTROL TECHNOLOGY, INST. OF ELECTRICAL & ELECTRONICS ENGINEERS (T. Samad et al. eds., 2011), http://www.dis.uniroma1.it/~automatica/uploads/IEEE_ImpactControlTechnology_Report_2011.pdf.

670. U.S. GOV'T ACCOUNTABILITY OFF., *Intelligent Transportation Systems: Vehicle-to-Infrastructure Technologies Expected to Offer Benefits, but Deployment Challenges Exist* 1 (Sept. 2015), http://www.gao.gov/assets/680/672548.pdf.

671. *Id.* at 32.

> against public or quasi-public entities and not against vehicle manufacturers. According to DOT, this liability will likely be the same as existing liability for traffic signals and variable message signs.[672]

Installations of traffic control devices that utilize V2I technology are a good example of infrastructure that facilitates the deployment of ACVs. An overview of the tort liability framework governing the installation and maintenance of these traffic control devices is necessary for a successful transition to the autonomous vehicle age.

2. Qualified Immunity of Local Municipal Corporations

a. General Rule for Immunity: Governmental vs. Proprietary Function

Traffic control devices are usually built and maintained by local municipal corporations. Thus, when injury occurs due to malfunctioning of a traffic control device, the injured typically sue a public entity. "The general rule is that . . . there can be no recovery against a state or municipal corporation for injuries caused by its negligence or nonfeasance in the exercise of functions essentially governmental in character, but there can be recovery insofar as the state or municipal corporation acts in its private or proprietary capacity."[673] In other words, a municipality may have immunity from tort liability if it was performing a governmental function rather than a proprietary function.

For example, courts in states including Michigan, California, and New York have concluded that in the absence of a statute requiring installation of traffic control devices at certain intersections, the decision to install one is a governmental function. Indeed, the Virginia Transportation Research Council has suggested that a decision to install or not to install devices such as traffic lights, blinking lights, warning signals, roadway markings, railings, barriers, guardrails, and curbing that regulates traffic for safety are all examples of governmental functions.[674]

Once the court in a particular case decides that the municipal corporation involved is not immune from tort liability because it was not performing a governmental function, then principles of common law negligence would govern the case.[675] While most jurisdictions including Michigan, California, and New York have construed the maintenance of installed traffic control devices as a governmental function, some jurisdictions including Illinois, Iowa, and New Jersey have concluded that it is a proprietary function.[676] The

672. *Id.*
673. 34 A.L.R.3d 1008.
674. VA TRANSP. RES. COUNCIL, *Tort Liability: A Handbook for Employees of the Virginia Department of Transportation and Virginia Municipal Corporations* 11 (2004), http://www.virginiadot.org/vtrc/main/online_reports/pdf/04-r30.pdf.
675. CAL. GOV. CODE § 830.
676. *See id.*

routine maintenance and repair of streets and sidewalks for the safety of travelers have been cited as examples of proprietary functions.[677] On the other hand, "cleaning the street in response to *emergency* weather conditions in order to open the streets to vital public services" constitutes governmental function.[678]

Courts are more likely to determine that the municipality is performing a proprietary function and therefore not immune from tort liability when the municipality failed to repair damaged traffic control devices within a reasonable time.[679] Conversely, if the case involves removal of a traffic sign or signal from an intersection under proper authorization or a claim by the plaintiff that the traffic control system had been negligently planned or designed, public entities typically prevail.[680]

b. Statutory Exceptions to Immunity

Some state statutes explicitly provide exceptions to sovereign immunity for particular actions of municipalities. For example, Cal. Gov. Code § 835 expressly provides:

> "Except as provided by statute, a public entity is liable for injury caused by a dangerous condition of its property if the plaintiff establishes that the property was in a dangerous condition at the time of the injury, that the injury was proximately caused by the dangerous condition, that the dangerous condition created a reasonably foreseeable risk of the kind of injury which was incurred, and that either: (a) A negligent or wrongful act or omission of an employee of the public entity within the scope of his employment created the dangerous condition; or (b) The public entity had actual or constructive notice of the dangerous condition under Section 835.2 a sufficient time prior to the injury to have taken measures to protect against the dangerous condition."

