Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 31 | Issue 1 Article 3

Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles

William J. Kohler

Alex Colbert-Taylor

CURRENT LAW AND POTENTIAL LEGAL ISSUES PERTAINING TO AUTOMATED, AUTONOMOUS AND CONNECTED VEHICLES

William J. Kohler[†] & Alex Colbert-Taylor[††]

*As vehicle automation technology advances toward vehicle autonomy and vehicles become increasingly connected, the legal community anticipates substantial legal issues and developments pertaining to such technology. The federal government has the power to regulate the design, sale, and use of autonomous vehicles, has expressed interest in doing so, and has provided recommendations for state-level regulations. A few states have recently established laws in an attempt to ensure the safe operation of autonomous vehicles. Moreover, the use and collection of locational and other personal data generated by and required for the effective operation of a network of connected autonomous vehicles presents significant privacy concerns. Such concerns must be balanced against the utility of the generated information in ensuring the safe and efficient operation of autonomous vehicle networks and the interests of carmakers and other industries involved in the commercial use of this data. Another concern relating to automation advances is the threat of cyberhacking and cyberterrorism. All of the above factors play a role in the timing of automated vehicle technologies' implementation.**

TABLE OF CONTENTS

INTRODUCTION 100
I. BACKGROUND INFORMATION REGARDING THE TECHNOLOGY AND FUNCTIONALITY OF AUTOMATED, AUTONOMOUS AND CONNECTED VEHICLES SYSTEMS .102
II. EXISTING FEDERAL LAW AND POLICY RELATING TO AUTONOMOUS VEHICLES 105

---

† Chief Legal Officer and Corporate Secretary at Dura Automotive Systems, LLC.

†† J.D. Student at University of Michigan Law School. The authors are grateful for the contributions of University of Michigan Law student Julia Muhlnickel with respect to state laws pertaining to autonomous vehicles.

* Abstract provided by Azadeh Morrison, J.D. Candidate at Santa Clara School of Law and Associate on the Santa Clara High Tech. Law Journal.

III. NHTSA'S EXPRESSED INTEREST IN REGULATING AUTOMATED VEHICLES 108
IV. STATE LAW AND AUTONOMOUS VEHICLES 111
A. Enacted Legislation 112
1. Nevada 112
2. Florida 114
3. California 115
4. District of Columbia 116
5. Michigan 117
B. Failed Legislation 118
C. Concluding Thoughts on State Legislation 120
V. PRIVACY AND DATA USE 120
VI. SECURITY, CYBERATTACKS, AND TERRORISM 132
VII. REGULATORY OPTIONS, COMMERCIAL PROSPECTS AND THE POTENTIAL PACE OF CHANGE 134

INTRODUCTION

Vehicle automation technologies that modestly manipulate a vehicle's direction and speed without driver involvement have already been introduced into the market and are becoming increasingly commonplace. Different than mere warning systems, such as those that sense and warn a driver of fatigue or unsafe speed while approaching a turn, automated vehicle technologies assume a limited level of command over vehicle performance. Examples of currently available automated vehicle technologies include front crash prevention systems, adaptive cruise control, lane departure prevention systems, blind spot detection, park assist, backover prevention, and antilock brakes.[1]

The commercial introduction and consumer acceptance of such vehicle automation technologies indicate the potential for autonomous vehicles that assume full command of vehicle operation except under specific limited circumstances. Although autonomous vehicles have not yet been offered for mainstream sale, development of autonomous vehicle technologies has advanced rapidly. Google has been a forerunner in developing and testing autonomous vehicle technologies,[2] while traditional automotive manufacturers have placed an emphasis on limited automated vehicle technologies and their current

1. *See Crash Avoidance Technologies*, INS. INST. FOR HIGHWAY SAFETY, http://www.iihs.org/iihs/topics/t/crash-avoidance-technologies/topicoverview (last visited Jan. 30, 2015).

2. *See* Liz Gannes, *Google's New Self-Driving Car Ditches the Steering Wheel*, RE/CODE (May 27, 2014, 6:59 PM PDT), http://recode.net/2014/05/27/googles-new-self-driving-car-ditches-the-steering-wheel/.

determination that drivers must continue to be engaged in driving vehicles.[3]

Technological advances in vehicle automation and autonomy will lead to significant legal developments. This article presents the current state of applicable law and reviews significant legal issues pertaining to automated and autonomous vehicles. In addition, because many vehicle automation and vehicle autonomy technologies are not feasible without electronic communications between vehicles or between vehicles and infrastructure—vehicle "connectivity"—this article also reviews data privacy issues relating to vehicle connectivity.

In Part I, we provide a description of automated and autonomous vehicle technologies, as well as the parties involved in manufacturing and operating such technologies that establishes terminology and a framework for understanding the legal issues reviewed in this article.[4] Part II addresses the federal government's power to regulate the design, sale, and use of autonomous vehicles.[5] We discuss both the potential extent of this regulatory power under the United States Constitution and the federal agencies that may regulate areas related to autonomous vehicles.[6] In Part III, we discuss the National Highway Transportation Safety Administration's (NHTSA) expressed interest in regulating autonomous vehicles, what this regulation might look like, and NHTSA's recommendations regarding state-level laws and regulations.[7] In Part IV, we discuss the established autonomous vehicle laws of Nevada, California, Florida, the District of Columbia and Michigan,[8] as well as failed legislative attempts to enact similar laws in other states.[9] In Part V, we discuss legal issues related to the use and collection of locational and other personal data likely to be generated by and necessary for the operation of a network of connected autonomous motor vehicles.[10] These issues include the balancing of privacy concerns against the utility of this information in ensuring the safe and efficient operation of the autonomous vehicle network and the

3. *See* Jarah Jacobsson Purewal, *Toyota and Lexus Showcase Autonomous Research Vehicle*, TECHHIVE (Jan. 7, 2013, 11:01 AM), http://www.techhive.com/article/2023858/toyota-and-lexus-showcase-autonomous-research-vehicle.html; *GM Studying Operator Behavior in Self-Driving Vehicles*, GM (June 20, 2012), http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2012/Jun/0620_humanfactors.html.

4. *See* discussion *infra* Part I.

5. *See* discussion *infra* Part II.

6. *See* discussion *infra* Part II.

7. *See* discussion *infra* Part III.

8. *See* discussion *infra* Part IV.A.1–5.

9. *See infra* Part IV.B.

10. *See infra* Part V.

interests of carmakers and other industries involved in the technology in the commercial use of this data.[11] In Part VI, we address the threat that cyberhacking poses to the autonomous vehicles and related technologies.[12] In Part VII, we discuss the manner in which various factors, including regulatory efforts and automobile manufacturers' willingness to commercialize technologies, may influence the timing of implementation of automated vehicle technologies.[13]

I. BACKGROUND INFORMATION REGARDING THE TECHNOLOGY AND FUNCTIONALITY OF AUTOMATED, AUTONOMOUS AND CONNECTED VEHICLES SYSTEMS

Some additional background information regarding automated and autonomous vehicle technologies will serve as a useful foundation for understanding resulting legal issues. In May 2013, the NHTSA issued a *Preliminary Statement of Policy Concerning Automated Vehicles*, a non-binding document in which the agency described the potential benefits of automated vehicle systems and provided recommendations for initial state regulation of automated vehicles.[14] In this document, the NHTSA lays out a useful five-tier framework defining five relative degrees of automation in a given vehicle. These five levels are:

- Level 0 (No Automation): "[D]river 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."[15]
- Level 1 (Function-Specific Automation): Examples include dynamic emergency braking, lane maintenance, and similar technologies that do not "replace driver vigilance."[16]
- Level 2 (Combined-Function Automation): Where multiple automation technologies working together (for instance, a combination of adaptive cruise-control, automatic emergency breaking, and lane

11. *See infra* Part V.

12. *See infra* Part VI.

13. *See infra* Part VII.

14. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., PRELIMINARY STATEMENT OF POLICY CONCERNING AUTOMATED VEHICLES 1 (2013) [hereinafter PRELIMINARY STATEMENT], *available at* http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf; Press Release, NHTSA 14-13, *U.S. Department of Transportation Releases Policy on Automated Vehicle Development*, NHTSA (May 30, 2013), http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development.

15. PRELIMINARY STATEMENT, *supra* note 14, at 4.

16. *Id.*

maintenance) under specific operating conditions, allow for the driver to have "his or her hands off the steering wheel AND foot off pedal at the same time."[17]

- Level 3 (Limited Self-Driving Automation): Allows for total autonomous control of the vehicle except in limited circumstances where the driver needs to assume control, such as in construction zones or where the system detects that its map data may be inaccurate, and it is up to the "vehicle to monitor for changes in those conditions requiring transition back to driver control."[18]
- Level 4 (Full Self-Driving Automation): Complete automation requiring no human participation beyond setting the destination.[19]

NHTSA describes Level 3 as the highest level of automation currently being tested and states that it is not aware of any Level 4 automated vehicle systems in existence.[20] However, Google's recently announced second-generation automated car prototype, which has no steering wheel, appears to belong to this category.[21]

The types of technologies necessary for creating any level of autonomous vehicle can be categorized as either a sensor- or a connectivity-based solution.[22] Sensor-based solutions, also referred to as Advanced Driver Assist Systems, "use a combination of advanced sensors, such as stereo cameras and long- and short-range RADAR, combined with actuators, control units, and integrating software, to enable cars to monitor and respond to their surroundings."[23] In contrast, connected-vehicle solutions "use wireless technologies to communicate in real time from vehicle to vehicle (V2V) and from vehicle to infrastructure (V2I), and vice versa."[24] The authors of the present article believe that the development of dependable technology within both of these categories, and the convergence of these categories, will be a necessary precursor to the commercial introduction of substantially autonomous vehicles.[25] At those degrees of technological

17. *Id.* at 5.

18. *Id.*

19. *Id.*

20. *Id.* at 5 n.1.

21. *See* Gannes, *supra* note 2 (as the new Google car lacks any way for the occupant to assume control of the vehicle, it seems necessarily to be a Level 4 vehicle).

22. KPMG & CTR. FOR AUTO. RESEARCH, SELF-DRIVING CARS: THE NEXT REVOLUTION 10 (2012), *available at* http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/self-driving-cars-next-revolution.pdf.

23. *Id.*

24. *Id.* at 12.

25. *See id.* at 25 ("Eventually, convergence will lead to vehicles that can drive themselves and operate autonomously. . .[C]onvergence also implies a multitude of redundant systems that

advancement—Level 3 and Level 4—the safe operation of vehicles without drivers is dependent on the reliable functioning of sensors detecting risks near a vehicle and the accurate and timely receipt by, and provision to, multiple vehicles of information about those vehicles and their respective environments.[26]

In theory, as autonomous vehicle systems and their commercial introduction advance from Level 2 to Level 3 to Level 4, the number and types of participants involved in providing technology and data will change and increase. At Level 3, traditional vehicle manufacturers will, as they have already begun doing, create sensor-based solutions or obtain them from third parties for incorporation into vehicles. To advance to Levels 3 and 4, they must also create or obtain from third-parties V2V and V2I technologies that are compatible across the full spectrum of vehicles, likely necessary to comply with yet-to-be-designated governmental or industry association standards.[27] In addition, a central party—akin to air traffic control—might provide and perhaps staff infrastructure, such as data hubs or traffic control stations, that is necessary to ensure the timely communication of information about vehicles and their environments.

