NOTE

BETTER KEEP YOUR HANDS ON THE WHEEL IN THAT AUTONOMOUS CAR: EXAMINING SOCIETY'S NEED TO NAVIGATE THE CYBERSECURITY ROADBLOCKS FOR INTELLIGENT VEHICLES

I. INTRODUCTION

Envision your future self waking up Monday morning. You check the commute time to work on your app, which has been consistently thirty-four minutes, and establish that this is just enough time to look over the materials for your meeting. You jump into your autonomous car and say, "Navigation, Work," while putting on your headphones and beginning to type your notes. After some time, you look up and realize that the car is stuck in heavy traffic and has not even made it a quarter of the way! In a panic, you throw off your headphones and pull up your vehicle's on-board news telecast. The telecast describes a hacker group taking total control of a fleet of vehicles and forcing them to a complete standstill further down the highway. As the news camera zooms into the section of gridlock, you see agitated commuters stepping out of their vehicles. Realizing that the commute time on your app has jumped to over 150 minutes, you quickly take the exit and look for an alternate route while switching your car over to manual control. Hopelessly speeding, you begin thinking of excuses you can tell your boss who never liked the idea of "computerized cars" in the first place.

Remarkably, computerized technology has been utilized in vehicles for many years.[1] This technology controls and monitors the vehicle using millions of lines of code connected by internal networks.[2] Today,

1. *See* Jim Motavalli, *The Dozens of Computers That Make Modern Cars Go (and Stop)*, N.Y. TIMES, Feb. 5, 2010, at B6; Jose Pagliery, *Your Car Is a Giant Computer—and It Can Be Hacked*, CNN MONEY (June 2, 2014, 3:33 PM), http://money.cnn.com/2014/06/01/technology/security/car-hack.

2. Motavalli, *supra* note 1. It has been mentioned that even basic vehicles have at least thirty microprocessor controlled devices, known as electronic control units, and that luxury cars have even

automated technology continues to push this technological innovation even further, to produce a vehicle that can be engaged in auto-pilot.[3] As a result, the car, as we know it, is becoming less like a car and more like a computer.[4] Current laws do not provide a viable means of addressing the cybersecurity concerns associated with the hacking of autonomous vehicles.[5] Car makers need to "reduce vulnerabilities to malware and cyberattacks that exist in their computers on wheels as they continue to roll out new products with even more technology."[6] Additionally, legislatures and judges need to "examine how today's laws apply to damage caused when hackers or terrorists exploit these vulnerabilities."[7]

Having a viable means to address this problem would better the welfare of the nation and provide better protection to its citizens.[8] This includes "relieving the enormous emotional toll on families, . . . lives lost, hospital stays, days of work missed, [insurance premiums,] and property damage—totaling in the hundreds of billions of dollars each year."[9] There are many concerns with these vehicles being used as weapons in the hands of hackers.[10] Proper regulation is needed to

---

more. *Id.*

3. *See* Jerry Hirsch, *Self-driving Cars' New Focus; Ford Teams with MIT and Stanford to Figure Out Ways to Make Them Intuitive*, L.A. TIMES, Jan. 23, 2014, at B2. An important function for cars on autopilot includes mapping that will allow the car to plan a path to safely avoid pedestrians and other vehicles without the need for driver intervention. *Id.* Some have already driven cars with the autopilot feature available, such as the Tesla Model S P90 D, where the car had automatic steering and lane changing. *See* Chris Perkins, *I Tested Tesla Autopilot in Manhattan Traffic—And Lived to Tell About It*, MASHABLE (Nov. 6, 2015), http://mashable.com/2015/11/06/tesla-autopilot-new-york/#72vswY0ZEkqt.

4. *See* Hirsch, *supra* note 3.

5. *See* Cheryl Dancey Balough & Richard C. Balough, *Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?*, BUS. L. TODAY 1, 4 (2013), http://www.americanbar.org/content/dam/aba/publications/blt/2013/11/cyberterrorism-cars-201311.authcheckdam.pdf. In order to adequately address cybersecurity concerns, the adoption and implementation of industry-wide standards may be necessary—meanwhile, "cars, their owners, and passengers are vulnerable, creating liability concerns for the automotive industry." *Id.* at 2.

6. *Id.* at 4.

7. *Id.*

8. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., PRELIMINARY STATEMENT OF POLICY CONCERNING AUTOMATED VEHICLES 1 (2013), https://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf (highlighting that continuing advances in automotive technology and current research in testing new vehicles create new possibilities for improved traffic safety, increased environmental benefits, expanded mobility, and new economic opportunities for jobs).

9. *Id.* ("Moreover, these dramatic changes will offer significant new opportunities for investments in [autonomous vehicle] technologies and employment in the various industries that develop, manufacture, and maintain them.").

10. *See* Tom Krishner, *Hackers Find Ways to Hijack Car Computers and Take Control*, FIN. POST (Sept. 3, 2013, 11:28 AM), http://business.financialpost.com/2013/09/03/hackers-find-ways-to-hijack-car-computers-and-take-control/?__lsa=0376-eb61; *see also* Richard Gray & Gwyn Topham, *Driverless Cars Could Face Threat from Hackers Trying to Cause Road Chaos*, GUARDIAN (Nov. 21, 2014, 12:59 AM), http://www.theguardian.com/technology/2014/nov/21/

prevent dangerous and unethical situations and to deter potential hackers from taking control in the first place.[11] Situations can include a hacker using a hacked vehicle to inflict harm.[12] Other possible threats include kidnapping passengers and programming cars to forcibly slow down traffic.[13] The Federal Bureau of Investigation ("FBI") has warned that these vehicles can be lethal weapons, emphasizing that although this technology can have many benefits, these dangers are only a modest representation.[14] Studying current hacking and transportation laws, and implementing an overarching federal statute for autonomous vehicle regulation are strong first steps in addressing this problem.[15]

It has been asserted that the major obstacle to motorists and firms adopting autonomous vehicles stems from "whether the government will take prudent and expeditious approaches to help resolve important questions about assigning liability in the event of an accident, the availability of insurance, and safety regulations."[16] There is also the need to consider that the change over time to autonomous vehicles is incremental, and market penetration will increase in proportion to the degree of consumer demand for such vehicles, as well as how

---

driverless-cars-hacking-threat-road-trials-january. Cybersecurity and transport experts have warned that driverless cars need to be protected from hackers who could take control and cause chaos on the roads. *Id.*

11. *See* Balough & Balough, *supra* note 5, at 2 ("[A] terrorist could control cars via malware, using many of the same techniques for hacking into regular computers.").

12. *See id.* (describing how a hacker could create mayhem on the roads if he breaks into a vehicle network, and then orders car ignitions to turn off or brakes to engage and disengage).

13. Jeffrey K. Gurney, *Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles*, 5 WAKE FOREST J.L. & POL'Y 393, 437 (2015) (depending on the situation, a hacker could also be charged with kidnapping); *see* Ryan M. Gerdes et al., *CPS: An Efficiency-Motivated Attack Against Autonomous Vehicular Transportation*, *in* PROCEEDINGS OF THE 29TH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE 99, 100-01 (2013).

14. *See* Mark Harris, *FBI Warns Driverless Cars Could Be Used as 'Lethal Weapons,'* GUARDIAN (July 16, 2014, 6:14 PM), https://www.theguardian.com/technology/2014/jul/16/google-fbi-driverless-cars-leathal-weapons-autonomous. At the same time, the FBI predicts that autonomous cars "will have a high impact on transforming what both law enforcement and its adversaries can operationally do with a car." *Id.* The FBI believes surveillance will be more effective since tailing suspects will be much simpler in more technologically advanced patrol cars. *Id.*

15. *See* Dorothy J. Glancy, *Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J.L. SCI. & TECH. 619, 686-88 (2015) (describing the option of preempting inconsistent state law and creating a uniform national autonomous vehicle legal regime for first generation autonomous vehicles).

16. *See* Clifford Winston & Fred Mannering, *Implementing Technology to Improve Public Highway Performance: A Leapfrog Technology from the Private Sector Is Going to Be Necessary*, ELSEVIER 158, 164 (2014) (illustrating that the policymakers' failure to implement comparable technology in the past creates more controversy in deciding whether the public, or the private sector, is better able to spur such technological change that contributes to adequate growth).

effectively safety regulations are implemented.[17] Security concerns will undoubtedly directly impact adoption of autonomous vehicles and are already leading to calls for proper regulation.[18]

This Note begins by examining the potential impact autonomous vehicles will have on society by looking at the benefits the innovation may employ.[19] Part II examines existing federal and state law in relation to regulating autonomous vehicles.[20] Part III focuses on the lack of proper regulation against potential hackers of autonomous vehicles as it relates to criminal liability.[21] Current concerns and ideas for proper regulation of autonomous vehicle liability with regard to the issue will also be explored.[22] Part IV argues that for regulation to be effective a federal statute on autonomous vehicles must be crafted to include certain vital elements, one of which includes a specialized license to operate such a vehicle.[23] The purpose of this is to facilitate law enforcement access to evidence needed for criminal prosecution without prompting major privacy concerns.[24]

II. AN OVERVIEW OF TECHNOLOGICAL AND LEGAL DEVELOPMENTS OF AUTONOMOUS VEHICLES

It is important to understand that the concept of autonomous vehicles is no longer outlandish.[25] Automobile manufacturers already have prototype vehicles that successfully completed self-driven cross-country trips.[26] The National Highway Traffic Safety Administration

17. *See* Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 WAKE FOREST J.L. & POL'Y 339, 370 (2015) (illustrating that comprehensive change does not come overnight—the roadways will not be instantaneously populated by a fleet of autonomous vehicles).

18. *Id.* at 370-71; *see* Jaclyn Trop, *The Next Data Privacy Battle May Be Waged Inside Your Car*, N.Y. TIMES, Jan. 11, 2014, at B1.

19. *See infra* Part II.B.

20. *See infra* Part II.C.

21. *See infra* Part III.A.

22. *See infra* Part III.B.

23. *See infra* Part IV.

24. *See infra* Part IV.

25. *See* Pagliery, *supra* note 1 ("Most people aren't aware their cars are already high-tech computers."). Cars can already network, giving them wireless capabilities like a smartphone with wheels. *See id.*; *see also* Anne Teigen et al., *Driving the Future*, ST. LEGISLATURES, Mar. 2013, at 12, 12, 15 (illustrating how forty years ago the thought of riding in a car that can steer itself would have been unimaginable, unlike today).

26. *See* Devin Coldewey, *Self-Driving Car Completes Cross-Country Trip in 9 Days*, NBC NEWS (Apr. 2, 2015, 3:02 PM), http://www.nbcnews.com/tech/innovation/driverless-car-completes-cross-country-trip-9-days-n334776 (describing an autonomous, modified Audi Q4 SUV, created by Delphi Automotive, equipped with cameras and laser rangefinders, that completed a 3400-mile trip across the country).

("NHTSA") segments vehicle automation into six levels ranging from vehicles without any automated control systems (level zero) to fully automated vehicles (level five), based on definitions created by SAE International ("SAE").[27] Subpart A introduces the concept and performance of autonomous vehicles, and follows with their benefits and uses in Subpart B.[28] Then, Subpart C analyzes current federal and state laws that relate to autonomous vehicles.[29]

A. Functionality and Technology of Autonomous Vehicles

The discussion in this Note generally refers to full (level five) automation, defined as an "automated system [that] can perform all driving tasks, under all conditions that a human driver could perform."[30] The design will anticipate the driver, will provide navigational input, and will not require any driver control. In fact, the vehicle does not even need to be occupied by a person.[31] Automobile manufacturers indicate that autonomous vehicles will be interconnected.[32] The vehicle-to-vehicle ("V2V") and vehicle-to-infrastructure ("V2I") technologies will facilitate interconnected communications via wireless data exchanges between vehicles and nearby entities.[33] Interconnected communications

---

27. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY 9 (2016), http://www.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf. Level zero has no automation, where the driver is in complete control of primary vehicle controls such as braking, steering, throttle, and motive power at all times. *Id.* Levels one and two have function-specific automation, where the driver has overall control but can choose to give up limited authority over a primary control to the vehicle, such that the vehicle can assume limited authority over that primary control. *Id.* Level three has combined function automation, where at least two primary control functions are designed to work in unison to relieve the driver of control over those functions. *Id.* Level four has limited self-driving automation, which would enable the driver to cede full control over all safety-critical functions under certain traffic or environmental conditions. *Id.* Level five has full self-driving automation, where the driver will solely provide destination or navigation input, and is not expected to be available for control at anytime during the trip. *Id.*

28. *See infra* Part II.A–B.