A "dangerous condition" is defined in a different part of the statute as "a condition of property that creates a substantial . . . risk of injury when such property or adjacent property is used with due care in a manner in which it is reasonably foreseeable that it will be used."[681] Moreover, the statute further provides that a dangerous condition is not created merely because of the failure to provide regulatory traffic control signals, stop signs, yield right-of-way signs, or speed restriction signs . . . ."[682]

---

677. *See id.* § 830.4.
678. *See id.*
679. *See id.* § 830.
680. *See id.*
681. CAL. GOV. CODE § 830.
682. *Id. at* § 830.4.

Pennsylvania is another state whose statute expressly provides exceptions to government immunity:

> "(4) Trees, traffic controls and street lighting. — A dangerous condition of trees, traffic signs, lights or other traffic controls, street lights or street lighting systems under the care, custody or control of the local agency, except that the claimant to recover must establish that the dangerous condition created a reasonably foreseeable risk of the kind of injury which was incurred and that the local agency had actual notice or could reasonably be charged with notice under the circumstances of the dangerous condition at a sufficient time prior to the event to have taken measures to protect against the dangerous condition."

These statutes seem to combine common law doctrines of negligence and nuisance by incorporating concepts such as "foreseeability" and "dangerous condition," respectively.

Michigan contains a "highway exception statute," M.C.L. § 691.1402, providing that:

> Each governmental agency having jurisdiction over any highway shall maintain the highway in reasonable repair so that it is reasonably safe and convenient for public travel. . . . The duty of the state and the county road commissions to repair and maintain highways, and the liability therefore, shall extend only to the improved portion of the highway designed for vehicular travel and shall not include sidewalks, crosswalks or any other installation outside of the improved portion of the highway designed for vehicular travel.[683]

As described by the Michigan Supreme Court, "[t]he highway exception waives the absolute immunity of governmental units with regard to defective highways under their jurisdiction."[684] In *Scheurman,* the Michigan Supreme Court held that courts should narrowly construe the highway exception.[685] In that case, the court held that government immunity extended to the installation and maintenance of street light, which did not fall under the highway exception.[686] Concerning traffic control devices, such as traffic signals,[687]

683. M.C.L. § 691.1402.

684. Scheurman v. Department of Transportation, 456 N.W.2d 66, 71 (Mich. 1990)

685. *Id.* ("No action maintained under the highway exception unless it is clearly within the scope and meaning of the statute.")

686. *Id.* at 72.

687. Marchyok v. City of Ann Arbor, 679 N.W.2d 703 (Mich. 2004).

street signs,[688] and railroad crossing warnings,[689] Michigan courts have routinely held that the devices are outside the scope of the highway exception, and thus within the municipality's immunity.[690]

c. Public-Private Partnership for Infrastructure

In many situations, the government entity is not the only party involved in deploying, operating, and maintaining transportation infrastructure. The amount of public funding available to state and local municipalities to spend on highway construction, operation, and maintenance projects "has failed to keep up with the increasing need to invest" in those infrastructures.[691] One of the ways that governmental agencies have devised to increase the availability of funds for building new infrastructures is the utilization of the private sector's capital, expertise, and other resources to design, construct, operate, or maintain public highways.

This kind of public-private partnership ("PPP") might be necessary in building and installing new traffic control devices that are essential for the successful integration of ACV technology. One of the major concerns that the private sector participants would have in a PPP is tort liability. The potential for unlimited tort liability in the absence of protections such as sovereign immunity granted to public entities could become a major burden.

One solution to this problem is state legislation that applies the damage caps of the public sector to the private partner. This kind legislation has been seen in the Mississippi River Bridge PPP project. The Missouri legislature imposed tort liability caps on "any private partner and such private partner's employees, agents, and insured that develops and/or operates the project . . . ."[692]

Other efforts to limit tort liability of private sector partners could be seen with water and electric utility companies. In return for providing water and power companies with near monopolies, they have been subject to greater degrees of government regulation compared to other businesses including the obligation to provide service to all members of the public and rate-setting. Particularly, rate-setting is accomplished through an administra-

688. Nawrocki v. Macomb Cty. Rd. Comm'n, 463 Mich 143, 615 N.W.2d 702 (Mich. 2000).

689. Iovino v. State, 577 N.W.2d 193 (Mich. 1998) (MDOT was not liable for failure to install warning signals at railroad crossing).