The timing of technology and its commercial introduction is uncertain. However, some analysts have attempted to forecast likely timelines. For example, Morgan Stanley anticipates further penetration of Level 1 vehicles over the next three years, the introduction of Level 2 vehicles in three to five years, of Level 3 vehicles in five to ten years, and of Level 4 vehicles in twenty years or more.[28]

---

can substitute for one another and yield safe operation even when failures occur. This crash less future would eliminate the injuries and property damage associated with vehicle crashes and save more than 30,000 lives a year.").

26. *Id.*

27. *See id.* at 15 ("The regime for connected vehicles is fairly mature. . .but additional standards will be needed to ensure full interoperability. A mandate, if it occurs, should provide momentum to develop them."); PRELIMINARY STATEMENT, *supra* note 14, at 6 ("NHTSA's research will inform agency policy decisions, assist in developing an overall set of requirements and standards for automated vehicles."); *see also* NHTSA V2V Security Credential Management System ANPRM, FR Doc. No. 2014–24482, 79 Fed. Reg. 61927 (Oct. 14, 2014) (announcing advance notice of proposed rulemaking and seeking comment on developing a standardized security credential management system for V2V applications).

28. RAVI SHANKER ET AL, MORGAN STANLEY RESEARCH, AUTONOMOUS CARS: SELF-DRIVING THE NEW AUTO INDUSTRY PARADIGM 39 (2013).

II. EXISTING FEDERAL LAW AND POLICY RELATING TO AUTONOMOUS VEHICLES

As of the time of this writing, the U.S. federal government has not attempted to regulate autonomous motor vehicles as such, though various administrative agencies, as well as individual legislators, have signaled their intent to involve themselves in the area. There is no doubt that the federal government possesses substantial authority to regulate the design and operation of vehicles used on public roadways and legislation already exists that will allow certain federal administrative agencies to regulate many significant aspects of autonomous vehicle control technology.

Federal agencies already involved with autonomous vehicle control technology include the U.S. Department of Transportation (DOT), which oversees the NHTSA and hosts the Intelligent Transportation Systems Joint Program Office (ITS JPO). The NHTSA, established by the Highway Safety Act of 1970,[29] possesses regulatory authority to, *inter alia*, develop and enforce safety standards for new motor vehicles[30] and aftermarket replacement or improvement car components or equipment.[31] An example of relevant rulemaking by NTSHA are its recent changes to rules that transform the Agency's long-standing recommendation that all new vehicles sold in the United States include an event data recorder (EDR) into a mandate.[32] EDRs, as currently used, are functionally analogous to an airplane's black box; recording and archiving for relative short periods of time data from the vehicle's various electronic control units for analysis in the case of an accident or malfunction.[33] The data typically collected include information concerning: "vehicle speed; whether the brake was activated in the moments before a crash; crash forces at the moment of impact; information about the state of the engine throttle; air bag deployment timing and air bag readiness prior to the crash; and whether the vehicle occupant's seat belt was buckled."[34] Most newer vehicles

29. Pub. L. No. 91-605, § 202(a), 84 Stat. 1739, 1739–40 (1970) (codified as amended at 49 U.S.C. § 105).

30. *See* 49 U.S.C. §§ 30101–33118 (2013).

31. *See id.* § 30102 (a)(7)(B).

32. NHTSA Event Data Recorders Rules, 49 C.F.R. pt. 563 (2013).

33. *See* 49 C.F.R. § 563.5 (defining "event data recorder"); Press Release, NHTSA 46-10, *U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety*, NHTSA (Dec. 7, 2012) http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Safety [hereinafter *EDR Press Release*].

34. *EDR Press Release*, *supra* note 33; *see also* 49 C.F.R. § 563.7 (data elements).

are already equipped with EDRs, some of which can wirelessly communicate with emergency response centers in the event of a crash.[35] The potential role of an EDR as a site where data from all of a vehicle's computers might be aggregated and communicated to an external network makes EDRs a potentially central piece of technological hardware to watch with legal considerations, such as data privacy, in mind.

The ITS JPO, a branch of the DOT within its Office of the Assistance Secretary for Research and Technology, is responsible for "[c]onducting an ongoing intelligent transportation system program to research, develop, and operationally test intelligent transportation systems and to provide technical assistance in the nationwide application."[36] Currently, the ITS JPO is engaged in the development and promulgation of intelligent transportation standards that will likely serve as the foundation of V2V and V2I networks for connected and autonomous vehicle technologies in the future.[37] One example of ITS IPO's efforts has been its role in developing standards for wireless communication for connected vehicles, including technologies using the reserved 5.9GHz Dedicated Short Range Communications (DSRC) bandwidth range.[38] DSRC was specifically reserved by the Federal Communication Commission (FCC) for enabling wireless communication between multiple vehicles on the road and between vehicles and roadside infrastructure.[39] Envisioned as a cornerstone of connected vehicle technologies, relatively few licenses have been issued to make use of this bandwidth.[40] DSRC applications are in their infancy, but it is likely that this bandwidth range will become essential

35. Cheryl Dancey Balough & Richard C. Balough, *Cyberterrorism On Wheels: Are Today's Cars Vulnerable to Attack*, BUS. L. TODAY, Nov. 2013, at 6, *available at* http://www.americanbar.org/content/dam/aba/publications/blt/2013/11/cyberterrorism-cars-201311.authcheckdam.pdf.

36. Moving Ahead for Progress in the 21st Century (MAP–21) Act, Pub. L. No. 12-141, § 53003, 126 Stat. 405 (2012); *About ITS*, ITS JPO, http://www.its.dot.gov/its_jpo.htm (last updated Jan. 22, 2015 9:50 AM).

37. *About the ITS Research Program*, ITS JPO, http://www.its.dot.gov/its_program/about_its.htm (last updated Dec. 11, 2014, 3:57 PM).

38. *See* FCC Rules to Allocate the 5.850-5.925 GHz Band to the Mobile Serv. for DSRC of Intelligent Transp. Servs., No. 99-305, 14 FCC Rcd. 18221 (1999) (report and order) [hereinafter *DSRC Order*].

39. *Id.*; *see also* Robert B. Kelly & Mark D. Johnson, *Defining a Stable, Protected and Secure Spectrum Environment for Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1271, 1281–82 (2012).

40. Kelly & Johnson, *supra* note 39.

to connected and autonomous vehicles as these technologies become prevalent.[41]

Beyond these transportation-oriented federal agencies, agencies such as the FCC and the Federal Trade Commission (FTC) will be involved in regulating aspects or applications of the technology—the former in administrating wireless communication standards used by autonomous vehicles, and the latter in regulating the use of consumer data, as they have done or proposed doing in the related fields.[42] Elsewhere in the government, the Department of Defense has been a prominent supporter of autonomous motor vehicles, with Defense Advanced Research Programs Agency hosting multiple competitions, such as the 2007 Urban Challenge in Victorville, California, to encourage the development and public visibility of this technology.[43]

It is almost inevitable that arrival at Level 4 will be accompanied by an extensive regulatory regime that will ensure the standardization, safety, and security of autonomous vehicles and their underlying technologies. It is clear that, for instance, in the absence of such a regime, there would be no guarantee of the interoperability of the V2V and V2I systems used in different vehicles, leading at least to significantly less efficient automated roadway than the smooth-flowing intersections, intelligently managed traffic patterns, and close-packed platoons described by industry technologists.[44] Beyond these inefficiencies, one can easily imagine that incompatible V2V and V2I systems operating on the same communication channels could interfere with each other, leading to potentially catastrophic accidents.

---

41. *See generally* NHTSA V2V Security Credential Management System ANPRM, FR Doc. No. 2014–24482, 79 Fed. Reg. 61927 (Oct. 14, 2014) (requesting input from the public on future rulemaking in reference to secure V2V communication systems using the DSRC spectrum).

42. *See DSRC Order*, *supra* note 38; FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

43. *See Urban Challenge*, DARPA, http://archive.darpa.mil/grandchallenge/ (last visited Jan. 1, 2015).

44. *See, e.g.*, Emily Badger, *What Intersections Would Look Like in a World of Driverless Cars*, CITYLAB (Mar. 1, 2012), http://www.citylab.com/tech/2012/03/what-intersections-would-look-world-driverless-cars/1377/; Sebastian Thrun, *Leave the Driving to the Car, and Reap Benefits in Safety and Mobility*, N.Y. TIMES, Dec. 6, 2011, at D4 (describes platooning).

III. NHTSA'S EXPRESSED INTEREST IN REGULATING AUTOMATED VEHICLES

NHTSA is the federal agency that has thus far been the most visible and active in promoting automated vehicles. It has announced its interest in regulating autonomous vehicles, as well as its willingness to advance and support the wide adoption of related technology. As its name suggests, the NHTSA's essential function is to maximize highway safety. The Agency describes its mission as being "to save lives, prevent injuries, and reduce economic costs due to road traffic crashes,"[45] and as to "achiev[e] the highest standards of excellence in motor vehicle and highway safety."[46] The NHTSA is also responsible for setting Federal Motor Vehicle Safety Standards, and therefore possesses broad authority to regulate the design and use of future autonomous motor vehicles,[47] including the power to preempt contrary state regulation.[48]

Insight into NHTSA's internal concerns about the issues raised by autonomous vehicles and potential regulatory solutions for overcoming these issues can be gleaned from the Agency's *Preliminary Statement*.[49] Further information can be found in *The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicle*s, an article authored by Stephen P. Wood, NHTSA's Assistant Chief Counsel for Vehicle Standards and Harmonization, and three NHTSA and DOT Attorney–Advisors.[50]

---

45. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., THIS IS NHTSA 2 (2006), *available at* http://www.nhtsa.gov/DOT/NHTSA/reports/810552.pdf.

46. *About NHTSA*, NHTSA, http://www.nhtsa.gov/About (lasted visited Mar. 23, 2014).

47. Stephen P. Wood et al., *The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles*, 52 SANTA CLARA L. REV. 1423, 1441 (2012). "The views expressed in that article fairly encompass the agency's views of its regulatory authority." NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., REP. NO. DOT HS 812 014, VEHICLE-TO-VEHICLE COMMUNICATIONS: READINESS OF V2V TECHNOLOGY FOR APPLICATION 33 n.40 (2014) [hereinafter V2V READINESS REPORT].

48. *See* 49 U.S.C. § 30103(b)(1) (2013) (expressly preempting State laws that apply to the same aspect of performance of a motor vehicle or motor vehicle equipment as an FMVSS issued under this chapter); *see also*, Catherine M. Sharkey, *Inside Agency Preemption*, 110 MICH. L. REV. 521, 545 (2012) (describing NTSHA's broad power to preempt state law).