29. *See infra* Part II.C.

30. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 27, at 9.

31. *Id.* at 9-10.

32. Dave Guilford, *Like EVs, Self-Guided Cars Need Infrastructure*, AUTOMOTIVE NEWS (Mar. 10, 2014, 12:01 AM), http://www.autonews.com/article/20140310/OEM06/303109959/like-evs-self-guided-cars-need-infrastructure.

33. Stephen P. Wood et al., *The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles*, 52 SANTA CLARA L. REV. 1423, 1434 (2012); *see* Gurney, *supra* note 13, at 400-01. V2V technology is automobile technology that essentially lets vehicles communicate with each other by broadcasting their position, speed, and other data to nearby vehicles. *See* Olivia Marcus, *Car-to-Car Communication May Hit Roads Soon*, U.S. NEWS (Mar. 4, 2015, 5:00 PM), http://www.usnews.com/news/articles/2015/03/04/car-to-car-communication-may-hit-roads-soon. This information is then used to communicate with other vehicles to avoid crashes and accidents. *Id.* V2I technology, like V2V technology, is automotive technology that lets vehicles communicate

may produce information on other vehicles, traffic conditions, road work, and the like. This "enables a vehicle to sense threats and hazards . . . ; calculate risk; issue driver advisories or warnings; or take pre-emptive actions to avoid and mitigate crashes."[34] The global positioning system ("GPS") is an example of currently available technology that provides information not just useful for driving purposes but also potentially valuable for V2V and V2I communications.[35] Another example is lane departure warning, which alerts a driver when the vehicle begins to drift out of the lane of travel.[36]

Companies developing these types of autonomous vehicles include Google, Apple, Tesla, and Toyota.[37] The systems will use on-board technology to evaluate traffic conditions, make decisions, and take action while driving.[38] Since autonomous vehicles will require an incredible amount of information about the road to navigate safely, Tesla is not only mapping the roads but also each lane.[39]

B. Benefits and Uses That Support a Possible Smart Vehicle Market

The paramount benefit of autonomous vehicles, proven through testing, is increased road safety.[40] It is believed that driver error is the

---

with infrastructures by sharing data, such as stop light information. *See* Richard Read, *Vehicle-to-Infrastructure Technology, on the Road in Germany*, CAR CONNECTION (Oct. 24, 2012), http://www.thecarconnection.com/news/1080042_vehicle-to-infrastructure-technology-on-the-road-in-germany. This information is also used to prevent crashes and accidents. *Id.*

34. *What Public Officials Need to Know About Connected Vehicles*, U.S. DEP'T TRANSP., http://www.its.dot.gov/factsheets/pdf/JPO_PublicOfficials_v6.pdf (last visited Dec. 31, 2016).

35. *See* Wood et al., *supra* note 33, at 1429.

36. *Id.* at 1429-30 (describing lane departure warning as a system that does not intervene to prevent the driver from departing the lane, and merely monitors the lane markings on the road to determine whether the vehicle is keeping within the lane).

37. *See* Nathan Bomey, *Secret's Out: Toyota Also Making a Self-Driving Car*, USA TODAY, Oct. 7, 2015, at 2B; Associated Press, *Google Expects Public in Driverless Cars in 2 to 5 Years*, FOX NEWS (Jan. 15, 2015), http://www.foxnews.com/auto/2015/01/15/google-expects-public-in-driverless-cars-in-2-to-5-years.html ("Google is working on sensors to detect road signs and other vehicles, and software that analyzes all the data."); Fred Lambert, *Elon Musk on Tesla Fully Autonomous Car: 'What We've Got Will Blow People's Minds, It Blows My Mind . . . It'll Come Sooner Than People Think*,' ELECTREK (Aug. 3, 2016), https://electrek.co/2016/08/03/elon-musk-tesla-fully-autonomous-car-blows-mind; Nick Statt, *Apple Is Already Testing Self-Driving Cars Amid 'Reboot' of Project*, VERGE (Sept. 9, 2016, 9:02 PM), http://www.theverge.com/2016/9/9/12868610/apple-self-driving-electric-cars-titan-project-testing.

38. *See* Bomey, *supra* note 37.

39. *See* Chris Perkins, *Tesla Is Mapping the Earth, 'Cause Your GPS Won't Cut It for Self-Driving Cars*, MASHABLE (Oct. 14, 2015), http://mashable.com/2015/10/14/tesla-high-precision-digital-maps/#72vswY0ZEkqt. Tesla is creating this map by acquiring data through its drivers—each Tesla Model S is connected to the cloud where the cars contribute to the shared database called a fleet learning network. *Id.*

40. *See* Lauren Keating, *The Driverless Car Debate: How Safe Are Autonomous Vehicles?*, TECH TIMES (July 28, 2015, 9:00 AM), http://www.techtimes.com/articles/67253/20150728/

main reason behind over ninety percent of all crashes, with the main causes being "drunk driving, distracted drivers, failure to remain in one lane and [failure] to yield the right of way."[41] Recent research has also shown that the majority of accidents involving autonomous vehicles on the road were not the fault of the autonomous vehicle but, rather, caused by human inattention in the non-autonomous vehicle.[42] To illustrate, Google has revealed that other drivers have hit the firm's cars fourteen times since the start of their testing in 2009, and stated that "not once has the self-driving car been the cause of the collision."[43]

Reducing car accidents could also result in significant cost savings as automobile accidents in the United States cost around $400 billion per year—as measured in deaths, health care, property loss, insurance, and traffic congestion costs.[44] Additionally, autonomous vehicles would

---

driverless-cars-safe.htm. Since autonomous vehicles will be able to travel at a much higher speed and closer to other cars without the concern of hitting each other, the rate of traffic and congestion can be reduced. *Id.* This would lead to a decrease in the amount of time individuals spend traveling, while simultaneously increasing productivity since people do not actually have to drive cars. *Id.*; *see also* Andy Sharman, *Automated Autos May Be a Game Changer for Health and Safety*, FIN. TIMES (Dec. 13, 2015), https://www.ft.com/content/d6de9398-982b-11e5-95c7-d47aa298f769. Reducing the economic costs stemming from vehicle accidents can be achieved "by taking away control from the people who cause more than 90 percent of road accidents—human drivers." *Id.* Autonomous vehicles are a potential game changer for the health and safety of roads with their potential to reduce accidents because of their increased situation awareness. *Id.*

41. *See* Keating, *supra* note 40.

42. *See* Jerry Hirsh & Joseph Serna, *Cars Without Drivers Rack up Crashes; Human Error Is Cited in the Four Accidents Involving Self-Driving Cars Since September*, L.A. TIMES, May 12, 2015, at C1; *see also* Mark Prigg, *Google Self-Driving Car Is Involved in Its First Injury Accident: Tech Giant's Autonomous Car Is Rear-Ended Causing 'Minor Whiplash' to Three Employees*, DAILY MAIL (July 16, 2015, 6:30 PM), http://www.dailymail.co.uk/sciencetech/article-3164675/A-self-driving-SMASH-Watch-Google-s-autonomous-car-rear-ended-firm-admits-drivers-hitting-surprisingly-often.html. In addition, Google's cars have been driven more than 700,000 miles on public roads without causing a crash. *See* Associated Press, *supra* note 37. Although not an example of a level five full self-driving autonomous vehicle, there was an incident where the driver of an auto-pilot assist vehicle (Tesla Model S) crashed into an eighteen-wheel truck trailer—allegedly stemming from the auto-pilot driver's inattentiveness. *See* Sam Levin & Nicky Woolf, *Tesla Driver Killed While Using Autopilot Was Watching Harry Potter, Witness Says*, GUARDIAN (July 1, 2016, 1:43 PM), https://www.theguardian.com/technology/2016/jul/01/tesla-driver-killed-autopilot-self-driving-car-harry-potter.

43. *See* Prigg, *supra* note 42. *But see* Alex Davies, *Google's Self-Driving Car Caused Its First Crash*, WIRED (Feb. 29, 2016, 2:04 PM), https://www.wired.com/2016/02/googles-self-driving-car-may-caused-first-crash ("A public transit bus was approaching from behind. The Google AV test driver saw the bus approaching in the left side mirror but believed the bus would stop or slow . . . as the Google AV was reentering the center of the lane it made contact with the side of the bus.").

44. *See* Jeffery K. Gurney, *Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles*, 2013 U. ILL. J.L. TECH. & POL'Y 247, 251 (2013). The World Health Organization states that about 1,250,000 people die each year from car accidents, and that at least 20,000,000 people suffer non-fatal injuries in car accidents. *See Road Traffic Injuries*, WORLD HEALTH ORG., http://www.who.int/mediacentre/factsheets/fs358/en (last visited Dec. 31,

harmonize traffic flow and, in turn, increase fuel efficiency.[45] Using V2V and V2I technology, autonomous vehicles will be able to share information with each other better than human drivers and will benefit from what every other car has learned on the road.[46] Driving will become a networked activity, leading to greater cooperation and efficiency, rendering steering wheels, rear-view mirrors, and horns obsolete.[47] Vehicles on the market have already made some of this technology possible, as new cars such as the Tesla Model X have demonstrated the use of advanced sensors and software to detect an impending crash and automatically apply the brakes.[48]

C. Existing Law and Regulations Within the Sphere of Autonomous Vehicles

Congress enacted the National Traffic and Motor Vehicle Safety Act of 1966 ("Safety Act")[49] to reduce injuries and deaths resulting from operational and non-operational safety hazards attributed to motor vehicles.[50] A few years later, the NHTSA was established within the U.S. Department of Transportation, pursuant to the Highway Safety Act of 1970.[51] Much of the NHTSA's authority is derived from the Safety

---

2016); *Auto Crashes*, INS. INFO. INST. (Sept. 2016), http://www.iii.org/issue-update/auto-crashes (describing a statistic limited to information put together by the NHTSA).

45. *See* Gurney, *supra* note 44, at 251 (illustrating that this will help protect the environment and save consumers money—Americans used 2.8 billion gallons of excess gasoline totaling $87.2 billion in 2007 alone).

46. *See* Reid Hoffman, *Driving in the Networked Age*, LINKEDIN PULSE (July 18, 2015), https://www.linkedin.com/pulse/driving-networked-age-reid-hoffman (showing that present cars already act as network node driving apps like Waze, which uses smart phone GPS capabilities to crowd source real-time traffic levels, road conditions, and even gas prices).

47. *Id.* These benefits might be "so significant that in time the public will demand prohibitions against old-fashion driving in most public places." *Id.*

48. Timothy B. Lee, *Tesla's Model X SUV Is Ludicrously Fast and Ludicrously Expensive*, VOX (Sept. 30, 2015, 4:20 PM), http://www.vox.com/2015/9/30/9428011/tesla-model-x-explained. Other sensors on the Model X have additional capabilities, such as detecting the driver's approach and opening the doors automatically, as well as measuring the distance to objects both above and beside the vehicle when its falcon-wing doors open—these doors swing in an upward, folding fashion and compensate to avoid surrounding objects. *Id.*

49. National Traffic and Motor Vehicle Safety Act of 1966, Pub. L. No. 89-563, 80 Stat. 718 (repealed 1994). The Safety Act was originally codified in chapter 38 of title 15 of the U.S. Code. 15 U.S.C. §§ 1381–1431 (1988) (repealed 1994). Years later, the Safety Act was repealed by the Act of July 5, 1994, Pub. L. No. 103-272, 108 Stat. 745, but its substance was recodified in chapter 301 of title 49 of the U.S. Code. 49 U.S.C. §§ 30101–30183 (2012).

50. *See* 49 U.S.C. § 30101; 15 U.S.C. § 1381; Wood et al., *supra* note 33, at 1434-35.