690. The above discussion does not relate to the actual operation of motor vehicles by municipalities, such as might occur if municipalities deploy their own AV ridesharing platforms. Such activity would be more likely to constitute a proprietary function in various states, and might even incur common carrier treatment. Indeed, Michigan has a "motor vehicle exception" to government immunity for government owned vehicles. *See* M.C.L. § 691.1405.

691. Edward Fishman, *Major Legal Issues for Highway Public-Private Partnerships*, 51 LEGAL RES. DIG. 3 (2009).

692. MO. REV. STAT. § 227.663.

tive process that considers possible tort liability payments incurred by the utility companies arising from interruption of services.[693] However, despite such administrative processes, the fear that imposing tort liability on the utility companies would result in "unfairly rushing liability"[694] has led to regulators often concluding that it is more desirable to limit liability arising from the interruption of utility services.[695]

Watt v. County of Nassau, 130 A.D.3d 613 (2015) is a good example of how a private company contracting with a local municipality to maintain traffic control device infrastructure could limit its liability through common law. In this case, a private company, Welsbach, was under contract with Nassau County to respond to a malfunctioning traffic light within two hours of receiving notification. On the day of the accident, Welsbach successfully repaired the malfunctioning traffic light within two hours of receiving notification from the Freeport Police Department, but the plaintiff allegedly sustained injuries from an accident because of the malfunctioning traffic light before Welsbach responded. The NY Supreme Court relied on a general rule established by precedents that a "contractual obligation, standing alone, will generally not give rise to tort liability in favor of a third party."[696] The court went on to remind that "[e]xceptions to this general rule exist '(1) where the contracting party, in failing to exercise reasonable care in the performance of [its] duties, launche[s] a force or instrument of harm; (2) here the plaintiff detrimentally relies on the continued performance of the contracting party's duties[;] and (3) where the contracting party has entirely displaced the other party's duty to maintain the premises safely.' "[697] Accordingly, the court decided that Welsbach did not owe the plaintiff a duty of care "since its limited maintenance contract with the County did not displace the County's duty to maintain the traffic signal at the subject intersection in a reasonably safe condition and it did not launch an instrument of harm.

D. *Addressing Market Failures Concerning ACV Deployment Models*

As discussed throughout this report, there are many aspects of ACV deployment that will require significant investment on the part of state or local governments, industry, or vehicle operators. Due to the network effects related to ACVs, many of the societal benefits discussed in Section V.A above can only be achieved if local governments or private parties make spending decisions that they would not make if looking only at their own personal interests. In this way, many of the societal benefits provided by

693. John C. P. Goldberg, *Tort Law: Responsibilities and Redress* 493 (3D ED. 2012).
694. Stephen D. Sugarman, *Why No Duty?*, 61 DEPAUL L. REV. (2012).
695. *See supra* note 23.
696. *Watt*, 130 A.D.3d at 614.
697. *Id.*

ACV represent positive externalities.[698] Accordingly, a form of subsidy or other tool may be required in some instances to incentivize an actor to take action they would not otherwise take in an unregulated market. These tools include liability caps,[699] insurance discounts, tax credits, taxing the disfavored activity, reinsurance backstops for insurance providers, statutory mandates requiring certain behavior, or creating a market (such as access to the vehicular data) that allows profitable business models around the desired activity. This section talks about possible incentives that could be provided in situations presenting externalities.

1. The Deployment, Maintenance, and Operation of Transportation Infrastructure

As discussed above in Section V.B.3, the roadside infrastructure necessary to support a vehicle-to-infrastructure communication network will be expensive (estimated at over $50,000 per traffic signal). Municipalities likely do not possess the funding to deploy that type of infrastructure. Yet, the safety, traffic control/congestion, fuel savings, and other benefits of a connected infrastructure will only be fully realized if municipalities (or some other entities) invest in installing this infrastructure. Accordingly, municipalities will either need to receive significant federal funding[700] or private enterprises will need to be incentivized to invest in the necessary infrastructure.