49. *See generally* PRELIMINARY STATEMENT, *supra* note 14.

50. Wood et al., *supra* note 47, at 1423. Note that the article specifically disclaims any relationship between its opinions and conclusions and the position of NHTSA. *Id.* at 1423 n.1. Wood presented that paper at the Santa Clara Law's spring 2012 symposium on autonomous vehicles. Symposium, *Legal Aspects of Autonomous Driving*, 52 SANTA CLARA L. REV. 1145 (2012). The papers presented at this conference and published in Volume 52 of the Santa Clara Law Review are a particularly rich source for perspectives on the law of autonomous vehicles.

In its *Preliminary Statement*, the NHTSA recognizes many potential societal and economic benefits that may arise from autonomous vehicles, from reduced greenhouse gas emissions to enhanced access for disabled people.[51] The Agency was careful to emphasize that its mission is safety-oriented, and that its purpose in involving itself early on in the process of developing and regulating autonomous vehicles is above all because the technology has "the potential to reduce significantly the many thousands of fatalities and injuries that occur each year as a result of motor vehicle crashes."[52] NHTSA suggested that "[p]reventing significant numbers of crashes will, in addition to relieving the enormous emotional toll on families, also greatly reduce the enormous related societal costs—lives lost, hospital stays, days of work missed, and property damage—that total in the hundreds of billions of dollars each year."[53]

Although NTSHA does not appear ready to issue its own nationwide regulations specifically relating to autonomous vehicles, it made several recommendations for how state governments should regulate the testing and use of autonomous vehicles. The Agency recommended that states wishing to allow testing should require specific driver's license endorsements for operators of autonomous vehicles, and that a licensed operator should be required to be seated in the driver's seat, with the ability to immediately assume control over the vehicle during all testing on public roads. It recommends that states require businesses seeking to test an autonomous vehicle certify that the vehicle has already been operated for some unspecified number of miles in self-driving mode, and in traffic and environmental conditions similar to those in which it would be tested on public roads. Data from these earlier tests should be submitted to the state. The NHTSA also recommends that state regulatory bodies require testing businesses to submit plans demonstrating their efforts to minimize risk to others. The Agency also suggests that states require businesses that test autonomous vehicles report information about crashes or near-crashes involving the vehicles, and also any instances in which the vehicles prompt their human operators to assume control because of the failure of the automated system to function properly.[54]

At this still-early stage in the development of autonomous vehicles, the NHTSA remains deferential to individual States insofar

51. *See* PRELIMINARY STATEMENT, *supra* note 14, at 1.
52. *Id.*
53. *Id.*
54. *Id.* at 12–14.

as the States seeking to regulate the testing of prototype vehicles on public roads, "believ[ing] that states are well suited to address issues such as licensing, driver training, and conditions for operation related to specific types of vehicles."[55] However, the Agency has expressed its preference that States not permit the operation of autonomous motor vehicles for any purpose other than testing.[56] Among the States that have passed statutes regulating the testing of autonomous vehicles, Michigan is the only state that has explicitly banned their use in circumstances other than testing and research.[57]

It is interesting to note that although no federal law or regulation currently is explicit in prohibiting the use of autonomous vehicles outside of the context of testing,[58] the NTSHA's recommendations appear to presume that operating autonomous vehicles on public roads is illegal in the absence of either state or federal laws specifically authorizing their use.[59] In contrast, legal scholar Bryant Walker Smith views the use of autonomous vehicles on public roads and highways as probably already legal, precisely because they are not explicitly prohibited in the United States under the Geneva Convention, Federal Motor Vehicle Standards, or state laws.[60] Smith's theory is based on a statutory reading to the effect that everything is permitted unless explicitly prohibited.[61] However, because NHTSA has the express power to conduct investigations into safety defects and can recall and remedy of motor vehicles and motor vehicle equipment determined to have a safety defect,[62] it is not a stretch to imagine that NHTSA would promptly exercise this power if autonomous vehicles were prematurely introduced onto American roadways. Therefore, NHTSA may exercise its powers as, effectively, a prohibition, at least if it can reasonably find that the use of autonomous vehicles presents some safety risk. Such a

55. *Id.* at 10.

56. *Id.*

57. *See* MICH. COMP. LAWS § 257.663 (2014) ("Except as otherwise provided in section 665, a person shall not operate an automated motor vehicle upon a highway or street in automatic mode."); § 257.665 (exemptions for research or testing).

58. *See* Bryant Walker Smith, *Automated Vehicles are Probably Legal in the United States*, 1 TEX. A&M L. REV. 411, 412–13 (2014).

59. *See* PRELIMINARY STATEMENT *supra* note 14, at 10–11 (The recommendation that states not act to "permit operation of self-driving vehicles for purposes other than testing" implies that without such permission the use of autonomous vehicles would be unlawful).

60. *See* Smith, *supra* note 58.

61. *Id.* at 413.

62. 49 U.S.C. § 30166(b) (2013) (authority to conduct inspections or investigations); § 30120 (remedies for defects or noncompliance): § 30118 (notification of defects or noncompliance). *See generally* Stephen P. Wood et al., *supra* note 47.

risk could probably be found in the mere proliferation of non-standardized and potentially incompatible autonomous technologies operating simultaneously.

In addition, Smith attempts to demonstrate how each prevailing law (the Geneva Convention, federal law, and state law) does not disallow operation of autonomous vehicles, substantially relying on the concept that, even though such laws require or assume that drivers must operate vehicles, they do not necessarily require that a driver be human. He states: "'Driver' is a broad concept—so much so that, at least textually, even nonhuman persons can be drivers."[63] We, however, believe that the foundation of each regime discussed by Smith is the material assumption that a human driver—not driverless technology or a fictitious legal person that might be deemed a driver—is operating a vehicle being driven on public roadways.

Hypothetically, were Google or another company to start selling autonomous car conversion kits right now, enabling Smith's interpretations to be tested in court, we believe it more likely that a judge would endorse a more conservative textual reading of these laws. We believe that, because these laws were written well before any serious discussion of the possibility of autonomous vehicles, where they refer to a "driver" must be interpreted according to their plain meaning in light of usage at the time they were adopted. The courts are likely to find, then, that for a vehicle to be legal in the current regime, it must have a human operator, and therefore they will probably accept NHTSA's apparent position that states or other governments must specifically authorize automated vehicles to be driven on highways.

IV. STATE LAW AND AUTONOMOUS VEHICLES

The NHTSA recommends that states not develop detailed safety regulations over autonomous vehicles, citing the "rapid evolution and wide variations in self-driving technologies" as making this impractical.[64] Instead, the Agency recommends that states enforce four basic principles: (1) ensure that "the process for transitioning from self-driving mode to driver control is safe, simple, and timely"; (2) "self-driving test vehicles should have the capability of detecting, recording, and informing the driver that the system of automated technologies has malfunctioned"; (3) "installation and operation of any self-driving vehicle technologies does not disable any federally required safety features or systems"; and (4) "self-driving test vehicles record

63. *See* Smith, *supra* note 58, at 463.

64. *See* PRELIMINARY STATEMENT, *supra* note 14, at 12–13.

information about the status of the automated control technologies in the event of a crash or loss of vehicle control."[65] At the time that NHTSA issued its *Preliminary Statement*, three States had already enacted autonomous vehicle legislation legalizing the operation of autonomous vehicles on public roads for the purpose of testing. These laws are substantially consistent with NHTSA's state policy recommendations.

A. Enacted Legislation

We will now look in detail at the recently enacted state legislation authorizing the testing of autonomous vehicles.

1. Nevada

In June 2011, Nevada became the first State to authorize the operation of automated vehicles on public roads.[66] Nevada defines autonomous vehicle as one equipped with autonomous technology that which has the capability to drive the motor vehicle without the active control or monitoring of a human operator.[67] Before testing the vehicle on state highways, the operator must submit proof of insurance for $5,000,000 or post a surety bond or other form of security for the same amount.[68] The car also must be equipped with several safety measures, including a means of easily engaging and disengaging the autonomous technology by the human operator, a visual indicator inside the vehicle that indicates when the autonomous technology is in operation, and a mechanism of alerting the human operator to take control if the autonomous technology fails.[69] Upon approval by the state, the tester will be licensed to operate the vehicle only in specified geographic zones, but may apply to test in additional zones.[70] When testing, the human operator must be seated in a position that allows the operator to take immediate control of the vehicle if needed, monitoring the autonomous technology, and capable of immediately taking over

65. *Id.* at 13–14.

66. Act of June 16, 2011, ch. 472, §§ 2, 8, [2011] Nev. Stat. 2,873, 2,876 (codified as amended at NEV. REV. STAT. §§ 482A.010–.200 (2014)); Adopted Regulation Providing for the Operation of Autonomous Vehicles, 174 Nev. Reg. Admin. Regs. R084-11 (Nev. Dep't of Motor Vehicles Feb. 15, 2012) (codified as amended at NEV. ADMIN. CODE ch. 482A (2014)).

67. NEV. REV. STAT. §§ 482A.025, .030 (2014) (defining "autonomous technology" and "autonomous vehicle"); NEV. ADMIN. CODE § 482A.010 (2014) (interpreting definition of autonomous technology to exclude any vehicle unable to perform the operations of driving without active control or monitoring of a human person).

68. NEV. REV. STAT. § 482A.060.

69. *Id.* § 482A.080(2)(a)–(c).

70. *Id.* § 482A.120.

manual control of the vehicle in case of failure of the automated technology.[71] Nevada also releases the manufacturer of the vehicle from liability resulting from the third party conversion of the vehicle to an autonomous vehicle.[72]

Nevada was also the first state to require its motor vehicle department to propose regulations for autonomous vehicles by a certain date.[73] Nevada adopted its department's proposed regulations in February 2012.[74] The regulations require a special driver's license certification and license plates, along with pre-operation certifications by the manufacturer that the vehicle complies with safety regulations, including an electronic data recorder, separate from the NHTSA-mandated EDR, that stores information about the condition of autonomous vehicle system's state for at least thirty seconds prior to any accident.[75] Nevada requires a cash deposit or surety deposit before issuing a license to test autonomous vehicles, in the amount of $5,000,000.[76] A certificate will be issued to the licensee that specifies the geographic regions where a vehicle is allowed to operate.[77] Nevada's regulations also require the presence of a second human in the vehicle, also trained in the operation of the vehicle and its capabilities and limitations, which "shall each actively monitor for any aberration in the functioning of the autonomous vehicle while it is engaged."[78]

The State also instituted similar certification requirements before the vehicles may be sold to the public.[79] Either a manufacturer or licensed technology certification facility must issue the certificate of compliance in order for the vehicle to be sold, as well as a certification that the driver is able to operate the technology.[80] By allowing independent facilities to certify autonomous vehicles, Nevada is creating the opportunity for a market of privately operated certification facilities. Since this requirement is only for vehicles sold with

71. *Id.* § 482A.070.