51. Highway Safety Act of 1970, Pub. L. No. 91-605, § 2(a), 84 Stat. 1713, 1739 (repealed 1983); *see* 23 U.S.C. § 401 note (2012) (National Highway Traffic Safety Administration; Creation; Appointment of Administrator and Deputy Administrator; Duties; Retroactive Effect). The NHTSA's authority remained, pursuant to the Act of January 12, 1983, Pub. L. No. 97-449, § 1(b), 96 Stat. 2413, 2415 (codified as amended at 49 U.S.C. § 105).

Act, such as its power to set safety standards for motor vehicles and motor vehicle equipment and its control over the "recall and remedy of vehicles and equipment that do not comply with the standards in place at the time of manufacture."[52] A standard promulgated by the NHTSA must "be practicable, meet the need for motor vehicle safety, and be stated in objective terms."[53] In addition, 49 U.S.C. § 30102(b)(9) makes clear that each standard must relate to performance.[54]

The NHTSA, which has broad authority over motor vehicle safety, has been very active in promoting autonomous vehicles.[55] Since the development of autonomous vehicles is still in the early stages, the NHTSA remains deferential to individual states.[56] This is evidenced by the relative surge of state legislation that permits testing of autonomous vehicles.[57] However, none of this enacted legislation addresses any real future user operation of autonomous vehicles.[58] States have delayed

52. Wood et al., *supra* note 33, at 1435 (explaining that the NHTSA is also authorized to conduct investigations about possible safety defects); *see* 49 U.S.C. §§ 30101, 30111–30128. Further, a self-certification framework has been created to help ensure compliance—the NHTSA promulgates standards for motor vehicles and motor vehicle equipment and, in turn, manufacturers are required to certify that their products conform. 49 U.S.C. § 30115.

53. 49 U.S.C. § 30111(a).

54. *Id.* § 30102(a)(9); *see id.* §§ 30102(a)(8), 30111.

55. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 8, at 1-2 (reasoning that this statement is issued for the purpose of helping states implement the new autonomous vehicle technology safely so that its full benefits can be realized). The NHTSA has been conducting research on vehicle automation for many years—this research has lead to some regulatory and policy developments, including work on electronic stability control ("ESC"), and crash avoidance technologies such as lane departure warning and forward collision warning. *Id.* at 5-6. This has led to the development of standards that require mandatory ESC technology on all light vehicles, and reports on crash avoidance features that are noted on equipped models in a New Car Assessment Program—for the purpose of encouraging consumers to consider choosing specific models. *Id.*

56. *See id.* at 10 ("In general, we believe that states are well suited to address issues such as licensing, driver training, and conditions for operation related to specific types of vehicles."). However, the agency does express their preference that states not permit operation of autonomous vehicles for purposes other than testing based on many considerable concerns. *Id.*; *see also* William J. Kohler & Alex Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles*, 31 SANTA CLARA HIGH TECH. L.J. 99, 109-10 (2015) (noting that the NHTSA "does not appear ready to issue its own nationwide regulations specifically relating to autonomous vehicles").

57. *See* Kohler & Colbert-Taylor, *supra* note 56, at 112-18; *see also Autonomous: Self-Driving Vehicles Legislation*, NCSL (Dec. 12, 2016), http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx (stating that sixteen states introduced legislation relating to autonomous vehicles in 2015, compared with twelve states in 2014, nine states in 2013, and six states in 2012). Three states had already enacted legislation to legalize the operation of autonomous vehicles on public roads for testing purposes at the time the NHTSA issued its 2013 *Preliminary Statement of Policy Concerning Automated Vehicles*. Kohler & Colbert-Taylor, *supra* note 56, at 112.

58. *See* Kohler & Colbert-Taylor, *supra* note 56, at 120. Apart from pre-operation requirements, some states have only instituted "stipulations for insurance, safety mechanisms, and a human operator." *Id.* The state's enacted legislation has "either authorized the eventual deployment

passing autonomous vehicle laws until a liability scheme can be adopted.[59] In the next Subpart, this Note starts by introducing current federal law and regulation directly addressing autonomous vehicles, followed by an introduction of relevant state law and regulation.[60] Other federal laws that have an indirect influence on the regulation of autonomous vehicles will then be discussed.[61]

1. Possible Federal Laws and Regulations

There is currently no federal law or regulation explicitly prohibiting the use of autonomous vehicles outside the context of testing.[62] Therefore, from the NHTSA's recommendations, operating autonomous vehicles on public roads appears to be illegal in the absence of state or federal laws specifically authorizing their use.[63] It is important to note that "vehicle technologies that make autonomous operation possible are vastly different than those that existed when the Safety Act was enacted in 1966"—a time when "vehicle operating systems were largely mechanical and controlled by the driver via mechanical inputs and linkages."[64] In contrast, modern vehicles possess an ever-increasing number of electronic functions that can be controlled automatically by electronic control units, and the "operation of those units can be substantially altered by post-manufacture software updates."[65]

---

of autonomous vehicles for operation . . . or remained silent on the issue." *Id.*

59. *See* Gurney, *supra* note 44, at 250 (asserting that though some states have passed an autonomous vehicle law, no states have permitted driverless autonomous cars, yet). Arizona is among the states who delayed in passing such laws based on debates and controversial issues involving the assignment of liability should an accident occur. *See* Dan Strumpf, *Liability Issues Create Potholes on the Road to Driverless Cars*, WALL ST. J., Jan. 28, 2013, at B1.

60. *See infra* Part II.C.1–2.

61. *See infra* Part II.C.3.

62. Kohler & Colbert-Taylor, *supra* note 56, at 110.

63. *Id.* NHTSA recommends that states not permit operation of an autonomous vehicle for purposes other than testing for the time being. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 8, at 12-13, 14. *But see* Bryant Walker Smith, *Automated Vehicles Are Probably Legal in the United States*, 1 TEX. A&M. L. REV. 411, 413 (2014) (arguing that operating autonomous vehicles on public roads and highways is legal because they are not explicitly prohibited by any laws under the United States nor the Geneva Convention). However, Michigan is one state that recently enacted a ban on operation of autonomous vehicles outside the context of testing. *See* MICH. COMP. LAWS § 257.663 (2014).

64. *See* Wood et al., *supra* note 33, at 1438-39 ("Components and systems were either designed into the vehicle at the time of original manufacture or were later attached to or physically carried in the vehicle."); *see also* Jerry Flint & Douglas Flint, *The Real Cause of Toyota's Problems*, FORBES (Feb. 23, 2010, 5:33 PM), http://www.forbes.com/2010/02/23/flint-autos-toyota-business-recall.html. The article states, "In the old days incorrectly installed linkages or other mechanical problems, such as broken motor mounts" can cause runaway acceleration. Flint & Flint, *supra*. And, in the 1980s, although some car components became electronic, parts, like the throttle, were still a cable linkage to the gas pedal. *Id.*

65. *See* Wood et al., *supra* note 33, at 1439 (highlighting advances in communications

The NHTSA's authority extends to new motor vehicles and motor vehicle equipment. "Motor vehicle" is defined in 49 U.S.C. § 30102(a)(6) as "a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways."[66] "Motor vehicle equipment" is defined in 49 U.S.C. § 30102(a)(7) as follows:

> (A) [A]ny system, part, or component of a motor vehicle as originally manufactured; (B) any similar part or component manufactured or sold for replacement or improvement of a system, part, or component, or as an accessory or addition to a motor vehicle; or (C) any device or an article or apparel, including a motorcycle helmet and excluding medicine or eyeglasses prescribed by a licensed practitioner . . . .[67]

The definition of motor vehicle equipment is noticeably broader, and this effectively establishes the outer limits of the NHTSA's authority.

A federal privacy statute that governs personal information and may have a potential impact on autonomous vehicles is the Driver's Privacy Protection Act of 1994 ("DPPA").[68] The DPPA protects an individual's personal information held by a state's department of motor vehicles ("DMV") against disclosure without the written consent of that individual, unless a statutory exception applies.[69] A protected "motor vehicle record" is defined as "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles."[70] Although the DPPA seems to protect not only drivers but also their motor vehicle records, it is still important to point out that classification of a "driver" or "operator" in autonomous vehicles may be different.[71]

---

technology, making it possible for devices with vehicle-related capabilities to be compatible with the vehicle).

66. 49 U.S.C. § 30102(a)(6) (2012). Motor vehicle can include trailers but generally excludes vehicles that only use public roads for limited durations and vehicles that run exclusively on rails. *See* Wood et al., *supra* note 33, at 1439 n.48.

67. 49 U.S.C. § 30102(a)(7); *see* Wood et al., *supra* note 33, at 1439-40.

68. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 (codified as amended at 18 U.S.C. §§ 2721–2725 (2012)).

69. 18 U.S.C. § 2721; *see* Maracich v. Spears, 133 S. Ct. 2191, 2222 (2013) (holding that respondent lawyers' use of information from the department of motor vehicles fits within the exception delineated in § 2721(b)(4)). Subsection (b)(4) allows permissible use as follows:

> [I]n connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

18 U.S.C. § 2721(b)(4).

70. *Id.* § 2725.

71. *See infra* Part IV.B.

Numerous federal communications statutes may also apply depending on the technologies used in the autonomous vehicles, including the Electronic Communications Privacy Act ("ECPA"),[72] Telecommunications Act,[73] and Communications Assistance for Law Enforcement Act ("CALEA").[74] Under the Telecommunications Act, the consumer propriety network information ("CPNI") of autonomous vehicles, which includes information that relates to the quantity, technical configuration, destination, location, and amount of use of a telecommunications service subscribed, may be protected.[75] The CALEA might require telecommunications carriers, which includes autonomous vehicles if it should be classified as one, to facilitate law enforcement access to telecommunications networks.[76] It has been pointed out that since V2V might extend to V2I communication networks, which in turn are connected to the Internet or telephone systems, these communication networks would probably be subject to the CALEA requirements.[77] Regardless, the ECPA might permit law enforcement access to autonomous vehicle communications with a warrant.[78] Access to stored data in the vehicles based on a reasonable

72. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2511).

73. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

74. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 47 U.S.C. §§ 1001–1010 (2012)).

75. *See* 47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."); Glancy, *supra* note 15, at 679 (stating that CPNI is also made available to the carrier by the customer through a carrier-customer relationship).

76. *See* 47 U.S.C. § 1002(a) (requiring every telecommunications carrier to "ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—(1) expeditiously isolating and enabling the government . . . to intercept . . . all wire and electronic communications carried by the carrier within a service area"); Glancy, *supra* note 15, at 680 (highlighting that this could be done through CALEA solution switches that enable law enforcement interception). Additionally, the Federal Communications Commission, "which has jurisdiction to prescribe 'such rules as are necessary to implement' CALEA requirements, [has in the past,] extended the reach of CALEA [with] Voice over Internet Protocol (VoIP) and [other] facilities-based broadband." *Id.*

77. *See* Glancy, *supra* note 15, at 680 (reasoning that if first generation autonomous vehicles communicate only over V2V applications, they might very well avoid having to comply with law enforcement access through CALEA). However, V2I systems are connected to the Internet and public telephone systems, and such communications would be subject to CALEA requirements. *Id.*

78. *See* 18 U.S.C. § 2511(1)(a) (2012) (setting out punishment for "any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication"); Glancy, *supra* note 15, at 681 (agreeing that this existing privacy compromising law may permit law enforcement access to personal information and communications and would likely apply to autonomous vehicle communications);

belief that the records are relevant and material to a criminal investigation can be allowed under the Stored Communications Act.[79]

2. Mandated State Laws and Regulations

Dorothy J. Glancy states that "[f]irst generation autonomous cars will almost certainly have to comply with then-applicable state roadway laws and regulations" in the absence of federal preemption, since "each state owns and controls the highways and roadways within that state, including interstate highways."[80] States currently authorizing the testing of autonomous vehicles include California, Florida, Michigan, and Nevada.[81] When establishing these laws, the NHTSA recommended that states enforce four basic principles: (1) the process for transitioning from self-driver mode to driver control is safe, simple, and timely; (2) the self-driving test vehicles have the capability to detect, record, and inform the driver that the system of automated technologies has malfunctioned; (3) the installation and operation of any self-driving vehicle technologies not disable any federally required safety features or systems; and (4) the self-driving test vehicles record information about the status of the automated control technologies in the event of a crash or loss of vehicle control.[82] States have more or less followed these recommendations.[83]

---

see also Peter Van Valkenburgh, *What's So Bad About ECPA?*, TECH FREEDOM (Dec. 2, 2013), http://techfreedom.org/post/68822183836/whats-so-bad-about-ecpa (arguing that there are many problems with the ECPA actually protecting data—the ECPA is old, complicated and doesn't cover what it should). The ECPA does not make data obtained without a proper warrant inadmissible at trial. Van Valkenburgh, *supra*.

79. Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C §§ 2701–2712) (setting out punishment for "accesses without authorization [to] a facility through which an electronic communication service is provided," except for a required disclosure under § 2703); *see* Glancy, *supra* note 15, at 681 (stating that access to the stored data only requires a subpoena, or a court order under § 2703(d)); *see also* Kohler & Colbert-Taylor, *supra* note 56, at 125 (citing *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013)). In the context of a criminal investigation, and authorized under § 2703(d), the police did not commit a per se violation of the Fourth Amendment by requesting a court order requiring disclosure of historical location data without first obtaining a warrant or showing probable cause. *See In re U.S. for Historical Cell Site Data*, 724 F.3d at 602, 615.

80. Glancy, *supra* note 15, at 653 (believing that this makes the states' interest in regulation and use of state property strong); *see also* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 8, at 11-12 (providing recommendations for state regulations that govern the testing of self-driving vehicles).

81. *See Autonomous: Self-Driving Vehicles Legislation*, *supra* note 57; *see also* Jack Boeglin, *The Costs of Self-Driving Cars: Reconciling Freedom and Privacy with Tort Liability in Autonomous Vehicle Regulation*, 17 YALE J.L. & TECH. 171, 172-73 (2015) (explaining that even more states are considering similar legislative initiatives due to the high stakes involved from the amount of car crashes that occur every year).

82. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 8, at 13-14. The first principle recommends a driver who is familiar with the particular vehicle's automated systems and can "quickly and easily retake control of the vehicle from the automated system." *Id.* at 13. The second

Nevada was the first state to authorize the operation of autonomous vehicles for testing and defines an autonomous vehicle as one "equipped with autonomous technology" that "has the capability to drive the motor vehicle without the active control or monitoring of a human operator."[84] Nevada further required the vehicle be equipped with safety measures, including a means of easily engaging and disengaging the autonomous technology and a mechanism of alerting the human operator to take control if the autonomous technology fails.[85] Other regulations adopted by Nevada require that there be special driver's license certification and plates, pre-operation certifications, and an insurance deposit of $5,000,000.[86] This requires the state DMV to set up a regulation for establishing driver license endorsement for the operation of an autonomous vehicle on the highways of the State.[87]

Florida enacted legislation incorporating testing provisions similar to Nevada regarding autonomous vehicles, with nearly identical language in defining autonomous vehicle technology.[88] Florida defines an operator to include someone who causes the "autonomous technology to engage, regardless of whether or not that person is physically present

---

principle recommends the vehicles have this capability of recording such occurrences so that it can be easy to "establish the cause of any such malfunction, degradation and control failure." *Id.* The third principle says federal laws should prohibit manufacturers, dealers, and repairman of motor vehicles from "making inoperative any federally required [safety] system[]." *Id.* The fourth principle suggests a regulation which would require the "vehicle owner make available to the state all data recorded by the vehicle [EDR] in the event of a crash." *Id.* at 14.

83. *See infra* Part II.C.2.

84. NEV. REV. STAT. §§ 482A.025, .030 (2014) (adding that autonomous technology does not include an active safety system nor a system for driver assistance "including . . . a system to provide electronic blind spot detection, crash avoidance, emergency braking, parking assistance, adaptive cruise control, lane keeping assistance, lane departure warning, or traffic jam and queuing assistance," unless the vehicle with which such system is installed can utilize the system without driver assistance or monitoring); *see* Kohler & Colbert-Taylor, *supra* note 56, at 113 (stating that Nevada was also the first state to require its DMV to propose autonomous vehicle regulations).

85. NEV. REV. STAT. § 482A.080 ("An autonomous vehicle shall not be registered in this State unless the autonomous vehicle meets all federal standards and regulations that are applicable to a motor vehicle.").

86. *Id.* § 482A.060 (requiring proof of insurance or self-insurance acceptable to the DMV in the amount of $5 million before the person can begin testing an autonomous vehicle on a highway in the state). An electronic data recorder, for storing information about the condition of the vehicle system for at least thirty seconds prior to an accident, separate from the NHTSA-mandated EDR, might also be one of the requirements. *See* NEV. ADMIN. CODE § 482A.110 (2014); *see also* Kohler & Colbert-Taylor, *supra* note 56, at 113.

87. NEV. ADMIN. CODE § 482A.200.

88. *See* Kohler & Colbert-Taylor, *supra* note 56, at 114 (highlighting similarities such as required safety measures, surety deposit, and the release of liability for vehicle manufacturers). *Compare* FLA. STAT. § 316.003(90) (West 2014), *with* NEV. REV. STAT. §§ 482A.025, .030 (showing identical language).

in the vehicle while [it operates] in autonomous mode."[89] Legislation enacted in California also uses language similar to that of Nevada and Florida but with additional specifications with regards to liability.[90] California defines the manufacturer of an autonomous vehicle as the one who "originally manufactures [the] vehicle and equips [the vehicle with] autonomous technology," whether or not that person is the original manufacturer of the underlying vehicle.[91] In addition, the original manufacturer is not released from liability resulting from third-party installation of autonomous technology, and there is no designation that a third-party installer is liable for defects.[92] Like Nevada, the vehicle must also contain a separate device that stores autonomous technology sensor data for thirty seconds before a crash, which must be made available for three years after the accident.[93]

Michigan passed legislation permitting operation of autonomous vehicles for testing purposes but is the only state to specifically ban operation for non-testing purposes.[94] Before testing, Michigan requires registration of special license plates, and the vehicle can only be operated by an employee or other person authorized by the automated technology manufacturer.[95] Michigan incorporates civil penalties for violating autonomous vehicle laws, which include "remov[ing] 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."[96] Other laws that were passed also

89. FLA. STAT. §§ 316.85(2), .86(1) (adding that such operators, for the purposes of testing the vehicle, include employees, contractors, or other persons designated by manufacturers of autonomous technology).

90. CAL. VEH. CODE § 38750 (West 2014). An additional specification includes sensor data from accidents be captured, stored, and preserved for three years after the date of collision in a read-only format. *Id.* § 38750(c)(1)(G).

91. *Id.* § 38750(a)(5) ("A 'manufacturer' of autonomous technology is . . . [also] the person that modifies the vehicle by installing autonomous technology to convert it to an autonomous vehicle after the vehicle was originally manufactured.").

92. *See* Kohler & Colbert-Taylor, *supra* note 56, at 115; *see also* Boeglin, *supra* note 81, at 174 (stating that although California originally stipulated that "'the conversion of vehicles originally manufactured by a third party shall control issues of liability arising from the operation of an autonomous vehicle,' the legislation struck this provision on reconsideration").

93. *Compare* CAL. VEH. CODE § 38750(c)(1)(G), *with* NEV. ADMIN. CODE § 482A.110 (2014) (showing similar language).

94. MICH. COMP. LAWS § 257.663 (2014) (providing that a "person shall not operate an automated motor vehicle upon a highway or street in automatic mode" unless operation falls under a section 665 exception—for the purpose of research or testing the autonomous vehicle).

95. *Id.* §§ 257.244(3), .665(2)(a). Much like the other states, the individual, who has the ability to monitor the vehicle's performance, must also be present in the vehicle while it is being operated such that immediate control of the vehicle's movement is possible when necessary. *Id.* § 257.663(2)(b).

96. *Id.* § 257.666; Kohler & Colbert-Taylor, *supra* note 56, at 118.

require that autonomous vehicles cede operational authority to human users whenever a human user requests control, despite motivation from legal and economic pressures that might eventually restrict the frequency and scope of human driving.[97] Additional laws were motivated by the threat autonomous vehicles pose to user privacy.[98] For example, California demands that the "manufacturer of the autonomous [vehicle] technology . . . provide a written disclosure to the purchaser of an autonomous vehicle that describes what information is collected by the autonomous technology equipped on the vehicle."[99]

Despite early action taken by some states to regulate autonomous vehicles on their public roads, many other states have attempted but failed to pass such bills.[100] Arizona introduced legislation that would not require a person to be seated in an autonomous vehicle—a major difference from the states that have enacted laws.[101] This bill failed to clear Arizona's House Transportation Committee.[102] In 2015, the Oregon legislature failed to pass a bill through their Transportation Committee because of concerns over the unforeseeable risks of automated vehicles.[103] New Jersey's proposed legislation also failed to clear their own committee after Scott Mackey, a representative from the

---

97. CAL. VEH. CODE § 38750(c)(1)(D) (requiring the autonomous vehicle to "allow the operator to take control in multiple manners, including . . . the use of the brake, the accelerator pedal, or the steering wheel" while alerting the operator that autonomous mode has been disengaged); NEV. ADMIN. CODE § 482A.190(2)(g); *see* Boeglin, *supra* note 81, at 173 (highlighting the fact that automobiles have stood as a symbol of freedom and personal autonomy for generations); Philip E. Ross, *Driverless Cars: Optional by 2024, Mandatory by 2044*, IEEE SPECTRUM (May 29, 2014, 11:00 AM), http://spectrum.ieee.org/transportation/advanced-cars/driverless-cars-optional-by-2024-mandatory-by-2044 (arguing that autonomous vehicles might be so common that humans will be forced into the passenger seat).

98. *See infra* note 99 and accompanying text.

99. CAL. VEH. CODE § 38750(h); *see* Boeglin, *supra* note 81, at 174 (suggesting that the potential of autonomous vehicles infringing on privacy is so grave that self-driving cars should be prohibited altogether). In a poll regarding such privacy matters, seventy-five percent of respondents were concerned that companies would use software that controls a self-driving car to collect personal data, and seventy percent were worried that data would be shared with the government. *See* Joseph B. White, *The Big Worry About Driverless Cars? Losing Privacy*, WALL ST. J. (June 3, 2013, 1:46 PM), http://blogs.wsj.com/drivers-seat/2013/06/03/the-big-worry-about-driverless-cars-losing-privacy. In addition, eighty-one percent of the respondents were either very or somewhat concerned about the threat that hackers could gain control of a self-driving vehicle. *Id.*

100. *See Autonomous: Self-Driving Vehicles Legislation*, *supra* note 57 (listing Connecticut, Idaho, Maryland, Mississippi, Missouri, Oregon, and Texas among states that introduced legislation in 2015 but failed to enact the bill); *see also* Kohler & Colbert-Taylor, *supra* note 56, at 118-19 (believing that such failure illustrates some of the issues that stand in the way of universal state acceptance of autonomous vehicles).

101. *See* H.B. 2167, 51st Leg., 1st Reg. Sess. (Ariz. 2013).

102. *See* Kohler & Colbert-Taylor, *supra* note 56, at 118.

103. S.B. 620, 78th Leg., 1st Reg. Sess. (Or. 2015); *see* Kohler & Colbert-Taylor, *supra* note 56, at 119; *Autonomous: Self-Driving Vehicles Legislation*, *supra* note 57.