On one hand, ACV related infrastructure improvements will likely offset some existing transportation expenditures. Because widespread ACV deployment will likely result in fewer vehicles on the road, and more efficient use of existing roads, municipalities will likely spend less in traditional road maintenance. This is because less spacing between vehicles would be needed when computers take over and transcend the "human physiological limits of perception and reaction time," which in turn may lead to a significant increase in the carrying capacity of existing highways.[701] Such improvement may even allow more lanes to fit into the current road space. The resulting

698. *See* B. Taylor, *Positive Externality* (2006), ECONOMICS.FUNDAMENTALFINANCE.COM, http://economics.fundamentalfinance.com/positive-externality.php.

699. As one scholarly article has explained, when examining any liability cap subsidy it is critical to balance the risk management incentives of tort liability with the economic investment incentives of a liability cap. Alexandra Klass, Elizabeth Wilson, *Climate Change and Carbon Sequestration: Assessing Liability Regime for Long-Term Storage,* 58 EMORY L.J. 103 (Fall 2008).

700. Concerning the possibility of further federal funding, NHTSA has said "[s]ome have suggested that system could potentially be better protected if NHTSA had sufficient appropriations to develop the capacity itself to manage the security and communications components of the system, and did not have to rely on contracts/governments with other parties. NHTSA has no current plans to seek additional funding for this purpose." *See* V2V READINESS REPORT, *supra* note 49, at 62.

701. Thomas J. Bamonte, *Autonomous Vehicles: Drivers of Change*, TRANSP., MGMT. & ENGINEERING (July 23, 2013) at 7, http://www.tmemag.com/autonomous-vehicles-drivers-change.

increase in the carrying capacity may lead to less pressure to build new roads and expand existing roads. This is why some say that "investing in infrastructure and organization practices that facilitate the deployment of driverless-vehicle technology may be a better investment than pouring dollars into lane widening and new highways" when the relevant government authorities are putting together long-range capital plans.[702]

On the other hand, because federal funding for transportation is often tied to gas taxes, the more efficient use of vehicles will likely decrease the federal transportation funding available. Recent projections from the Congressional Budget Office estimate that the Highway Trust Fund, which funds road and transit projects and is funded through a gasoline tax, will have an average annual deficit of $15 billion through 2020.[703]

More than likely, however, municipalities will need to attract private partners to invest in the necessary infrastructure to support V2I communications. Given the liability exposure as well as the significant expenses of deployment, operation, and maintenance, such private partners may require some form of subsidy to engage in this partnership. Such as subsidy could be in the form of a liability cap or tax credit.

It is also possible that business models could be created around V2I infrastructure. Such business models could entice private enterprises to invest in infrastructure deployment, operation, and maintenance in order to profit from such activities. While such business models are currently in the research phase,[704] it is possible that these models would involve the data generated from ACVs. Further research needs to be conducted to assess how private enterprises could use ACV data for private purposes consistent with the privacy and security practices implemented in a CV system, such as NHTSA's proposed SCMS. The early state regulations proposed by states such as California and Michigan will also impact how industry can utilize ACV data.

2. Consumer Spending on ACVs

Incentives also might need to be considered to encourage consumers to invest in ACVs earlier than they otherwise would. For example, AVs may be expensive for the average consumer. Additionally, even if AVs are affordably priced, car owners might not consider purchasing an AV until their

---

702. *Id.* at 8.

703. Sandy Manche, *Maintaining the Highway Infrastructure as Alternative Fuel Vehicle Usage Increases,* 7 KY. J. EQUINE, AGRIC. & NAT. RESOUCES L. 515 (2014-1015).