72. *Id.* § 482A.090.

73. Act of June 16, 2011, ch. 472, § 12, [2011] Nev. Stat. 2873, 2877 (2011).

74. Regulation Providing for the Operation of Autonomous Vehicles, 174 Nev. Reg. Admin. Regs. R084-11 (Nev. Dep't of Motor Vehicles Feb. 15, 2012) (codified as amended at NEV. ADMIN. CODE ch. 482A (2014)).

75. NEV. ADMIN. CODE §§ 482A.040, .050, .110 (2014).

76. NEV. REV. STAT. § 482A.060 (2014).

77. NEV. ADMIN. CODE § 482A.120(1).

78. *Id.* § 482A.130.

79. *Id.* § 482A.190.

80. *Id.*

autonomous technology, it readies Nevada for the commercialization of autonomous vehicles. While an operator who wishes to drive an autonomous vehicle for non-testing purposes still must obtain the vehicle, certificate of compliance, endorsement on his driver's license, and private insurance, Nevada's regulations allow these processes to begin.

2. Florida

Florida, in April 2012, enacted legislation containing provisions that were similar or identical to Nevada law regarding autonomous vehicles.[81] These provisions are the definition of an autonomous vehicle,[82] the required safety measures for use of the automated technology in the vehicle,[83] a $5,000,000 insurance requirement,[84] and the release of liability for vehicle manufacturers.[85] Florida law requires a human operator who must be a licensed driver affiliated with the company conducting the test, with no special certifications required. Although Florida defines operator to include someone who causes the autonomous technology to engage, regardless of whether or not that person is present in the vehicle while it operates in autonomous mode, a human operator must still be present in the vehicle during testing on State roads.[86] The legislation includes the statement that "the Legislature finds that the state does not prohibit or specifically regulate the testing or operation of autonomous technology in motor vehicles on public roads."[87] The statute required Florida's Department of Highway Safety and Motor Vehicles to prepare a report making additional recommendations for legislative or regulatory action by February 2014.[88] The document the Florida Department of Highway Safety and Motor Vehicles eventually published compares its interpretation of the requirements of the Florida law with the NHTSA recommendations and the laws passed by Florida, Michigan, California, and their implementing regulations.[89] It concludes that the Florida legislation,

81. Vehicles with Autonomous Technology Act, ch. 2012-111, [2012] Fla. Laws 1223.

82. Florida Uniform Traffic Control Law, FLA. STAT. § 316.003(90) (2014).

83. *Id.* § 319.145.

84. *Id.* § 316.86(1).

85. *Id.* § 316.86(2).

86. *Id.* §§ 316.85(2), 316.86(1).

87. Vehicles with Autonomous Technology Act, ch. 2012-111, § 1(2), [2012] Fla. Laws 1223.

88. *Id.* § 5(3).

89. JULIUS L. JONES, FLA. DEP'T OF HIGH. SAFETY AND MOTOR VEH., HSMV NO. 13-008, AUTONOMOUS VEHICLE REPORT (2014), *available at* http://www.flhsmv.gov/html/HSMV AutonomousVehicleReport2014.pdf.

interpreted as setting very minimal barriers to parties interested in testing vehicles, needed no immediate changes—"In order to encourage innovation and foster a positive business environment toward that end, the Department proposes no changes to existing Florida laws and rules at this time."[90]

3. California

The legislation enacted in California uses the language of Nevada and Florida to define autonomous vehicle and the vehicle's operator, but with additional specifications.[91] California defines the manufacturer of an autonomous vehicle as the one who equips the vehicle with autonomous technology, whether or not that person is the original physical manufacturer of the underlying vehicle.[92] The California statute also does not release the original vehicle manufacturer from liability resulting from a third party installation of autonomous technology, nor does it designate the third party installer as liable for defects. California permits testing of automated vehicles on public roads if the operator is an employee of the testing company, is seated in the driver's seat monitoring the operations of the autonomous technology, is capable of taking over manual operation of the vehicle, and the testing company has an insurance policy in the amount of $5,000,000.[93]

The vehicle must also contain a separate device that stores autonomous technology sensor data for thirty seconds before a crash while operating in autonomous mode, which must not be destroyed for three years after the collision.[94] California does not suggest who the owner of that data is. Even though the capture of information surrounding autonomous technology in individual vehicles was one of the main recommendations in NHTSA's *Preliminary Statement*, California was the only state to require it statutorily.[95] Nevada's implementing regulations have made it clear that such a system is required there, as well.[96]

90. *Id.* at 7.

91. CAL. VEH. CODE § 38750 (West 2014); *see also* CAL. CODE REGS. tit. 13, §§ 227.00–.52 (2014).

92. CAL. VEH. CODE § 38750(a)(5).

93. *Id.* § 38750(b)(3).

94. *Id.* § 38750(c)(1)(G).

95. Act of Sept. 25, 2012, § 2, [2012] Cal. Stat. ch. 570.

96. Regulation Providing for the Operation of Autonomous Vehicles § 8, LCB File No. R084-11, 174 Nev. Reg. Admin. Regs. 1223 (Feb. 15, 2012).

The legislation adopted in California also sets a guideline for allowing operation for purposes other than testing. The manufacturer must apply for such permission, including in the application proof that the vehicle has specific mechanisms for engaging, monitoring, and disengaging the autonomous technology.[97] In cases of failure of the autonomous technology, the vehicle must have multiple means for the driver to take control.[98] If the driver does not take control, the vehicle must be capable of coming to a complete stop.[99] Additionally, the Department of Motor Vehicles must adopt specific regulations for allowing operation of autonomous vehicles by 2015.[100] The Department submitted its proposed regulations for testing vehicles in late 2013.[101] The testing regulations were adopted on May 19, 2014 and became effective on September 16, 2014.[102] Before enactment of this legislation, California did not prohibit or specifically regulate operation of autonomous vehicles on public roads.

California's implementing regulations appear in many aspects to be similar but not identical to those adopted by Nevada. Notable differences between the regulations adopted by the two states include that California does not contemplate private certification companies being authorized to approve vehicles for testing or sale, that its regulations do not impose geographical limits on its testing licenses, and that California only requires one person be present in the vehicle during testing, rather than Nevada's two.[103]

4. District of Columbia

The District of Columbia also enacted legislation with the purpose of authorizing "autonomous vehicles to operate on District roadways."[104] This language indicates that the District believed autonomous vehicles were not authorized to do so prior to legislation. The District defines autonomous vehicle in the same manner as Nevada and requires only that the driver have a manual control override feature

97. CAL. VEH. CODE § 38750(c)(1) (West 2014).

98. *Id.* § 38750(c)(1)(D).

99. *Id.* § 38750(c)(1)(C).

100. *Id.* § 38750(d)(1).

101. Notice of Proposed Regulatory Action Relating to Autonomous Vehicles, File No. 2013-1113-02, 48-Z Cal. Regulatory Notice Reg. 1859, 1868 (Nov. 29, 2013).

102. *See First Set of Autonomous Vehicle Regulations are Now in Effect*, CAL. DMV, https://www.dmv.ca.gov/portal/dmv/detail/pubs/newsrel/newsrel14/2014_61a (lasted visited Jan. 1, 2015).

103. *Compare* CAL. CODE REGS. § 38750 (2014); *with* NEV. ADMIN. CODE ch. 482A (2014).

104. Autonomous Vehicle Act of 2012, D.C. Law No. 19-278, 20 D.C. Stat. 906 (2013) (codified at D.C. CODE §§ 50-2351 to -2354 (LexisNexis 2014)).

for the autonomous technology and be seated in the car prepared to take control at any moment, and that the vehicle is capable of operating in compliance with District traffic laws at all times.[105] The vehicle itself must be either a 2009 model year or less than four years old when it is converted to an autonomous vehicle.[106] The District limits liability for vehicle manufacturers when a third party installs the autonomous technology.[107] Although the legislation placed further rulemaking power with the Mayor,[108] this authority was subsequently delegated to the Director of the Department of Motor Vehicles.[109] The Department promptly acted on this rulemaking authority, providing notice of its intent to adopt rules "establish[ing] a class of autonomous vehicles and procedures and fees for registration, titling, and issuance of permits to operate autonomous vehicles."[110]

5. Michigan

Most recently, Michigan passed legislation permitting the operation of autonomous vehicles on public roads.[111] While Michigan expressly authorizes the operation of these vehicles for testing purposes, it is the only state to specifically ban operation for non-testing purposes,[112] a measure publicly criticized by Google.[113] Before testing, Michigan requires manufacturers to register for special license plates, which must be displayed on the vehicle during testing on roads and highways,[114] and submit proof of insurance.[115] The vehicle must only be operated by an employee or other person authorized by the automated technology manufacturer while researching or testing the vehicle on a street or highway.[116] One person must to present in the

105. D.C. CODE § 50-2351(1) (definition of autonomous vehicle); § 50-2352(1)–(3) (requirements to operate autonomous vehicle on public roadways).

106. *Id.* § 50-2353(b).

107. *Id.* § 50-2353(a).

108. *Id.* § 50-2354.

109. Mayor's Order Delegating Rulemaking Authority under Autonomous Vehicle Act to Director of DMV, Ord. No. 2014-058, 61 D.C. REG. 2,501 (Mar. 21, 2014).

110. Notice of Proposed Rule Amending Title 18 of the D.C. Municipal Regulations, 61 D.C. REG. 3,587 (Apr. 4, 2014).

111. Act of Dec. 20, 2013, Pub. Act No. 231, [2013] Mich. Pub. Acts (codified at MICH. COMP. LAWS §§ 257.2b, 35a, 36, 244, 602b, 663, 665–66, 817 (2014)).

112. *See* MICH. COMP. LAWS §§ 257.663, 665 (2014).

113. Melissa Anders, *Autonomous Vehicle Testing Now Allowed Under Michigan Law*, MLIVE.COM (Dec. 27, 2013, 11:40 AM), http://www.mlive.com/politics/index.ssf/2013/12/autonomous_vehicle_testing_now.html.

114. MICH. COMP. LAWS § 257.244(3).

115. *Id.* § 257.665(1).

116. *Id.* § 257.665(2)(a).

vehicle during testing and must be capable of immediately taking over the vehicle's movements.[117] Michigan law also provides for civil penalties for a person violating automated vehicle laws.[118] Michigan's Transportation Department is also required to prepare and submit a report, in consultation with the Secretary of State and industry experts, "to the senate standing committees on transportation and economic development and to the house of representatives standing committees on transportation and commerce recommending any additional legislative or regulatory action that may be necessary for the continued safe testing of automated motor vehicles and automated technology installed in motor vehicles."[119] In a separate act, Michigan removed liability for vehicle manufacturers if damages were caused by autonomous technology and that technology was installed by a third party without the vehicle manufacturer's involvement.[120]

B. Failed Legislation

State bills that have failed to become law illustrate some of the issues that stand in the way of universal state acceptance of autonomous vehicles. For example, in Arizona, Representative Jeff Dial introduced legislation that would not require a human to be seated in an autonomous vehicle, a break from the states that have enacted laws.[121] The bill failed to clear Arizona's House Transportation Committee.[122]

Colorado's bill was halted by its own sponsor, Senator Greg Brophy.[123] The bill faced considerable opposition from Google and

117. *Id.* § 257.665(2)(b).