Alliance of Automobile Manufacturers, said that state legislation on automated vehicles was premature.[104] He believed that "if each state enacted slightly different regulations, it would [make it] difficult for manufacturers to standardize the technology for the wider market."[105] Mackey's statements suggest that federal, rather than state, regulations for autonomous vehicles can promote their use more quickly.[106]

3. Vehicle Law or Computer Law?

Autonomous vehicles may also be incidentally influenced by other existing federal and state criminal laws.[107] An attack might be staged by exploiting a vehicle's electronic control unit, either physically or through the V2V or V2I communication systems.[108] Such an attempt to exploit and gain control over an electronic control unit would likely subject the attacker to federal criminal liability under the Computer Fraud and Abuse Act of 1986 ("CFAA"),[109] Digital Millennium Copyright Act ("DMCA"),[110] and USA PATRIOT Act ("PATRIOT Act").[111]

An electronic control unit, which is a high-speed data processing device performing logical, arithmetic, or storage functions, may qualify as a "protected computer" pursuant to the CFAA.[112] The electronic

---

104. *See* Kohler & Colbert-Taylor, *supra* note 56, at 119; *see also* Andrew George, *Driverless Cars . . . in N.J.? Assembly Panel Considers Legislation Authorizing Tests*, NJBIZ (Nov. 25, 2013, 3:16 PM), http://www.njbiz.com/article/20131125/NJBIZ01/131129789/driverless-cars—in-nj-assembly-panel-considers-legislation-authorizing-tests (stating that Scott Mackey believes the prospect of driverless cars on the road is still ten years away).

105. *See* Kohler & Colbert-Taylor, *supra* note 56, at 119.

106. *Id.* Other statements include that "it would be best if there was a broader approach." George, *supra* note 104.

107. *See* Gurney, *supra* note 13, at 410-11 (asserting that autonomous vehicles will implicate criminal laws—including vehicle-related criminal laws, and those not necessarily related to vehicles, but will intersect with autonomous vehicles—because the technology is operated by a computer); *see also* Kohler & Colbert-Taylor, *supra* note 56, at 133-34.

108. *See* Kohler & Colbert-Taylor, *supra* note 56, at 133-34. An attack can be carried out by exploiting the vehicle's EDR system, which is accessible wirelessly and communicates remotely with other response towers. *Id.*; *see also* Balough & Balough, *supra* note 5, at 3.

109. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

110. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17, 28 U.S.C.); *see* 17 U.S.C. § 512 (2012).

111. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S.C.).

112. 18 U.S.C. § 1030(e)(1)–(2); *see* Balough & Balough, *supra* note 5, at 3 (highlighting that, even if the vehicle itself is not a protected computer, the pathway for hacking the electronic control unit may involve a protected computer). When a person takes the vehicle to a dealership for maintenance, he or she connects that vehicle to the dealer's computer—the dealer's computer is a protected computer under the CFAA since it is connected to the Internet. Balough & Balough, *supra* note 5, at 3; *see also* Gurney, *supra* note 13, at 439-41 (stating that an autonomous vehicle's

control unit must be deemed "a computer . . . used in or affecting interstate or foreign commerce."[113] Vehicles, of course, have the ability to travel across state lines, and their electronic control units could thereby be viewed as "affecting" interstate commerce. A case of this type could involve, for example, a hacker who willfully took control over a vehicle's electronic control system with the intent to endanger the safety of occupants.[114] Further, commercial autonomous vehicles could be "used in" interstate commerce based on the Supreme Court's "in commerce" language, which encompasses "persons or activities within the flow of interstate commerce—the practical, economic continuity in the generation of goods and services for interstate markets and their transport and distribution to the consumer."[115] Hacking a vehicle would also violate the DMCA, which "prohibits [the] circumvention of technological measures to gain access to a copyrighted work."[116] Although the PATRIOT Act does not directly provide for autonomous vehicle cyberterrorism, it addresses cyberterrorism via cars, terrorist attacks, and other acts of violence against mass transportation systems, and it adds a class to the CFAA—"threat[s] to public health or safety."[117] Therefore, it is possible to violate the PATRIOT Act if hacking an autonomous vehicle is classified as a threat to public health or safety.[118]

Existing criminal laws may prohibit tampering with autonomous vehicles and their supporting infrastructure by users or outsiders.[119]

---

computer system qualifies as a computer under the CFAA because it is an electronic device that performs logical functions).

113. 18 U.S.C. § 1030(e)(2)(B); Balough & Balough, *supra* note 5, at 3 (noting that, if a computing issue occurs in a single state, the "used in" interstate commerce clause is not satisfied).

114. *See* Gurney, *supra* note 13, at 440.

115. United States v. Am. Blg. Maint. Inds., 422 U.S. 271, 276 (1975) (quoting Gulf Oil Corp. v. Copp Paving Co., 419 U.S. 186, 195 (1974)). With respect to corporations, "[t]o be engaged 'in commerce' within the meaning of § 7 [of the Clayton Act], a corporation must itself be directly engaged in the production, distribution, or acquisition of goods or services in interstate commerce." *Id.* at 283; *see* Gurney, *supra* note 13, at 441 (believing that the defendants in an action for hacking a vehicle need to raise the question of "whether the vehicle was 'used, operated, or employed in interstate commerce'").

116. 17 U.S.C. § 506(a)(1) (2012); Balough & Balough, *supra* note 5, at 3-4 (referencing MDY Industries, LLC v. Blizzard Entertainment Inc., 629 F.3d 928, 945 (9th Cir. 2010)). A party seeking to use the DMCA against an electronic control unit hacker must show the vehicle contains technological measures that effectively control access. *Id.*

117. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(IV).

118. *Id.*; *see also* Balough & Balough, *supra* note 5, at 4 (explaining that mass transportation systems include "passenger vessels, railroads, intercity bus transportation, school buses, and charter and sightseeing transportation, but it does not mention private passenger vehicles or trucks").

119. *See* 49 U.S.C. § 32703 (2012) (stating, inter alia, that a person may not install a device "that makes an odometer of a motor vehicle register a mileage different from the mileage the vehicle was driven, as registered by the odometer within the designed tolerance of the manufacturer of the odometer"); MINN. STAT. § 609.546 (2016) (making it a misdemeanor for those who

Some states have anti-hacking laws that cover more than just physical trespassing or vandalism.[120] For example, New York sets out computer tampering by degree—computer tampering in the fourth degree occurs when a person "uses, causes to be used, or accesses a computer, computer service, or computer network without authorization and he or she intentionally alters in any manner or destroys computer data or a computer program of another person."[121]

Depending on the situation, a hacker could also be charged with kidnapping.[122] For example, South Carolina's kidnapping statute states that "[w]hoever shall unlawfully seize, confine, inveigle, decoy, kidnap, abduct or carry away any other person by any means whatsoever without authority of law . . . is guilty of a felony."[123] Therefore, a hacker that changed the route of an occupied autonomous vehicle could potentially be convicted of kidnapping the occupants in that vehicle.[124]

III. THE NECESSITY OF PROPER REGULATION AGAINST POTENTIAL HACKERS OF AUTONOMOUS VEHICLES

With the immense benefit of road safety outlined in Part II, it is believed that the main concern of autonomous vehicles is not from the potential onset of unclear tort liabilities in connection with autonomous vehicle road accidents but from the emergence of potential hackers to this new technology.[125] This Part first introduces the potential vulnerabilities of autonomous vehicles in relation to hacking.[126] Then, it

---

intentionally "tamper[] with or enter[] into . . . a motor vehicle without the owner's permission").

120. N.Y. PENAL LAW § 156.05 (McKinney 2010) (making it a misdemeanor for a person who "knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization").

121. *Id.* § 156.20.

122. *See, e.g.*, MISS. CODE ANN. § 97-3-53 (2016) (making it unlawful for any person to "forcibly seize and confine any other person, or . . . inveigle or kidnap any other person with intent to cause such person to be confined or imprisoned against his or her will"); *see also* N.C. GEN. STAT. § 14-39 (2006) (punishing "[a]ny person who shall unlawfully confine, restrain, or remove from one place to another"); S.C. CODE ANN. § 16-3-910 (1976).

123. S.C. CODE ANN. § 16-3-910; *see* State v. Porter, 698 S.E.2d 237, 243 (S.C. Ct. App. 2010) ("Kidnapping is a continuous offense that commences when one is wrongfully deprived of freedom and continues until freedom is restored.").

124. *See* Gurney, *supra* note 13, at 438.

125. *See* John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, N.Y. TIMES, Mar. 10, 2011, at B3 (highlighting how new cellular channels offered by electronic control units in vehicles offer many areas of exploitation for hackers); *see also* Andy Greenberg, *How Hackable Is Your Car? Consult This Handy Chart*, WIRED (Aug. 6, 2014, 6:30 AM), http://www.wired.com/2014/08/car-hacking-chart; Alexis C. Madrigal, *When Cars Are as Hackable as Cell Phones*, ATLANTIC (Sept. 8, 2014), http://www.theatlantic.com/technology/archive/2014/09/when-cars-are-as-hackable-as-cell-phones/379734.

126. *See infra* Part III.A.

follows with a discussion of how current laws and ideas do not adequately address these vulnerabilities.[127]

A. Problems and Concerns with Autonomous Vehicle Vulnerability Could Prove Explosive

Autonomous vehicles are a major hacking concern, because unlike an ordinary desk computer, these vehicles are physically vulnerable and easily accessible by hackers.[128] This could lead to major problems and concerns such as privacy, terrorist attacks, call-efficiency motivated attacks,[129] slow criminal prosecution with no effective method of deterrence, unclear liability issues, and other crimes such as kidnapping.[130] Senator Ed Markey has devoted attention to the vulnerability of connected vehicles to cyberattacks, stating that the vehicles could be hijacked and controlled to stage attacks by modifying the operation of the vehicle.[131] The potential vulnerabilities of autonomous vehicles that are introduced in the following Subparts

---

127. *See infra* Part III.B.

128. *See* Greenberg, *supra* note 125 (highlighting these vulnerabilities with a ninety-two-page paper presented at a Black Hat security conference—the paper presents results from dozens of different car makes and models, accessing vehicle schematics, and rating vehicles for potential hackability from their networked components).

129. *See* Gerdes et al., *supra* note 13, at 99 (defining call-efficiency motivated attacks to be an attack on a single vehicle, which yields data other autonomous vehicles utilize to operate). Thus, slowing down the single vehicle would in turn slow down an entire pack of autonomous vehicles—known as a platoon—on the road based on automated vehicle response. *Id.*; *see also* David A. Cornelio Sosa, An Efficiency-Motivated Attack Against Vehicles in a Platoon: Local Vehicle Control, Platoon Control Strategies, and Drive Train Technologies Considerations 14 (May 1, 2014) (unpublished M.S. dissertation, Utah State University) (on file with the Merrill-Cazier Library, Utah State University) (suggesting that vehicle platooning is a malicious attack, which can be the result of a company trying to sabotage the operation of another's vehicles to make it spend more energy than required and, thus, raise its transportation costs).

130. *See* Gurney, *supra* note 13, at 437-38 ("Depending on the situation, a hacker could also be charged with kidnapping."); Kohler & Colbert-Taylor, *supra* note 56 at 133 (explaining that remote hijacking of autonomous vehicles presents a very serious risk—for instance, traffic signals are rendered obsolete by the possibility of coordinating the flow of traffic through intersections, and traffic from two perpendicular lanes could be made to cross paths without any vehicles slowing down or coming to a stop); *see also* Frank Douma & Sarah Aue Palodichuk, *Criminal Liability Issues Created by Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1157, 1165 (2012) (discussing several degrees of culpability from third-party interference).

131. *See* SEN. ED MARKEY, TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 5 (2015), http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf (presenting data from 2011 by a group of researchers, which showed that wireless entry points in automobiles pose vulnerabilities—they were able to remotely hack into a vehicle and exploit these vulnerabilities, which included engaging in location tracking and eavesdropping, and controlling different features such as the locks and brakes).

include privacy concerns, terrorist attacks, drug trafficking, kidnapping, and the lack of established criminal laws to deter hackers.[132]

1. Data Use in Autonomous Vehicles and Its Overlap with the Right to Privacy

Privacy is a critical legal implication of autonomous vehicles, and it is made especially so with the implementation of V2V and V2I communication systems.[133] The interconnected vehicle presents risks to personal information by engaging in constant network communication at the user's real-time location.[134] In addition, potential data breaches may cause this personal information to be extracted, hacked, or leaked.[135] Autonomous cars "could compromise the users' privacy by transmitting not only 'the present location of an autonomous vehicle user and past travel patterns' but also 'his or her future travel plans,' which could be employed for 'targeted marketing,' 'law enforcement,' or 'surveillance.'"[136] V2V and V2I technology can potentially send internal vehicle status information through an external network, thereby subjecting users to greater risk of having this information compromised and improperly used.[137]

The privacy interests of the people regarding personal information will pose major challenges, as potential autonomous vehicle users will be reluctant to allow their information to be collected without knowing the inherent consequences.[138] This is especially true today after the

---

132. *See infra* Part III.A.1–2.