704. Oakland County, Michigan has been a leader in exploring business models around V2I deployment. *See* TECH248, *Grow Your IT/Tech Business Where Innovation Thrives*, https://www.oakgov.com/advantageoakland/media-center/Documents/tech248_2015AttractionBrochure_FINAL.pdf ("OEMs and government transportation agencies are leading the development of a business model for deployment of infrastructure and the next generation automobiles.").

current vehicle becomes sufficiently old or outdated. In the context of V2V connectivity, vehicle operators would likely need to purchase aftermarket V2V devices in order to connect their vehicle to NHTSA's proposed CV system. Because the safety benefits of AVs can only be realized once all, or a substantial portion of, the vehicles on the road are autonomous or connected, incentives may be necessary to encourage consumers to purchase ACV technology.

One possibility is that insurance companies will provide premium discounts that would encourage consumers to invest in ACVs. However, a chicken-and-egg problem may exist concerning the possibility of insurance benefits for ACV technology. In other words, insurance companies may not have the necessary data to offer discounts until they see the safety benefits from significant ACV deployment. In its comments to NHTSA's ANPRM for V2V connectivity, Delphi pointed out the possibility of insurance discounts incentivizing the adoption of aftermarket V2V devices:

> Wherever an economic benefit can be realized through the use of aftermarket devices, a market will materialize. As more new vehicles are deployed awareness of the technology will increase in the public domain. If the technology is received as beneficial and even "cool" by the general public, insurance companies who participate in usage based insurance models will likely study the cost-benefit tradeoffs and incorporate the technology into their aftermarket devices directly to drivers for other more traditional connected features, will also watch the general public's reaction and may incorporate the technology as a means of promoting safer driving.[705]
>
> The effectiveness of the V2V system is predicated in the percentage of vehicles fitted with V2V systems. Owners of non-equipped V2V vehicles would find it difficult to justify the expense of the system and installation if the overall efficacy of system to warn of collision is low. Furthermore, even as the percentage of V2V equipped vehicles rises, the economic reward of investing in a V2V system would be quite difficult for the public to quantify. In order to be able to justify the expense, immediate financial savings must be provided as perhaps a discount on insurance rates from insurers. This would require government collaboration with the insurance industry to estimate the actuarial savings based on the percentage of vehicles equipped. Furthermore, designations by the insurer for "V2V equipped vehicle" would need to [be] established and provided for insurance deduction, much like has been done with airbags.

705. DELPHI AUTOMOTIVE, *Comment to U.S. DOT and NHTSA Docket No. NHTSA-2014-0022 Advanced Notice of Proposed Rulemaking on Vehicle-to-Vehicle Communications*, (Oct. 16, 2014) at 7-8.

Other possibilities include government subsidies such as tax credits. Tax credits have been used to incentivize consumer adoption of electric vehicles.

Of course, if a ridesharing business model prevails, then questions about vehicle operators' willingness to spend on ACV technology may be moot. In 2014, Uber's CEO Travis Kalanick was famously quoted as saying "[w]hen there's no other dude in the car, the cost of taking an Uber anywhere becomes cheaper than owning a vehicle."[706] In such a system, riders would pay a fee per-ride or perhaps a subscription fee to access a TNC's autonomous ride-sharing fleet.

3. Industry Participation in CV Systems

As discussed above in Section III.B.2, there is likely to be a "network manager" that controls the cybersecurity aspects of any CV system. This manager would engage in activities such as issuing security credentials to participating vehicles. NHTSA's current position is that private entities should be the ones to manage and operate this system, not the government. Given the costs and liability risks of participating in this system, private entities (such as car manufacturers) may require incentives to engage in the necessary system management. In particular, the fundint model for the SCMS is unclear. While NHTSA can mandate the SCMS service, it might not be able to require users to pay for the service. During the authors' research, one OEM pointed to Vehicle Identification Numbers ("VIN"), which NHTSA funds through a contract with SAE International[707] and then OEMs receive for free. This source indicated that the VIN funding model might be one example of a funding model for the proposed SCMS. Other incentives could include liability caps or tax credits. Given the sizeable and uncertain risks related to cybersecurity, discussed above in Section III.C, liability protections may be particularly attractive incentives for CV system management participation.