118. *Id.* § 257.666.

119. *Id.* § 257.665(3) (no later than February 1, 2016).

120. Act of Dec. 26, 2013, Pub. Act No. 251, [2013] Mich. Pub. Acts (codified at MICH. COMP. LAWS § 600.2949b (2014)).

121. Autonomous Motor Vehicles, H.B. 2167, 51st Leg., 1st Reg. Sess. (Ariz. 2013); *see also*, Howard Fischer, *Arizona Lawmakers May Give OK for Driverless Cars*, E. VALLEY TRIB. (Jan. 31, 2013, 7:03 AM), http://www.eastvalleytribune.com/arizona/politics/article_7bd7e948-6b35-11e2-9d8e-0019bb2963f4.html; Dan Strumpf, *Liability Concerns Put the Brakes on Driverless Cars*, WALL ST. J. (Jan. 28, 2013, 12:01 AM ET), http://blogs.wsj.com/drivers-seat/2013/01/28/liability-concerns-put-the-brakes-on-driverless-cars/.

122. *Presentation by the Ariz. Department of Transportation: Hearing on H.B. 2167 Before the H. Comm. on Transp.*, 51st Leg., Reg. Sess. (Ariz. 2013). The minutes, agenda, a video recording of this hearing are available on the Legislature's website, *H. Rep. Standing Comm. on Transp.*, Committee Info, 51st Leg., 1st Reg. Sess., AZLEG.GOV., http://azleg.gov/CommitteeInfo.asp?Committee_ID=5&Session_ID=110 (last visited on Dec. 12, 2014).

123. Monte Wahley, *Colorado Driverless Car Bill Shelved Until Further Notice*, DENV. POST (Feb. 5, 2013, 6:44PM MST), http://www.denverpost.com/breakingnews/ci_22526956/colorado-driverless-car-bill-shelved-until-further-notice.

from trial lawyers.[124] Rather than risk a vote against the legislation, Brophy asked that it simply be postponed.[125] Google did not identify its concerns publicly.[126] Another concern was brought up in Oregon, whose bill did not pass the Transportation Committee. Legislators there seemed to simply be concerned about the unforeseeable risks of automated vehicles. The hearing took place only a few days after the Boston Marathon bombing and Representative Cliff Bentz, possibly influenced by this act of terrorism, identified vehicles as carriers of bombs as a particular concern.[127]

Finally, New Jersey's legislation to regulate autonomous vehicles failed to clear committee after testimony by Scott Mackey, a representative from the Alliance of Automobile Manufacturers.[128] Mackey viewed state legislation on automated vehicles as premature, estimating widespread use of the vehicles to be about ten years away.[129] In addition, he stated that if each state enacted slightly different regulations, it would be difficult for manufacturers to standardize the technology for the wider market.[130] Mackey's statements appear to suggest that a code of federal, not state, regulations for automated vehicles may promote their use more quickly.

---

124. *Id.*

125. *Id.*

126. *Id.*

127. Joseph Rose, *Oregon Robo-Car Bill Stalls as ODOT Moves Forward With 'Connected Car' Study*, OREGONLIVE (April 18, 2013, 12:48 PM), http://www.oregonlive.com/commuting/index.ssf/2013/04/oregon_driverless_car_bill_sta.html.

128. For more information, see *About the Alliance*, AUTO ALLIANCE, http://www.autoalliance.org/about-the-alliance (last visited Dec. 12, 2014).

129. Andrew George, *Driverless cars in N.J.? Assembly Panel Considers Legislation Authorizing Tests*, N.J. BIZ. (Nov. 25, 2013, 3:13 PM), http://www.njbiz.com/article/20131125/NJBIZ01/131129789/Driverless-cars-in-NJ?-Assembly-panel-considers-legislation-authorizing-tests.

130. *Id.*

C. *Concluding Thoughts on State Legislation*

Since driverless technology is still very young, allowing the general public access to automated vehicles would be taking unknown risks. While each State's policy has different specifics, the States that have passed autonomous vehicle testing legislation, in line with the NHTSA's recommendations, all require licensing of the vehicle's human operator as well as prior approval from the state authorizing the testing company prior to driving an automated vehicle on public roads. Apart from these pre-operation requirements, States have instituted stipulations for insurance, safety mechanisms, and a human operator. States have also chosen to address liability for autonomous technology defects, future non-testing operation, and requiring future regulatory action. Each of the States that has enacted legislation has either authorized the eventual deployment of autonomous vehicles for operation by the general public or remained silent on the issue, with the exception of Michigan, which has only authorized testing of autonomous vehicles and has explicitly banned the operation of autonomous vehicles in other contexts.

V. PRIVACY AND DATA USE

Far more profusely than today's vehicles, mature and market-ready autonomous vehicles will generate and broadcast personal data, the use and storage of which will implicate important privacy rights in complicated ways that will likely have to be faced well before Level 3 and Level 4 vehicles become a commercial reality.[131] Although exclusively sensor-based autonomous vehicles are certainly a possibility,[132] many of the most compelling reasons for adopting self-driving cars are dependent on the vehicles sharing and coordinating data with each other, both locally and through centralized infrastructure. It is self-evident that the efficient management of traffic at intersections, the intelligent distribution of traffic to minimize congestion, and the ability of autonomous vehicles to safely travel in close-packed platoons, for instance, are all largely or completely reliant on communication both between the individual vehicles and other cars in the vicinity, and between the autonomous vehicles and an external network. Even if this

131. *Cf.* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1239 (2012).

132. Google's self-driving cars are an example of an almost exclusively sensor-based technology. *See* Erico Guizzo, *How Google's Self-Driving Car Works*, Posted in *Automation Blog*, IEEE SPECTRUM (Oct. 18, 2011, 9:00 GMT), http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works.

data is scrubbed of unique individual identifying markers, for instance VIN-numbers, or IP- or MAC- addresses, data-mining techniques will almost certainly be able to reconstruct personal identifying information about particular vehicles and by extension their regular occupants.[133] The way this data is used will be the subject of regulation and legal controversy. Concerns about user privacy have already drawn substantial attention from the media.[134]

The privacy concerns fall broadly into two categories: government access to and use of locational and other personal data, and the private, primarily commercial, use of the personal data. These issues are parallel to the concerns that are already emerging around the use of personal data generated by cellular phones, GPS devices, and Internet usage, and so the law surrounding many of these issues may be substantially settled well before any fully autonomous vehicles are ready for the market. The connected vehicle technologies that will almost certainly precede autonomous vehicles to the market will raise essentially the same or very similar privacy and security concerns as autonomous cars. NHTSA recently announced plans to require the inclusion of connected vehicle technologies, including both V2V and V2I, for all new vehicles 2014 connected vehicles initiative.[135] These technologies are therefore likely to be commonplace well before autonomous vehicles enter the consumer market. How these issues will be resolved is very uncertain, however, and the path privacy law takes will certainly have an impact on the rate of autonomous vehicle adoption. Federal privacy law in respect to these technologies is extremely underdeveloped and is the subject of a great deal of controversy, with interested parties having substantially incompatible views.

Consider how businesses may make use of personal data generated by autonomous vehicles. Automakers and other companies

133. *See* Glancy, *supra* note 131, at 1196, 1200 (showing how individual identity can be determined without reference to explicit identifiers).

134. *See, e.g.*, Doug Newcomb, *Privacy Group Voices Concerns Over Google-Backed Autonomous Vehicle Legislation*, WIRED (June 1, 2012, 3:23 PM), http://www.wired.com/2012/06/watchdog-autonomous-privacy; John M. Simpson, Blog, *DMV's Autonomous Vehicle Regulations Must Protect Users' Privacy*, CONSUMER WATCHDOG (Mar. 10, 2014), http://www.consumerwatchdog.org/blog/dmv%E2%80%99s-autonomous-vehicle-regulations-must-protect-users%E2%80%99-privacy.

135. *See generally* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., NHTSA ANNOUNCES DECISION TO MOVE FORWARD WITH VEHICLE-TO-VEHICLE COMMUN. TECH. FOR LIGHT VEHICLES (Feb. 3, 2014), *available at* http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles.

involved in autonomous vehicle technology have already received patents relating to in-car advertising.[136] Manufacturers or third parties could create advertising profiles based on the past travel of individual vehicles, derived from metadata that although not specifically identifying individuals as such, effectively achieves the same function. These advertising profiles could be linked to similar profiles derived from Internet usage patterns and other consumer data.[137] Advertising would then be able to be specifically tailored to the vehicles' occupants, and channeled into the car and its passive occupants, or even into the surrounding external environment, *à la* Steven Spielberg's film *Minority Report*.[138] The technology that would allow this sort of individualized targeting of ads based on aggregated metadata is already widely used in other contexts and underlies much of the advertising on the Internet.[139]

If route planning is left to private commercial entities, additional concerns may arise. In an extension of the in-vehicle advertising scenario, it is easily conceivable that a vehicle's route could be planned, without the users' knowledge, so that it happens to go by the physical businesses of paid advertisers. Past driving and purchasing habits could be analyzed to determine businesses a user would be likely to make impulse purchases from, and routing and advertising could then be coordinated to encourage the vehicle users to make unplanned stops. Vehicles could easily be routed so that, when they need to be refueled

136. For instance, in-car advertising that will likely make extensive use of locational and other personal data are emerging. Google has already patented technology that would enable ad-based taxi services, which would offer free or discounted trips to the brick-and-mortar locations of advertisers. *See* Ron Amado, *Google Patents Ad-Powered Taxi Service That Would Offer Free Rides to Shoppers*, ARS TECHNICA (Jan. 23, 2014), http://arstechnica.com/gadgets/2014/01/google-patents-ad-powered-taxi-service-that-would-offer-free-rides-to-shoppers. Ford has patented in-car advertiser technology, and both Ford and BMW are preparing to release in-car advertising apps. *See* Damon Lavrinc, *You Can Order a Pizza With Ford's New In-Car App*, WIRED (Jan. 7, 2014), http://www.wired.com/autopia/2014/01/ford-applink-dominos-parking/; *BMW Developing In-Car Advertising App*, CARADVICE, http://www.caradvice.com.au/267639/bmw-developing-in-car-advertising-app (last visited Mar. 28, 2014).

137. Among the many types of data available about individuals are records of their past purchases. Data brokerages gather and sell this information and it is put to myriad uses. For instance, certain purchasing habits are shown to be strongly correlated to credit worthiness, apparently including such trivial items felt furniture coaster pads. Thus, aggregated personal data may be used as a proxy for a credit score in contexts where the law forbids credit from being considered. *See* Steve Henn, *If There's Privacy in the Digital Age, It Has a New Definition*, NPR (Mar. 23, 2014), http://www.npr.org/blogs/alltechconsidered/2014/03/03/285334820/if-theres-privacy-in-the-digital-age-it-has-a-new-definition.