133. *See supra* Part II.C.3.

134. *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1180 (2012) (stating that the network on which interconnected, autonomous vehicles would rely would be used for surveillance on every other interconnected vehicle); *Connected Cars Roll into Privacy Concerns*, INFOSECURITY MAG. (Jan. 18, 2014), http://www.infosecurity-magazine.com/news/connected-cars-roll-into-privacy-concerns (informing the public that Ford engages in constant network communication at the user's real-time location using GPS chips in the vehicle).

135. *See* Glancy, *supra* note 134, at 1180 (emphasizing that robust personal information protection and network security measures are needed to guard against privacy risks).

136. *See* Boeglin, *supra* note 81, at 181 (determining that a vehicle is more likely to threaten its passengers' safety if the vehicle is "communicative"—a communicative vehicle can relay vehicle information to third parties, receive driving instructions from external sources, and speak with other autonomous or communicative vehicles in its vicinity).

137. *See id.* Boeglin emphasizes the vulnerability of these networks by showing that over 300,000 wireless routers were hacked in 2014. *Id.*; *see also* Dan Goodin, *Hackers Hijack 300,000-Plus Wireless Routers, Make Malicious Changes*, ARS TECHNICA (Mar. 3, 2014, 2:42 PM), http://arstechnica.com/security/2014/03/hackers-hijack-300000-plus-wireless-routers-make-malicious-changes.

138. *See* Natasha Singer, *Sharing Data, but Not Happily*, N.Y. TIMES, June 5, 2015, at B1 (highlighting a study from the Annenberg School for Communication in which the majority of Americans do not believe the trade-off of their personal data for giveaways and discounts is a fair deal).

National Security Administration leak—more people have started to change privacy settings on their social media accounts, showing that many do care about their personal privacy.[139] This is potentially an expansion of *United States v. Jones*[140] and would raise Fourth Amendment issues involving law enforcement interaction with autonomous vehicles.[141] Possible cases include that of a dishonest police officer having a "wide latitude to remotely pull over vehicles."[142] It could be argued, from a public safety perspective, "that by operating an autonomous vehicle a person lessens his reasonable expectation of privacy typically associated with driving a car."[143]

It is expected that autonomous vehicles will require operation of a "black box" used to reconstruct events should an incident occur, as "data collected by the black boxes has already been the center of litigation by law enforcement agencies . . . seeking to use the information against car owners."[144] Vehicles today are equipped with black boxes that record information typically only accessed after traffic accidents.[145] This and other data recorded by vehicles are usually also gathered by car companies.[146] The pressing concern is not what the car company might do with the data but what the government might be able to demand of the car company, knowing that it possesses such data.[147] As some have illustrated, "surveillance data collected by private entities can easily be subpoenaed or otherwise obtained by law enforcement agencies, without

---

139. *See* Byron Acohido, *Snowden Effect: Young People Now Care About Privacy*, USA TODAY (Nov. 18, 2013, 2:52 PM), http://www.usatoday.com/story/cybertruth/2013/11/13/snowden-effect-young-people-now-care-about-privacy/3517919. A poll was commissioned by an information technology security company, ESET, which revealed that young people actually do care about the privacy of their online personas. *Id.*

140. 132 S. Ct. 945 (2012).

141. *Id.* at 949 (holding that a GPS device used to monitor a vehicle's movements constitutes a search under the Fourth Amendment).

142. *See* Douma & Palodichuk, *supra* note 130, at 1167 (stating that giving law enforcement officers the ability to force a vehicle pull over is potentially a seizure under the Fourth Amendment and a "slippery slope").

143. *Id.* (illustrating a scenario where a young child is trapped inside a hacked or malfunctioned vehicle that is misbehaving).

144. *See* Trop, *supra* note 18. The black box is a recorder that collects information like direction, speed and seatbelt use in a continuous loop. *Id.* It is in nearly every car today, and has brought up privacy concerns on the part of the public. *Id.*

145. *See* Douma & Palodichuk, *supra* note 130, at 1168.

146. *See* Thierer & Hagemann, *supra* note 17, at 382 (discussing a Ford executive's comments and response to questions about their data collection).

147. *Id.* Ford had said, "[W]e know everyone breaks the law, we know when you're doing it. We have a GPS in your car, so we know what you're doing . . . [but] we don't supply that data to anyone." Jim Edwards, *Ford Exec: 'We Know Everyone Who Breaks the Law' Thanks to Our GPS in Your Car*, BUS. INSIDER (Jan. 8, 2014, 8:16 PM), http://www.businessinsider.com/ford-exec-gps-2014-1.

a warrant or probable cause."[148] These concerns are not unique to autonomous vehicles, but they may forestall innovation and regulation if not properly addressed.[149]

2. Dangers Arising from Criminal Acts and Opportunity

Hackers may stage an attack by exploiting a vehicle's electronics, such as its event data recorder ("EDR") system.[150] This could pose a serious risk by coordinating the flow of traffic through intersections, and making real time speed adjustments, causing significant damage and disruption.[151] The impact is magnified by the fact that each vehicle could be used as a bomb and controlled to target specific locations or civilians—far more dangerous than the situation in *United States v. McVeigh*,[152] where a rental truck packed with explosives was identified after the defendant had left the scene.[153] The opportunities presented by autonomous vehicles "[are] unprecedented in the way that [they] could allow terrorists to quickly strike targets miles away from their current location."[154] Without serious regulation of these vehicles, the first line of defense would be regulating the sale and distribution of explosive material by a sort of tracking.[155] With further progression, providing law enforcement officials with tracking information may not only justify a more reasonable basis of suspicion that would allow law enforcement to search these vehicles but may also allow them to pull over or disable a suspected vehicle en route.[156]

---

148. *See* Eugene Volokh, *Tort Law vs. Privacy*, VOLOKH CONSPIRACY (Nov. 25, 2013, 2:59 PM), http://volokh.com/2013/11/25/tort-law-vs-privacy.

149. *See* Thierer & Hagemann, *supra* note 17, at 383 (illustrating that concerns over privacy are not unique to the ongoing development of autonomous vehicles, as many non-autonomous smart vehicles already have similar concerns).

150. *See* Kohler & Colbert-Taylor, *supra* note 56, at 133.

151. *Id.*

152. 940 F. Supp. 1541 (D. Colo. 1996).

153. *Id.* at 1545-46 (examining that the defendant was thought to have had an explosive device in his truck, prompting investigators to evacuate all occupants from an area north of where the truck was parked); *see* Kohler & Colbert-Taylor, *supra* note 56, at 133 ("Many autonomous vehicles being hijacked at once in an urban center could lead to terror on the scale of the September 11 attacks.").

154. *See* Douma & Palodichuk, *supra* note 130, at 1165-66. Another issue includes using autonomous vehicles to deliver drugs to an obscure meeting place—the option is attractive because in the event that the cargo is discovered, there would be no driver to arrest. *Id.*

155. 6 U.S.C. § 1203 (2012) (providing rules governing hazardous material highway routing); *see* Douma & Palodichuk, *supra* note 130, at 1166 (explaining that this tracking of information may provide a reasonable basis to allow law enforcement to search a vehicle before it reaches its target).

156. *See* Douma & Palodichuk, *supra* note 130, at 1166-67.

As first generation autonomous vehicles begin to operate on public roads, a number of existing criminal offenses will naturally apply to autonomous vehicles.[157] However, it is emphasized that these traditional legal concepts and applications may be challenged, as autonomous vehicles can create difficult issues in criminal law, such as determining when criminal penalties should apply to vehicle hacking that produces undesirable consequences.[158] In the United States, deterrence is one theory of punishment that society uses to police itself.[159] Under this theory, punishment serves as a function to dissuade potential criminals from committing crimes in the first place.[160] However, the dissuasion of crimes arising from hacking autonomous vehicles remains absent.[161] The technological concepts are relatively new, and many of the problems discussed in this Subpart, such as privacy and terrorist concerns, are not yet adequately addressed by the U.S. government.[162] For example, would the need for evidence used to prosecute hackers require that operators of autonomous vehicles turn over personal information to law enforcement officials since the right is not covered under the Fourth Amendment or would a warrant be required as in *Riley v. California*?[163] The answer to this question would undoubtedly impact resources associated with criminal prosecution.[164]

In addition, if hackers find it easy to stage attacks with a small likelihood of getting caught or having a severe punishment imposed, there would be no incentive for hackers to stop if the destructive impact of their crime is greater than the cost of their punishment.[165] As seen

---

157. *See supra* Part III.A.

158. *See* Glancy, *supra* note 15, at 662-63 (explaining that it is likely for autonomous vehicles to change existing models of local traffic regulation that relies on "low-level criminal sanctions for deterrence of a wide spectrum of anti-social behavior"). The first wave of autonomous vehicles may lead to the legislative creation of new crimes, most of which may primarily be enforced by state and local governments. *Id.* at 663.

159. *See* Gurney, *supra* note 13, at 404 (stating that the overriding objectives of criminal law are "to make people do what society regards as desirable and to prevent them from doing what society considers to be undesirable"); *see also* WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 1.5 (West Group 2d ed. 2014).

160. *See* LAFAVE, *supra* note 159.

161. *See* Michele Cotton, *Back with a Vengeance: The Resilience of Retribution as an Articulated Purpose of Criminal Punishment*, 37 AM. CRIM. L. REV. 1313, 1316 (2000) (emphasizing that deterrence treats punishment as a tool of social control and protection by dissuading criminals from offending).

162. *See supra* Parts II.A–B, III.A.2.

163. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014) (holding that a warrantless search and seizure of digital content on a cell phone is unconstitutional).

164. *See infra* Part IV.D–E.

165. *See supra* note 161 and accompanying text; *see also* Gurney, *supra* note 13, at 404-06 (adding that the punishment should be proportional to that of the offense). The punishment for speeding is proportional to the speed—or the potential to inflict harm—and also depends on if

previously, the ability to use autonomous vehicles to commit crimes is substantial, and no clear formulation on this class of criminal liability has been established through any federal or state laws relating to autonomous vehicles.[166] Many more complex crimes, such as kidnapping and drug trafficking, may arise out of hacking autonomous vehicles.[167] Problems include determining whether the act of kidnapping would be included with hacking into a vehicle and taking control of the vehicle with someone in it.[168] Therefore, the question becomes, to what extent could hackers be prosecuted under other criminal laws?[169] For instance, if the hacker uses the vehicle to kill the occupants of the autonomous vehicle, or a bystander, what would be the measure used to prosecute that hacker for murder?[170]

Another area of potential criminal exploitation includes call-efficiency motivated attacks.[171] Call-efficiency motivated attacks focus on causing targeted vehicles to expend excessive energy during travel with the intent of decreasing the efficiency gains of other autonomous vehicles driving with them.[172] An incentive for such an attack might come from one company seeking to reduce its competitor's profit margins by increasing its costs for transportation.[173] It is worth noting that this problem depends on a certain conception of how autonomous vehicles might operate—namely that a group of vehicles will cooperate to act as one unit while following one another at fixed speeds.[174]

---

anyone was harmed. *See* Gurney, *supra* note 13, at 406. This theory should hold true at the intersection of criminal law and vehicles, including autonomous vehicles. *Id.*

166. *See supra* Parts II–III.

167. *See* Douma & Palodichuk, *supra* note 130, at 1165-66; *see also* Gurney, *supra* note 13, at 437. To dealers, the drastic reduction of being physically caught while delivering drugs would be a "welcome buffer." *See* Douma & Palodichuk, *supra* note 130, at 1165-66.

168. State v. Porter, 698 S.E.2d 237, 244 (S.C. Ct. App. 2010) (finding that it is possible to base a conviction for kidnapping on the restraint of the employees and customers that was incidental to the armed robbery).