Additionally, as discussed in Section III.D, the availability of cybersecurity insurance will be important to private entities participating in any integrated ACV system. Here, because of the degree of uncertainty and the magnitude of the potential risk associated with cyber-attacks (which are comparable to the risk of terrorist attack), government supported reinsurance backstops, such as under the Terrorism Risk Insurance Act of 2002, may be one vehicle for providing liability protection for CV system participants.[708]

---

706. Casey Newton, *Uber Will Eventually Replace All Its Drivers With Self-Driving Cars,* THE VERGE (May 28, 2014), available at: http://www.theverge.com/2014/5/28/5758734/uber-will-eventually-replace-all-its-drivers-with-self-driving-cars.

707. SAE INT'L, *WMI/VIN Information*, available at: http://www.sae.org/standardsdev/groundvehicle/vin.htm.

708. The Congressional Budget Office examined the Terrorism Risk Insurance Act in January, 2015. *See* CONG. BUDGET OFF., *Federal Reinsurance for Terrorism Risk: An Upda*te,

VI. Conclusion

As discussed above, the authors have presently reached the following conclusions, and will be interested in receiving comments at the University of Michigan Law School Autonomous Vehicles Conference on April 15, 2016:

- Much has changed since NHTSA's Preliminary Statement in 2013, and the federal government will likely take a close look at several issues: (i) ways to promote uniformity in AV deployment regulations; (ii) revised FMVSSs, or a new class of FMVSSs, to address AVs and to permit AV OEMs to self-certify compliance; (iii) liability protections, reinsurance, or other incentives to encourage broad ACV deployment.
- To the extent they make safety conclusions that disfavor a particular track of ACV technology, state and federal regulations may play a gate keeping function in determining which business models come to market.
- Under any model where ACVs come to market, we will likely see an evolution of the contractual relationships within the ACV supply chain, with entities paying closer attention to intellectual property and product liability risk allocation provisions.
- Among the risk to be allocated among ACV providers, cybersecurity presents new risks due to the coordinated and integrated technology involved in any ACV system. Many of the limitations on private causes of action for data breaches, would likely not apply to litigation involving a cyber attack causing property damage or personal injury.
- Any integrated ACV system, such as NHTSA's proposed SCMS will present liability and operational questions for private entities looking to engage in that system. While NHTSA suggested in its 2014 V2V Readiness Report that the risks associated with such a system were manageable by OEMs and other ACV providers, much has changed in the last two years. The assumptions underlying the reasons provided by NHTSA for those risks being manageable have likely evolved for the reasons discussed in this Report.
- Insurance models for ACVs will evolve as the proportion of liability for vehicle accidents shifts from the driver to the technology providers. While most product liability risks associated with ACVs seem to be of the type that the insurance industry can

(Jan. 2015), https://www.cbo.gov/sites/default/files/114th-congress-2015-2016/reports/49866-TRIA.pdf.

price and insure, liability risk for cyber attacks likely poses the risks that are hardest to quantify for insurers.

- Due to the shifting liability from driver to a mesh of coordinated and integrated technology providers, there will be heightened emphasis on the following tort liability models: component part supplier liability, including aftermarket parts; standard-setting organization liability, product liability implications of automated warning devices (assuming cars do not quickly transition to fully autonomous and driverless); and joint liability.
- NHTSA has broad authority to regulate many of the safety aspects of ACVs, such as the performance of in-vehicle safety equipment. However, there are aspects of any likely ACV deployment, such as the transportation infrastructure, where NHTSA's legal authority is less certain. There are aspects of ACV adoption that NHTSA likely cannot mandate.
- While local governments likely enjoy qualified immunity that might shield them from many of the aspects of deploying ACV infrastructure, private parties involved in such deployment would likely not benefit from that immunity.
- Due to the network effects of ACVs, and the positive externalities reflected in many of the societal benefits of ACVs, incentives should be considered to promote various aspects of ACV deployment, including, for example: (i) the deployment, operation, and maintenance of ACV infrastructure; (ii) consumer spending on ACVs that come to market, unless they come to market via ridesharing in which case consumers may be incentivized by the favorable economics of transitioning from a vehicle ownership model; and (iii) industry participation in the management and operation of any CV system, such as the SCMS.