138. MINORITY REPORT (Twentieth Century Fox 2002).

139. U.S. Patent No. US 20120054028 A1 (filed Aug. 31, 2010).

the nearest gas stations would tend to belong to a company that paid for that privilege.

Vehicle routing and locational data raises concerns about privacy and autonomy relative to the government, as well. If government has access to users' routing information, it can easily derive information of a deeply personal nature—as New York's highest court recently described:

> Disclosed in [locational] data . . . will be trips the indisputably private nature . . . trips to the psychiatrist, the plastic surgeon, the abortion clinic, . . . the union meeting, the mosque, synagogue or church, the gay bar and on and on[.] . . . [I]t will be possible to tell . . . with ever increasing precision who we are and are not with, [and] when we are and are not with them[].[140]

Government having unfettered access to this data could only have a chilling effect on free speech and the expression of political dissent.

If a vehicle's navigation route decision is actually made by a centralized government network, there will be additional concerns about whether this infringes on the individual right to privacy, including the right to physical autonomy. Vehicle rerouting may be put to such questionable ends as routing traffic away from public protests. Other concerns that may arise if these decisions were left to the government include possible objections from individuals who were consistently forced to use a route slower than optimal, for the sake of overall traffic efficiency and at the expense of the individual's time. Governments may reserve access to faster routes options to those willing and able to pay for the privilege.[141]

Existing federal privacy protections are clearest and strongest where the party seeking access to an individual's private data is doing so under the authority of the government. The Fourth Amendment guarantees that individuals shall be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[142] Under present case law, this clause creates a broad right to privacy, including a right to have electronic communications and private data protected, in contexts where individuals have a "reasonable expectation of privacy," and where it would be unreasonable for the government to

---

140. People v. Weaver, 909 N.E.2d 1195, 1199 (2009).

141. This practice would mirror the subscription-based, reserved fast lanes on highways in cities such as Atlanta. *See e.g.*, *I-85 Express Lanes are Open*, STATE ROAD & TOLLWAY AUTH., http://www.peachpass.com/peach-pass-toll-facilities/about-i-85-express-lanes (last visited Mar. 28, 2014).

142. U.S. CONST. amend. IV.

violate this expectation of privacy.[143] The application of the reasonable expectation of privacy test has been unpredictable in the past,[144] and it is not clear whether such a reasonable expectation of privacy will be found to exist with respect to vehicular location information derived from GPS data or other tracking technology.

The Supreme Court, in *United States v. Jones*,[145] recently held that police placement of a GPS device on a person's vehicle and subsequent monitoring of that person's movements constituted a search under the terms of the Fourth Amendment, but the Court declined to decide whether the search was unreasonable.[146] The Court held that, because automobiles were "effects" under the Fourth Amendment, the placement of the GPS device on the vehicle was a physical trespass.[147] Because of this, the majority concluded that it did not need to reach the question of whether a reasonable expectation of privacy existed that would make GPS tracking an unconstitutional violation of the Amendment, even in the narrow context of the case, where the GPS device had placed on a vehicle by police, without a warrant, in the course of an investigation.[148]

Justice Alito, joined by three other justices, concurred in the judgment in *Jones* and would have found that a reasonable expectation of privacy existed under the circumstances of the case.[149] Justice Sotomayor wrote a concurrence arguing that she would have found the use of the GPS tracking data to be contrary to a reasonable expectation of privacy given the facts of *Jones*, and argued further that such a reasonable expectation of privacy would exist even if the police had not physically placed the GPS device on the vehicle but instead relied on technology already present in the car.[150] She suggests:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained

143. *See* Katz v. United States, 389 U.S. 347, 361–62 (1967) (Harlan, J, concurring).
144. Kyllo v. United States, 533 U.S. 27, 34 (2001).
145. 132 S. Ct. 945 (2012).
146. *Id.* at 949.
147. *Id.*
148. *Id.*
149. *Jones*, 132 S. Ct. at 957–58 (Alito, J., concurring).
150. *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring).

> power to assemble data that reveal private aspects of identity is susceptible to abuse.[151]

Thus, at least five justices might consider government tracking of autonomous or connected vehicles to be a violation of the Fourth Amendment's privacy guarantee, at least in some contexts. Given the difference between individual police tracking of one particular automobile compared to the possibility of tracking at will the potentially vast network of connected automobiles, it is not at all certain whether the courts would find a reasonable expectation of privacy to exist in the context of autonomous or otherwise connected vehicles.

Even if a strong expectation of privacy were found relative to GPS and other types of locational data, it is not clear that this would present government with a substantial barrier preventing access to the locational data history of individual autonomous or connected vehicle users, if the government is able to obtain this data from private sources to whom the vehicle users have constructively granted access. The United States Fifth Circuit Court of Appeals recently ruled in *In re U.S. for Historical Cell Site Data* that, in the context of a criminal investigation and as specifically authorized by section 2703(d) of the Stored Communications Act ("SCA"),[152] police had not committed a *per se* violation of the Fourth Amendment by requesting a court order requiring cellular phone service companies to provide historical location data of three cellphone users suspected of criminal activity, without having first obtaining a warrant or demonstrating probable cause.[153] The court characterized the cellphone companies' records of individual users' past locational data as mere "business records," documenting the voluntary communication of the phone user's locational data to his cellular service provider, where the user was "not conveying location information to anyone other than his service provider."[154] The court held "a conventional order for a third party's voluntarily created business records [does not] transform[] into a Fourth Amendment search or seizure when the records . . . shed light on a target's activities in an area traditionally protected from governmental intrusion."[155] Thus, barring further rulings or legislation to the contrary, it is likely that the government could access an individuals' autonomous vehicle location history by requesting records from a third party, such as the

151. *Id.*
152. 18 U.S.C. §§ 2701–12 (2013).
153. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013)
154. *Id.* at 612.
155. *Id.* at 615.

car's manufacturer, and thereby skirt the Fourth Amendment concerns raised by Sotomayor in *Jones*.[156] As described below, there are presently only very weak protections in place limiting the collection of personal data, including locational data, by businesses. Thus, *In re U.S. for Historical Cell Site Data* presents a very plausible means by which government may be able to circumvent Fourth Amendment barriers to surveillance.

Even if the courts where to hold that the locational data such as that sought in *In re U.S. for Historical Cell Site Data* is not a mere business record, it is likely that other data would be available to governments that may be sufficient to reconstruct a detailed locational history of a particular vehicle. By examining metadata and disregarding explicit individual identifiers, governments may be able to bypass the Fourth Amendment issues altogether while being able to reconstruct the individual movements of particular vehicles.[157] The ongoing litigation over the National Security Agency's large-scale use of internet and cellular phone metadata to track the movements and behavior of individuals may lead to the further specification of the government's ability to access and analysis these types of data.[158]

Legislators have attempted and continue to attempt to regulate the use of GPS and other locational data in order to protect users' privacy. For instance, the Geolocational Privacy and Surveillance Act has been introduced multiple times since 2011.[159] This Act would prohibit, under most circumstances, acquisition by the Government of an individual's geolocation data without first establishing probable cause and obtaining a warrant.[160] The Act, and similar proposed legislation, appears to have substantial bipartisan support, but despite this, it has not yet been put to a vote.[161]

Autonomous vehicles will likely generate other forms of data, not necessarily associated with location or historical destinations, over which users may still have a reasonable expectation of privacy. In the

156. *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring).

157. *Cf.* Glancy, *supra* note 131, at 1196, 1200 (showing how individual identity can be determined without reference to explicit identifiers).

158. *Cf.* Am. Civil Liberties Union v. Clapper, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013) (holding the NSA's bulk telephony metadata collection program to be lawful) (appeal pending).

159. Geolocational Privacy and Surveillance Act, H.R. 1312, 113th Cong. (2013); *Geolocation Privacy Legislation*, GPS.GOV, http://www.gps.gov/policy/legislation/gps-act/ (last visited Jan. 1, 2015) (showing that the GPS act has been introduced during the 112th, 113th, and 114th Congresses).

160. H.R. 1312 sec. 2(a), §§ 2603–04.

161. *Geolocation Privacy Legislation*, *supra* note 159.

realm of non-autonomous but highly connected vehicles, such data would include information about a user's driving habits, such as information about rates of acceleration, speed, braking data, and the like, which could be used to demonstrate liability in case of accidents, to form an individualized and empirical basis for car insurance rates, or even to automate the process of traffic law enforcement.[162] These particular privacy concerns may be less relevant in a world of fully autonomous vehicles, where individual vehicle occupants would likely be unable to cause the vehicle to disobey traffic rules. Still, it is possible that autonomous vehicles may generate data that could be construed as evidence of liability it certain contexts, which could raise Fourth Amendment issues. Future vehicles may default to recording in-cabin sounds or video, perhaps ostensibly for analysis in case of accidents.[163] If such data were stored, it seems there would likely be a strong expectation of privacy relative to its use in many contexts.

While some limited protections exist preventing the government from unrestrained access to vehicle users' private data, very little regulation exists preventing private parties from collecting, aggregating, analyzing, marketing, and monetizing individuals' private data in whatever creative ways they might imagine.

The Government Accountability Office (GOA) recently summarized the existing federal law governing private-sector use of personal information.[164] Aside from limited protection provided to children under thirteen years old by the Children's Online Privacy Protection Act,[165] and the relatively strong consumer data privacy guaranteed in the narrower realms of credit reporting and health care,[166] GAO identified the only federal limitation on the use of personal data in a

162. This type of data is already collected by many vehicles' EDR's. EDR's as noted in Section I, became mandatory for all new cars in 2014. Although current regulations limit the use of EDR data, it is conceivable that it may become the basis for the automated enforcement of traffic laws.

163. Some new vehicles are already recording cabin audio, including the 2015 Corvette Stingray. The data recorder in this model records video from the drivers' perspective as well as any in-vehicle noise. The Stingray is a high-performance sports car and this data is ostensibly recorded so that the driver can review past laps on a racetrack, for example. *See* Jaclyn Trop, *The Next Data Privacy Battle May Be Waged Inside Your Car*, N.Y. TIMES (Jan. 10, 2014), http://www.nytimes.com/2014/01/11/business/the-next-privacy-battle-may-be-waged-inside-your-car.html.

164. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-903, MOBILE DEVICE LOCATION DATA: ADDITIONAL FEDERAL ACTION COULD HELP PROTECT CONSUMER PRIVACY 7 (2012) [hereinafter MOBILE DEVICE LOCATION DATA REPORT].

165. 15 U.S.C. §§ 6501–06 (2013).