169. *See* Gurney, *supra* note 13, at 433-38 (listing various ways hackers could be prosecuted under other criminal laws, including being charged for joyriding, grand larceny, or even murder). In addition, both federal and state governments would be able to prosecute a hacker as long as an applicable statute applies. *See id.* at 436-37.

170. *See id.* at 438.

171. *See supra* note 129 and accompanying text.

172. *See* Gerdes et al., *supra* note 13, at 107; Thierer & Hagemann, *supra* note 17, at 376.

173. *See* Gerdes et al., *supra* note 13, at 100; Thierer & Hagemann, *supra* note 17, at 376.

174. *See* Thierer & Hagemann, *supra* note 17, at 376 (stating that this concern only applies in the context of a "platoon framework," which depends on a narrow conception, and a very specialized form of attack that would occur only in the rarest cases).

B. Current Laws and Ideas Do Not Adequately Address These Autonomous Vehicle Problems and Concerns

Pursuant to its statutory authority, the NHTSA can craft standards to effectively regulate the implementation of automated vehicle technology.[175] These standards can be established as the automotive industry releases the technology.[176] Congress, however, has imposed requirements for a standard to be valid: it must be practicable and reasonable, it must increase motor vehicle safety, and it must be stated in objective terms.[177] The definitional criteria further requires that the standard relates to performance.[178] Lawmakers and scholars alike have searched for solutions to the hacking concerns that surround autonomous vehicles.[179] Many solutions prove inadequate when analyzed in circumstances surrounding the effective establishment of the hacker's criminal liability.[180] As previously mentioned, there is a substantial amount of failed local legislation on autonomous vehicles.[181] The inadequate amount of concrete legislation relating to specific civil liability arising from autonomous vehicles undoubtedly creates a huge gap to even start considering how to address specific criminal liability.[182]

1. Inadequacies of Law, Legislation, and Other Efforts in Relation to the Autonomous Vehicle Cybersecurity Issue

There is considerable federal and state legislation relating to computer hacking, transportation, and crimes that may naturally apply to autonomous vehicles.[183] The extent to which these laws may apply to relieve concerns outlined in the previous Subpart are explored.[184] This Subpart returns to potential laws that may influence privacy and security, which includes the DPPA, Telecommunications Act, ECPA, and CALEA.[185] It is important to note that the possibilities of

175. *See supra* Part II.C.

176. *See, e.g.*, Kohler & Colbert-Taylor, *supra* note 56, at 134-38 (emphasizing that barriers to achieve successive levels of automation must be ameliorated to arrive at levels two and three, and eventually eliminated to arrive at level four—levels as defined by the NHTSA's 2013 *Preliminary Statement of Policy Concerning Automated Vehicles*).

177. 49 U.S.C. § 30101(a) (2012).

178. *Id.* § 30102(a)(9).

179. *See infra* Part III.B.

180. *See infra* Part III.B.

181. *See supra* Part II.C.2.

182. *See supra* Part II.C.

183. *See supra* Part II.C.

184. *See supra* Part III.A.

185. *See supra* Part II.C.1.

certain laws applying, specifically those discussed in Part II, are only possibilities, even when viewed extensively.[186]

The DPPA does not point out whether a "driver" or an "operator" of an autonomous vehicle falls under the Act from the protection of personal information held by state DMVs.[187] It is also unclear whether the Telecommunications Act and the CALEA would cover the CPNI of autonomous vehicles, since the information in autonomous vehicles might not be classified as information that relates to the use of telecommunications services despite the fact V2V might extend to V2I communications.[188] Plus, even if it is assumed that the ECPA applies to autonomous vehicle communications, it does not necessarily provide a suitable ground for consumers to know the extent to which their personal information is protected or whether law enforcement officials would be able to sufficiently obtain information for prosecution of autonomous vehicle crimes.[189] The NHTSA's proposed measures would also be ineffective since, for now, they are purely standards for lawmakers to follow.[190] In fact, the NHTSA has said that before autonomous vehicles can be made widely available, a number of technological issues, as well as some human performance issues, must be addressed.[191] The NHTSA believes that autonomous vehicle technology is not yet at the necessary stage of sophistication or demonstrated safety capability.[192]

---

186. *See supra* Part II.

187. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 (codified as amended at 18 U.S.C. §§ 2721–2725 (2012)).

188. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C. §§ 1001–1010 (2012)); *see also* 47 U.S.C. § 222 (privacy of customer information).

189. Electronic Communication Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2511).

190. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 27, at 11-82; Wood et al., *supra* note 33, at 1447-48 (stating that although the NHTSA's authority over autonomous driving systems is broad, it is still currently faced with the challenge of determining effective ways of regulation).

191. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 8, at 14 ("As innovation in this area continues and the maturity of self-driving technology increases, we will reconsider our present position on this issue.").

192. *Id.* The NHTSA has also requested further information from the public on evaluating the potential safety benefits of V2V technology and whether complementary technology can enable self-driving vehicles over time. *See* Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 49,270, 49,275 (Aug. 20, 2014) (to be codified at 49 C.F.R. pt. 571).

2. Inadequacies of Proposals in Relation to the Autonomous Vehicle Cybersecurity Issue

In addition to current laws relating to autonomous vehicles, there have been proposals and ideas by legislatures and legal scholars. Legislators attempted to regulate autonomous vehicles by implementing safety standards, on a national level, to the vehicles' new technology.[193] The Geolocational Privacy and Security Act,[194] Online Communications and Geolocation Protection Act,[195] and Driver Privacy Act[196] have been attempts at a preemptive framework to govern access to data gathered by a vehicle's EDR and geographical tracking data.[197] The proposed legislation could require government agencies to show probable cause warrants to obtain geolocational information.[198] One potential approach to "addressing privacy and security concerns entails each [autonomous vehicle] being issued unique security certificates."[199] This would involve implementing a system for certifying each transmitter of information in a vehicle to ensure that the transmitter is a trusted source.[200] But the broadcasting of a unique security certification by each vehicle still raises concerns that the system could be used to track individual drivers.[201] Since it is unclear what shape autonomous vehicle innovation will take in the coming years, forbearance has also been considered to be a wise move at this time.[202] However, it does not solve the problem.[203]

---

193. Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. at 49,270.

194. Geolocational Privacy and Surveillance Act, S. 237, 114th Cong. (2015).

195. Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013).

196. Driver Privacy Act, S. 1925, 113th Cong. (2014).

197. S. 237 ("[T]o specify the circumstances in which a person may acquire geolocation information and for other purposes."). This is, in some ways, an expansion to what the ECPA minimally provides, to cover geolocation information pertaining to another person, in addition to any wire, oral, or electronic communication. *See supra* note 77 and accompanying text; *see also* H.R. 983 (setting to amend title 18 of the U.S. Code, "with respect to disclosures to governments by communications-related service providers of certain information consisting of or relating to communications"); S. 1925 (declaring any data retained by a vehicle's EDR is the property of the owner or lessee of the vehicle, regardless of when the vehicle was manufactured).

198. *See* Glancy, *supra* note 15, at 682 (highlighting that the Geolocational Privacy and Security Act could prohibit businesses from disclosing geographical tracking data, as well as provide guidelines for when such data can be accessed).

199. *See* Wood et al., *supra* note 33, at 1471.

200. *Id.*

201. *Id.* (emphasizing that taking steps to reduce vulnerability of autonomous vehicles will affect public acceptance).

202. *See* Thierer & Hagemann, *supra* note 17, at 388-89 (believing this is true in light of how rapidly technologies develop and the challenges posed to preemptively craft rules to keep pace); *see also* JAMES M. ANDERSON ET AL., RAND CORP., AUTONOMOUS VEHICLE TECHNOLOGY: A GUIDE FOR POLICYMAKERS 103 (2016), http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-2/RAND_RR443-2.pdf. Anderson argues that regulatory promulgation is fundamentally a slow process, and newness and rapid evolution in technology creates uncertainty in

Another proposed measure would be to amend the hacking, transportation, and criminal laws to address the potential problems with autonomous vehicles.[204] There are not only related federal laws, but many transportation and criminal laws specific to each state which could be applicable to autonomous vehicle hacking.[205] Amending each of these state specific laws, and some relevant federal laws, is an onerous task and would still leave regulation of autonomous vehicles scattered across many different jurisdictions.[206] The federal government may preempt state laws by creating its own regulations of autonomous vehicles.[207] Some believe that Congress could enact a statute that would apply uniformly nationwide to first generation vehicles and perhaps all other types of autonomous vehicles.[208] The hypothetical statute would consolidate all federal authority relating to autonomous vehicles into a single federal agency, delegate to the agency power to govern matters relating to autonomous vehicles, govern civil and criminal liability standards for cases involving autonomous vehicles, and establish a body of federal autonomous vehicle privacy protection requirements.[209]

3. Vehicle Manufacturer Efforts to Improve Security Systems

It is worth noting that manufacturers have powerful reputational and economic incentives, and companies like Chrysler and Ford are already working to improve their systems as to better compartmentalize the ability of hackers to gain access.[210] Security vulnerabilities have also been addressed by "utilizing two-way data-verification schemes . . . , routing software installs and updates through remote servers to check, and double-check, for malware, adopting routine security protocols like encrypting files with digital signatures, and other experimental

---

both rulemaking effects and of the technology itself. ANDERSON ET AL., *supra*.

203. *See* ANDERSON ET AL., *supra* note 202, at 105-06.

204. *See infra* Part IV.

205. *See supra* Part II.C.3.

206. *See supra* Part II.C.3.

207. U.S. CONST. art. VI, cl. 2; *see* Julie Goodrich, Comment, *Driving Miss Daisy: An Autonomous Chauffeur System*, 51 HOUS. L. REV. 265, 292 (2013) (adding that Congress had used its "general welfare and national security powers to create the Department of Transportation," whose goals include encouraging national and local governments to improve transportation).

208. *See* Glancy, *supra* note 15, at 686-90 (proposing a solution that would be based on U.S. congressional power to regulate interstate commerce).

209. *Id.*

210. *See* Thierer & Hagemann, *supra* note 17, at 377. The failure of an autonomous car has serious implications on human safety and is a serious reputational risk for the manufacturer if its vehicle is involved in an accident as people are more likely to take issue with car manufacturers. *See* GILLIAN YEOMANS, LLOYD'S, AUTONOMOUS VEHICLES: HANDING OVER CONTROL: OPPORTUNITY AND RISKS FOR INSURANCE 16 (2014), https://www.lloyds.com/~/media/lloyds/reports/emerging%20risk%20reports/autonomous%20vehicles%20final.pdf.

treatments."[211] Interestingly, this private-sector experimentation and research may likely become a de facto baseline for security settings due to the slow movement of government research and budget constraints.[212] Based on this information, it is important to continuously improve response mechanisms towards the security issues, which includes both combining new technological capabilities against hacking with that of anticipatory legislation and preemptive regulatory planning.[213]

IV. INTRODUCTION OF A FEDERAL AUTONOMOUS VEHICLE SAFETY AND PROTECTION ACT REQUIRING A SPECIAL LICENSE FOR COMMERCIAL AUTONOMOUS VEHICLE OPERATION

Current criminal, hacking, privacy, and transportation laws outlined in Part III may indeed solve the cybersecurity issue by allowing law enforcement access to vehicle data.[214] However, they would at the same time, alone, raise troubling issues relating to controversial Fourth Amendment rights.[215] Therefore, there is a need to seamlessly allow law enforcement expedited access to autonomous vehicle data, without having to prompt serious privacy issues—which may be accomplished by requiring a special license to operate an autonomous vehicle.[216] To effectively accomplish this goal and address the autonomous vehicle cybersecurity issue, it is necessary to craft an act that clarifies the categories of autonomous vehicle crimes while also allowing law enforcement more flexibility when obtaining evidence for criminal prosecution.[217] It will be shown that such regulation is necessary, and consent for this type of transparency should be required for all owners and operators of autonomous vehicles.[218] For additional efficiency, the proposed act will modify only federal law and have a federal preemption clause that would preempt not only state and other local statute regulations, but also common law rules.[219]

---

211. Thierer & Hagemann, *supra* note 17, at 377; *see* Keith Berry, *Can Your Car Be Hacked?*, CAR & DRIVER (July 2011), http://www.caranddriver.com/features/can-your-car-be-hacked-feature ("[A]utomakers are beginning to take steps to secure networks the same way the information-technology sector now locks down corporate servers.").