166. Under the regimes established by the Fair Credit Reporting Act, 15 U.S.C. §§ 1681–81x (2013), and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No.

prohibition of "unfair or deceptive acts or practices affecting commerce," arising from the Federal Trade Commission Act (FTCA).[167] GAO further explained:

> "An act or practice is unfair if the injury it causes or is likely to cause to consumers is: (1) substantial; (2) not outweighed by countervailing benefits to consumers or to competition; and (3) not reasonably avoidable by consumers themselves. . . . [an act] or practice is deceptive if: (1) it is likely to mislead consumers acting reasonably under the circumstances; and (2) it is material, that is, likely to affect consumers' conduct or decisions with respect to the product at issue."[168]

According to GAO, this provision of the FTCA allows in contexts where "[a] company was not adhering to the practices to protect a consumer's personal information that the company claimed to abide by in its privacy policy."[169]

Thus, existing federal protections of personal data are minimal at best. In the limited contexts where consumer data is protected from certain uses by law, it is often the case that businesses can easily include boilerplate contract language and thus avoid liability. There is, however, substantial pressure from within the federal government and from external privacy advocacy groups to reform and enhance consumer data privacy protections. In February 2012, the Obama administration called for Congress to develop and adopt what it called the *Consumer Privacy Bill of Rights* (*CPBR*), which, *inter alia*, would guarantee individuals control over "how companies collect, use, or disclose [their] personal data."[170]

The CPBR would in effect give legal force to the FTC's long-standing but non-enforceable guidelines for consumer data best practices, the Fair Information Practice Principles (FIPPs),[171] which are characterized in the White House's *Consumer Data Privacy in a Networked World* as including: individual control over what personal

104-191, 100 Stat. 2548 (1996).

167. MOBILE DEVICE LOCATION DATA REPORT, *supra* note 164 (citing 15 U.S.C. § 45).

168. *Id.* at 7 n.11 (internal citations omitted).

169. *Id.* at 7.

170. EXEC. OFFICE OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 11 (2012) [hereinafter PRIVACY BLUEPRINT], *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

171. The FIPPs framework originated in a 1973 report on Automated Personal Data Systems. *See* DEP'T OF HEALTH, EDUC. & WELFARE, COMPUTERS AND THE RIGHTS OF CITIZENS, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS ch. IV (1973) ("Recommended Safeguards for Administrative Personal Data Systems").

data businesses can collect and how this data may be used; transparency in businesses' data collection, privacy and security practices; respect for context, recognizing that "consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data[]"[172]and the secure handling of personal, private data; the consumers' right to access and ensure the accuracy of personal data; the principle of focused collection, guaranteeing reasonable limits on the personal data that companies collect and retain.[173] To these established FIPPs principles, the *CPBR* would add a right of accountability, ensuring that the preceding principles would be enforced.[174]

Among the more substantial guarantees of the *CPBR* would be the consumer's right to access and verify the accuracy of personal data stored by private companies, providing individuals with "the means and opportunity to correct inaccurate data or request its deletion or use limitation,"[175] as well as a right to impose "reasonable limits on the personal data that companies collect and retain,"[176] restricting the collection and use of personal data appropriate to the context in which the users provided them with the data.[177] The White House recommended that the *CPBR* be implemented as "enforceable codes of conduct," developed through a "multistakeholder process," involving "individual companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups[.]"[178] Envisioning such a process, the White House document does not provide any model language for legislation or regulation.

Government bodies and other organizations have advanced proposals similar to the White House's *CPBR*, developed contemporaneously to the White House document or in the two years since the White House document was issued. For instance, in a March 2012 report the FTC released a set of recommendations very much in-line with those of the White House, seeking cooperation between stakeholders and policymakers in developing what would ultimately be an

172. PRIVACY BLUEPRINT, *supra* note 170, at 15.
173. *Id.* at 18–20.
174. *Id.* at 21.
175. *Id.* at 19.
176. *Id.* at 21.
177. *Id.*
178. *Id.* at 23.

enforceable code of conduct modeled on the FIPPs.[179] In September 2012, GAO issued a report recommending that the National Telecommunications and Information Administration work with stakeholders to develop an analogous code of conduct relating specifically to location data derived from mobile devices.[180]

An earlier effort at establishing a variation on the FIPPs specific to the connected vehicle context was Vehicle Infrastructure Integration (VII) Coalition's *VII Privacy Policy Framework*.[181] The VII Coalition, disbanded in 2007, was an association of automakers, privacy advocate groups, and other interested parties, organized by the DOT that studied the potential implementation of a DSRC-based connected vehicle system to enhance vehicle safety.[182] The *VII Privacy Policy Framework*, achieved by consensus-building between the participant stakeholders and not legally binding, promulgated principles including "Respect for Privacy and Personal Information[,] . . . Information Purposes, Acquisition, Notice, Fair Information Use, Information Protection and Retention, Openness, Participation and Accountability."[183] Beyond this repetition of familiar FIPPs principles, the *Framework* included hard "privacy limits" that sought to limit the possibility of personal identifiers broadcast over DSRC being collected and used without the individual vehicle operators' consent.[184] Legal scholar Dorothy Glancy has suggested that the *VII Privacy Policy Framework* should be adopted as a model for establishing autonomous vehicle privacy standards, both as an example of stakeholder consensus building and because of the strong protections it would provide against the wholesale acquisition of user identifiers.[185]

It is clear that there is broad resistance to the very business-friendly status quo in the area of consumer data privacy rights, but it is less clear that anything like the *Consumer Privacy Bill of Rights* will actually be enacted in the foreseeable future. Further, given the deep involvement in the policy-making process interested companies will

179. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

180. MOBILE DEVICE LOCATION DATA REPORT, *supra* note 164, at 37.

181. LESLIE JOHNSON ET AL., VII PRIVACY POLICY FRAMEWORK VERSION 1.0.2 (2008), *available at* http://financecommission.dot.gov/Documents/April2008Meetings_Hearings/VII_Privacy_Policies_Framework-Approved_by_ELT.pdf

182. *Id.*

183. Glancy, *supra* note 133, at 1233.

184. JOHNSON ET AL., *supra* note 181, at 23.

185. Glancy, *supra* note 133, at 1235.

have as key stakeholders, it is perhaps doubtful that even if something akin to the *CPBR* were to be implemented that it would present a very great obstacle to the use of personal data in all but the most plainly illegitimate circumstances. In any case it appears that little substantive movement toward bringing the White House's proposal to fruition has been made in the intervening years, and in the meantime Big Data business techniques have become more and more ubiquitous. Unless consumers are more consistently vocal in their opposition to the commercial use of data derived from their vehicle use patterns then they have been historically to the use of similar data derived from their cellular phone, credit card, and internet usage habits, it seems unlikely that businesses in the automated and connected vehicle industries will be substantially barred from using consumer data in whatever manner they see fit.

Another route by which more substantial consumer data protection may conceivably come about would be through action by state governments. Sufficiently populous and powerful states may have leverage sufficient to require autonomous vehicle makers to disclose to state residents the data they collect and the uses to which the that data is put. Such legislation has already been proposed in California.[186] The Consumer Vehicle Information Choice and Control Act seeks to require manufacturers of new motor vehicles sold after January 1, 2016 to make disclosures to the vehicles' owners regarding the information generated and collected by the vehicle.[187] The owner would have full and sole access to the information and be able to transmit it to a third party.[188] The manufacturer would not be able to take action against the owner for accessing or using the information.[189] In limited circumstances a manufacturer or medical researcher would be able to access and use the collected information, provided all personally identifying information is removed.[190] If California or another state succeeds in passing such legislation, it will likely not have the same level of national impact that California's strict vehicle emissions laws have had. This is because the bill will not necessarily require the vehicle makers invest in any special new technology in order to access California's large markets—technology which would then be native to all vehicles whether they were sold in California or not. Instead, it

186. S.B. 994, Leg. 2013-2014 Reg. Sess. 7 (Cal. 2014), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB994.

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.*

would only grant a special right of access to information to vehicle owners in that state, leaving the manufacturers with full control of the data for users in every jurisdiction that was not subject to equivalent legislation.

The 2012 push for consumer privacy protections seems to have made little progress, but there is some recent movement in Washington with respect to automakers' usage of personal data. In a December 2, 2013 open letter to auto industry executives, Senator Edward Markey of Massachusetts raised concerns about the disclosure of individual user data and aggregated data from vehicles currently on the market, seeking information from automakers as to whom this data is shared with or sold to, how long the data is kept, whether vehicle users have any option to delete this data or else to have it not retained at all, and similar questions.[191] Senator Markey requested that automakers respond to his inquiry no later than January 3, 2014.[192] The Senator has not disclosed whether any responses were submitted, and if so, whether these responses will be made public.

VI. SECURITY, CYBERATTACKS, AND TERRORISM

Senator Markey's letter also focuses its attention on the vulnerability of connected vehicles to cyberattacks, citing DARPA-funded research that exposed the susceptibility of the electronic control units of certain vehicles already on the market.[193] These vehicles could be hacked, enabling external control of braking, acceleration, and steering.[194] Senator Markey asked the manufacturers for information on their plans for overcoming these risks.[195] Such information would be helpful in determining the feasibility of NHTSA's stated goal of insulating the automated, connected vehicle infrastructure it foresees from potential cyberattacks.[196]

Although the primary example of vehicle hacking cited by Senator Markey relied on being physically present in the vehicle, contemporary cars have been proven susceptible to wireless attacks as well. Researchers from Rutgers and the University of Southern California were able to control vehicles' electronic control units (ECUs), accessed

191. Letter from Edward J. Markey, Senator, to Auto Industry Executives, at 7 (Dec. 2, 2013), *available at* http://www.markey.senate.gov/documents/2013-12-2_GM.pdf.

192. *Id.*

193. *Id.* at 1; *see also* CHARLIE MILLER & CHRIS VALASEK, ADVENTURES IN AUTOMOTIVE NETWORKS AND CONTROL UNITS (2013), *available at* http://illmatics.com/car_hacking.pdf.

194. *Id.*

195. Markey, *supra* note 191.

196. PRELIMINARY STATEMENT, *supra* note 14, at 8.

through their wireless tire pressure monitoring systems.[197] It has been suggested that an attack might be staged by exploiting a vehicle's EDR system, which in newer vehicles are accessible wirelessly and may communicate remotely with emergency response centers.[198] The remote hijacking of autonomous vehicles presents a very serious risk in a world of fully automated motor vehicles, where, for instance, traditional traffic signals would be rendered obsolete by the possibility of coordinating the flow of traffic through intersections, making real-time speed adjustments such that traffic from two perpendicular multilane highways could cross paths without any vehicles coming to a stop or even substantially slowing down. One vehicle making a sudden and unannounced change in its path could cause significant damage and disruption. Many autonomous vehicles being hijacked at once in an urban center could lead to terror on the scale of the September 11 attacks.

Ensuring that autonomous and connected vehicle technologies are secure from such exploitation is a responsibility of NHTSA.[199] DOT and NHTSA, as well as various industry players, are dedicating significant resources to understand strategies to insulate vehicles from attack.[200] NHTSA has stated its goal of developing an "initial baseline set of requirements"[201] to ensure that the ECUs in contemporary and future vehicles, including autonomous vehicles, are secure from cyberattack.[202] In NHTSA's *Preliminary Statement*, the Agency suggests that the process of developing these requirements should be complete within four years of that document's 2013 publication.[203]

Although the evidence suggests that the ECUs of vehicles currently on the market are not well secured against attack, it does appear at least that such attacks would attach federal criminal liability to their perpetrators. Any substantial attempt at an attack designed to exploit and take control over a modern car's ECUs would almost certainly subject the attacker to federal criminal liability under the

197. *See* Peter Bright, *Cars Hacked Through Wireless Tire Sensors*, ARS TECHNICA (Aug. 10, 2010), http://arstechnica.com/security/news/2010/08/cars-hacked-through-wireless-tyre-sensors.ars.

198. Balough & Balough, *supra* note 35, at 1.

199. *See* PRELIMINARY STATEMENT, *supra* note 14, at 8.

200. *See* NHTSA V2V Security Credential Management System ANPRM, FR Doc. 2014–24482, 79 Fed. Reg. 61927 (Oct. 14, 2014).

201. PRELIMINARY STATEMENT, *supra* note 14, at 7.

202. *Id.*

203. *Id.* at 8.

Computer Fraud and Abuse Act (CFAA),[204] the Digital Millennium Copyright Act (DMCA),[205] the Wiretap Act,[206] and potentially the USA PATRIOT Act.[207]

VII. REGULATORY OPTIONS, COMMERCIAL PROSPECTS AND THE POTENTIAL PACE OF CHANGE

Although automotive industry analysts have attempted to anticipate the timing of automated vehicle technology deployment based on a variety of factors, the authors have concluded that timing will be substantially affected by three key variables that are generally unacknowledged by industry analysts. Each of these three variables involves the promise of significantly improved vehicle safety.

Beyond necessary technological developments, analysts generally concur that the following factors, expressed as barriers to achieving successive levels of automation, must be ameliorated to arrive at Levels 2 and 3, and eventually eliminated to arrive at Level 4:

(1) Limited driver acceptance of diminished control over vehicles. As noted in the report jointly issued by the Center for Automotive Research and KPMG LLP: "There is no margin for error with safety-critical technologies. They must work perfectly every time; life and death hang in the balance. Consumers will not relinquish control until they are certain their vehicles and the mobile environment are 100 percent safe and reliable."[208]

(2) Unacceptably high technology costs with respect to both automated vehicle technology and accompanying infrastructure. Presently, only 20% of consumers surveyed would be willing to spend as much as $3,000 for automated vehicle features.[209]

(3) Lack of cybersecurity, particularly with respect to V2V and V2I technologies that by their nature involve multiple, and perhaps many, vehicles whose functioning could be disrupted to cause catastrophic damage. NHTSA and DOT are working together with

---

204. 18 U.S.C. § 1030 (2008)

205. 17 U.S.C. § 512 (2006).

206. Pub. L. No. 90-351, 82 Stat. 197 (June 19, 1968); Pub. L. No. 99-508, 100 Stat. 1848 (Oct. 21, 1986) (amending the Wiretap Act to include electronic communication).

207. Arguments for and against finding liability under these acts can be found in Balough & Balough, *supra* note 35, at 5–7. The authors of that article are perhaps unduly skeptical that a vehicle's ECUs would be found to be "protected computers" under the language of CFAA, suggesting that they may not sufficiently be "used in or affect[] interstate or foreign commerce." The DMCA similarly requires that an intercepted communication affect interstate commerce.

208. KPMG & CTR. FOR AUTO. RESEARCH, *supra* note 22, at 19.

209. *Id.* at 20.

industry to establish a secure V2V credentialing system that may alleviate these concerns.[210]

(4) Lack of aftermarket automated vehicle technologies to accel-erate vehicle market penetration and, therefore, consumer acceptance and technology cost reductions.

Uncertainty as to who is liable for damages caused by automated vehicle crashes is cited by industry analysts as an impediment to implementing truly autonomous Level 4 vehicles,[211] but the authors view this as a concern to be addressed, rather than a fundamental impediment. As vehicle automation serves to reduce both crash rates and associated damage claims, the risk borne by insurance companies will also decline.[212] To maintain competitive standing, insurers can be expected to adapt timely to liability issues as technological advances reveal them, although they may resist providing insurance for Level 3 and 4 vehicles if there is any possibility of technology failure or cyber-hacking that could cause catastrophic damage involving multiple vehicles and property owned by third parties. Similarly, states, which must enact legislation authorizing the use of Level 3 and Level 4 vehicles on roadways, will likely resist doing so until they determine that such vehicles will not pose unreasonable safety hazards, probably with input from insurers. Other systems, such as the nation's system of air travel, have been insurable despite similar liability issues as those presented by autonomous vehicles systems. The authors recommend that significant resources be dedicated by stakeholders to formulating a proposed "architecture" for insuring autonomous vehicle systems.

With respect to legal battles over general responsibility for damages, those proven responsible for damages should be held accountable within the traditional, tort-based legal framework, though the process of determining liability can be expected to become more complicated as technology becomes more complex and the number and types of technology providers increases, as discussed in Section I.

Data privacy concerns are also cited as an impediment to implementing automated vehicles.[213] However, as we have shown, privacy concerns are not generally different in the automated vehicle context than any other involving technology developments accompanied by the prolific dissemination and accumulation of personal information.

---

210. *See* NHTSA V2V Security Credential Management System ANPRM, FR Doc. 2014–24482, 79 Fed. Reg. 61927 (Oct. 14, 2014).

211. SHANKER ET AL., *supra* note 28, at 18.

212. *Id.* at 57.

213. *See* Wood et al., *supra* note 47 at 1448. *See generally*, Glancy, *supra* note 131.

Therefore, it would seem that privacy concerns in the automated vehicle context should not be any more of an impediment to the introduction of automated vehicle technology than has been the case with respect to other already widely-adopted technologies, such as social media, smartphones, or GPS navigation. Accordingly, barring a catastrophic misuse of personal information by vehicle manufacturers or related parties that accumulate information, the regulation of private information use in the automated vehicle context should not be expected to proceed at a different pace than with respect to such other technologies.

The three safety-related variables identified by the authors as significant factors affecting the timing of automated vehicle technology implementation are:

(1) the degree to which automobile manufacturers conclude that safety-related automated vehicle technologies present profitable commercial opportunities;

(2) the extent to which they perceive implementation of such technologies to be a corporate social responsibility; and

(3) whether NHTSA will accelerate deployment by preemptively mandating vehicle automation technologies.

A confluence of circumstances indicates that automobile manufacturers and NHTSA may move aggressively with respect to technology implementation, rather than reluctantly. First, the proliferation of developing, existing and implemented vehicle automation safety features is enabling the development of a vision of radically safer vehicle travel. That vision should not necessarily be impaired by automobile manufacturers' reluctance to commercialize safety technologies because experiences of the past four decades demonstrate that safety features that add to the cost of vehicles (e.g., airbags) are frequently desired, and sometimes eventually sought after, by consumers, rather than avoided.

The hazards of vehicle travel are seen in data gathered and published by NHTSA. In 2011, the last year for which NHTSA has publicly released data, 2,217,000 people were injured in American crashes; 32,367 people were killed; and 3,778,000 crashes caused property damage.[214] These statistics represent a significant decline in incidents, as measured annually, over the preceding three years; but over the course of the preceding ten years, a total of 392,872 people

214. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., DOT HS 811 753, TRAFFIC SAFETY FACTS 2011 DATA 1 (2013).

were killed in vehicle crashes and 25,397,000 were injured.[215] In consideration of these statistics, vehicle crashes are an immense social issue, with associated costs in terms of loss of life, limb and property. The NHTSA recognizes the gravity of this issue and hopes to address it by expanding the use of more advanced crash avoidance technologies.[216] The issue persists even in the face of enormous strides made by automobile manufacturers toward improving vehicle safety, intensified enforcement of laws that prohibit driving under the influence of alcohol and narcotics, increasing disinterest in driving among younger people who are disproportionally involved in vehicle crashes, and NHTSA's robust regulatory scheme of regulations, including mandated safety features such as airbags, seatbelts and electronic stability control.[217]

If the next frontier for significantly, or perhaps radically, improved vehicle safety is to be found in automated vehicle technology, then NHTSA has several methods with which to advance its implementation. Under the National Traffic and Motor Vehicle Safety Act,[218] NHTSA may establish vehicle safety standards for new motor vehicles and motor vehicle equipment, require the recall and remedy of vehicles and equipment that do not comply with standards, conduct investigations into safety defects, and require the recall and remedy of motor vehicles and motor vehicle equipment determined to have a safety defect.[219] As noted by Wood, case law indicates that "NHTSA can establish standards to require the installation of certain specific equipment on vehicles and establish performance standards for that equipment."[220] Under the Safety Act, standards must be performance-oriented, objective, meet the need for safety and be practicable.[221] Further, NHTSA hosts its New Car Assessment Program, under which vehicle crashworthiness is ranked on a five-star scale (for which five

215. *Id.*

216. *Id.*

217. *Id.*

218. 49 U.S.C. §§ 30101–33118 (2013).

219. *Id.* § 30110 (motor vehicle safety standards), § 30166(b) (authority to conduct inspections or investigations), § 30120 (remedies for defects or noncompliance), § 30118 (notification of defects or noncompliance).

220. Wood et al., *supra* note 47, at 1450. To support this, Wood cites Washington v. Dept. of Transp., 84 F.3d 1222 (10th Cir. 1996) (holding NHTSA's regulatory authority enables it to require specific equipment be installed in vehicles). Additional cases cited in Wood and in the Washington v. DOT case in support of this authority include Wood v. Gen. Motors Corp. 865 F.2d 395 (1st Cir. 1988); Chrysler Corp. v. Rhodes, 416 F.2d 319 (1st Cir. 1969); Automotive Parts & Accessories Ass'n v. Boyd, 407 F.2d 330 (D.C. Cir. 1968).

221. Wood et al., *supra* note 47, at 1450.

stars is highest) and information about selected advanced crash avoidance technologies is made available to the public to promote such technologies.[222] As Wood also notes, "NHTSA selects crash avoidance technologies for inclusion in NCAP's crash avoidance ratings program based on technical maturity of the technology, the availability of the technology in the current fleet, and the availability of safety effectiveness data for the technology."[223]

Therefore, NHTSA can speed the implementation of automated vehicle technologies by establishing standards that require such technology, so long as such standards are performance-oriented, objective, meet the need for safety and are practicable. Alternatively, it can simply establish standards as the automotive industry rolls out technology, while also encouraging the proliferation of technology by including it in its New Car Assessment Program.

Different than ever before, however, the proliferation of technology provides NHTSA with regulatory opportunities, while automobile manufacturers may also conclude they have commercial opportunities, and a social responsibility, to accelerate the adoption of automated vehicle technologies and, in so doing, further address the hazards of vehicle travel.

222. *Id*. at 1426–27.
223. *Id*. at 1494.