212. *See* Thierer & Hagemann, *supra* note 17, at 377-78.

213. *Id.* at 378.

214. *See supra* Part III.

215. *See supra* Part III.A.1.

216. *See infra* Part IV.D–E.

217. *See* Glancy, *supra* note 15, at 686-90 (proposing a hypothetical national autonomous vehicle act for the purposes of promoting development and adoption of autonomous vehicle technologies by reducing legal risks and uncertainties).

218. *See infra* Part IV.E.

219. *See* Geier v. Am. Honda Motor Co., 529 U.S. 861, 886 (2000) (holding that the common law tort action is preempted since the potential common law liability interferes with the regulatory

This Note proposes a federal law entitled the Autonomous Vehicle Safety and Protection Act ("AVSA"), which would create and amend multiple provisions within title 49 of the U.S. Code.[220] For purposes of this Note, the AVSA, at a minimum, defines and addresses autonomous vehicles, establishes a federal agency to oversee all regulatory programs of autonomous vehicles, defines a category of persons, characterizes crimes associated with autonomous vehicle hacking, describes a person's rights with regard to privacy and status, and requires an autonomous vehicle license ("AVL") for operators and owners.[221] Additionally, amendments will be offered for classifying criminal conduct under title 18.[222] Federal regulation of autonomous vehicles is the most effective option, in light of the failure in establishing consistent state regulation for the testing of these vehicles.[223]

A. Establishment of a Federal Agency Overseeing All Matters Concerning Autonomous Vehicles

Implementation of a federal statute will authorize the creation of a federal agency that is made part of the U.S. Department of Transportation, and it oversees all regulatory programs regarding autonomous vehicles.[224] This can be done with AVSA creating a section within title 49 that defines the National Autonomous Vehicle Safety Administration ("NAVSA"), which would follow similar language to that of the NHTSA in 49 U.S.C. § 105.[225] NAVSA would be an administration in the Department of Transportation and have its own Administrator and Secretary of Transportation to carry out chapter 301 of this title alongside the NHTSA—limited to matters concerning autonomous vehicles, and deferring decisions on any conflicts to the Department of Transportation.[226] The amendment to 49 U.S.C. § 105 would require the NHTSA to consult with NAVSA on all matters related to autonomous vehicles.[227] Although, originally, the NHTSA would have authority under the statute to address these concerns, the amendment

---

methods chosen by the federal government to achieve the Safety Act's stated goals).

220. *See infra* Part IV.A.

221. *See infra* Part IV.A–E.

222. *See infra* Part IV.C.

223. *See supra* Part II.C.2.

224. *See* Glancy, *supra* note 15, at 688-89.

225. 49 U.S.C. § 105 (2012).

226. *See* Glancy, *supra* note 15, 688-89. The U.S. Department of Transportation would be reorganized, and "[j]urisdiction over regulatory programs regarding autonomous vehicles would be transferred from the Federal Motor Carrier Safety Administration, the Federal Transit Administration, the Federal Highway Administration, and NHTSA." *Id.* at 688.

227. *See supra* notes 224-25 and accompanying text.

would prevent the NHTSA from being overburdened by the introduction of this new technology.[228] The amendment would read:

> The Administrator shall consult with the Federal Highway Administrator on all matters related to the design, construction, maintenance, and operation of highways. *The Administrator shall consult with the National Autonomous Vehicle Safety Administration on all matters related to autonomous vehicles.*[229]

B. Defining Categories of Persons Within the Act

The AVSA would also define categories of persons that could potentially be touched by vehicular security issues, such as the hacker, operator, owner, mechanic, car manufacturer, tech manufacturer, and insurance company.[230] This could be expressed in 49 U.S.C. § 30102. At a minimum, the NAVSA would define "autonomous motor vehicle" and "operator."[231] The general definitions would read:

> *(11) "Autonomous motor vehicle" means a vehicle driven or drawn by mechanical or electrical power, and manufactured primarily for use on public streets, roads, and highways. The vehicle also has full-self driving automation, where the driver solely provides destination or navigation input, without being expected to be available for control at any time during the trip.*
> *(12) "Operator" means the driver of an autonomous motor vehicle.*[232]

---

228. *See* Glancy, *supra* note 15, at 688-89 (stating that a statute can be used to delegate to the new federal agency both legislative and adjudicative power to govern all matters related to autonomous vehicles).

229. 49 U.S.C. § 105(e).

230. *See* Boeglin, *supra* note 81, at 185 (discussing liability, including particular parties that may be held liable for an accident caused by an autonomous vehicle). This can include the user, owner, vehicle manufacturer, parts manufacturer, or even a government entity. *Id.*; *see also* Goodrich, *supra* note 207, 288-89 (stating that it is important to clarify those who are "operating" the vehicle, and those who "operate the vehicle in a meaningful way" to solve problems of civil and criminal liability). In the case the vehicle is operated in a meaningful way, the fault most likely falls on the automator or the manufacturer based on mistake or negligence. *Id.*

231. 49 U.S.C. § 30102.

232. *See id.* ("'[M]otor vehicle' means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways, but does not include a vehicle operated only on a rail line."); NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 27, at 9-10 (categorizing fully automated vehicles in level five); *see also* Goodrich, *supra* note 207, at 288-89 (emphasizing that it is important to clarify the operator); Gurney, *supra* note 13, at 411 (stating that there are different levels of blameworthiness on the part of a traditional driver, versus an operator—as such, it is recommended that traditional drivers and autonomous vehicle operators be treated differently).

C. Crime Characterization and Classification Within the Act

Hacking an autonomous vehicle is merely one crime that could be included in the AVSA. Vehicle tampering and call-efficiency motivated attacks can be considered their own category of crimes as well.[233] More complex crimes will arise out of vehicle hacking, such as kidnapping, drug trafficking, or use of an explosive or incendiary device, which would all need to be distinguished when prosecuting offenders.[234] Codifying these laws will deter potential violators from attempting to take over an autonomous vehicle.[235]

Given the amount of potential crimes arising from the sole crime of hacking an autonomous vehicle, it would be wiser to codify or amend that sole crime.[236] It is unnecessary to go through each potential crime already codified under title 18 to clarify its relation to autonomous vehicles.[237] Moreover, categorizing autonomous vehicle crimes as federal crimes would be more effective considering the large variations in state law and the strong interstate nature of vehicle hacking.[238] This Note proposes an amendment to 18 U.S.C. § 1030 that intends to increase the scope of fraud and related activity in connection with computers past those already given under the CFAA.[239] More specifically, 18 U.S.C. § 1030 would include in its list under the term "computer" to also mean a motor vehicle or an autonomous vehicle.[240] It is unnecessary to clarify that all other crimes arising out of this section involving unauthorized access to a motor vehicle or an autonomous vehicle are punishable, in addition to the initial hacking crime.[241] This is inherently established U.S. law.[242] For illustrative purposes, other crimes

---

233. *See* Goodrich, *supra* note 207, at 286-87 (recommending that the criminal legal system should codify laws relating to autonomous vehicles, including laws that prohibit "virtual carjacking and essentially equating the crime with today's prohibitions against manual carjacking"); *see also* Gurney, *supra* note 13, at 411 (examining at least four types of criminal laws that may be implicated by autonomous vehicles and might require clarity: (1) general traffic laws, (2) DUI laws, (3) reckless driving and due care laws, and (4) vehicular manslaughter).

234. *See supra* note 165 and accompanying text.

235. *See* Goodrich, *supra* note 207, at 286-87.

236. *See supra* Part III.A.2.

237. *See supra* Part III.A.2.

238. *See supra* Part II.C.3.

239. 18 U.S.C. § 1030 (2012).

240. *Id.* § 1030(e) (defining a computer as an "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device").

241. *See* MODEL PENAL CODE § 1.07(1) (AM. LAW INST., Proposed Official Draft 1962) ("When the same conduct of a defendant may establish the commission of more than one offense, the defendant may be prosecuted for each such offense.").

242. *Id.*

can include those listed within the same title: explosives (chapter 39);[243] kidnapping (chapter 55);[244] or stolen property (chapter 113).[245] In addition, 18 U.S.C. § 1030(c)(2)(B)(ii) takes into consideration greater punishment under the initial hacking crime for an "offense [that] was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[246] It is recommended that 18 U.S.C. § 1030 impose even greater penalties for offenses committed in furtherance of any criminal or tortious act in relation to unauthorized access to a motor vehicle or an autonomous vehicle.[247]

D. The Scope of the Right to Privacy and Operator Requirements

Beneficial to the proposed regulations mentioned above, and in consideration of the grave impact associated with the potential crimes, the legal system should also codify laws which may allow law enforcement officials better access to autonomous vehicle data stored in the vehicle system and in local state departments.[248] The privacy concerns and issues associated with the emergence of this new technology will have to be adequately addressed or circumvented.[249] Autonomous vehicles include operator personal information—from components like EDRs—which may need to be used by law enforcement officials when prosecuting criminals.[250] If officials have a hard time getting around privacy concerns with respect to vehicle operators in obtaining access to this data, criminal prosecution becomes slow and deterrence of autonomous vehicle crimes would be very ineffective.[251] Therefore, there is a strong interest to allow some way for law enforcement officials to delicately overcome some privacy issues.[252]

---

243. 18 U.S.C. § 831.

244. *Id.* § 1201.

245. *Id.* § 2312.

246. *Id.* § 1030(c)(2)(B)(ii) (providing punishment for fraud and related crimes in connection with computers).

247. *See* Gurney, *supra* note 13, at 441-42 (stating that the federal government is in the best position to prosecute hackers, and that regulators should amend criminal laws in such a way to provide for a smooth transition of autonomous vehicles into the marketplace).

248. *See supra* Part III.B.2.

249. *See* Glancy, *supra* note 134, at 1172-73 (explaining that in the future, autonomous vehicles will need to accommodate privacy interests, which can include autonomy privacy interests, personal information privacy interests, and surveillance privacy interests). The future success of autonomous vehicles will very much depend on how well privacy interests and autonomous vehicles can work together. *Id.* at 1239.

250. *See supra* Part III.A.2.

251. *See supra* Part III.A.2.

252. *See infra* Part IV.D–E.

Given that autonomous vehicle computer systems and data are continuously connected and transmitting data, most data records will likely be stored at state DMVs.[253] As mentioned, this data will include information recorded from a vehicle EDR, GPS, and anything mandated by law, including accident reconstruction data.[254] Therefore, limiting the protection provided by DPPA would be a possible approach given that it protects an individual's personal information held by the state DMV against disclosure, without the written consent of that individual, unless a statutory exception applies.[255] The statutory exception can be implemented in this statute or another statute. Specifically, chapter 123 of title 18 of the U.S. Code can be amended to include such a statutory exemption.

In 18 U.S.C. § 2721(b), Congress already provides for government access of "personal information" or "highly restricted personal information" for cases "in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; [and] performance monitoring of motor vehicles and dealers by motor vehicle manufacturers."[256] The pertinent disclosures include those "[f]or use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions," and "in connection with any civil, criminal, administrative, or arbitral proceeding in any . . . court or agency . . . including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court."[257] Though these pertinent disclosures encompass both personal information and highly restricted personal information, clarification and an expansion of what can be included are still needed.[258] This will require an amendment to 18 U.S.C. § 2725, which defines personal information to include data from autonomous

253. *See* 18 U.S.C. § 2721 (2012) (prohibiting some release of personal information by a state's DMV). Information includes information that identifies an individual—such as an individual's "photograph, social security number, driver identification number, name, address . . . telephone number, and medical or disability information." *Id.* § 2725(3). Highly restricted personal information can include an individual's social security number, and medical or disability information. *Id.* § 2725(4).

254. *See* Trop, *supra* note 18; *see also* 18 U.S.C. § 2725(3) (excluding information on vehicular accidents, driving violations, and driver's status).

255. 18 U.S.C. § 2721; *see* Glancy, *supra* note 134, at 1204 ("Simply not having personal information—through limiting personal information . . . helps to minimize these [privacy] risks.").

256. 18 U.S.C. § 2721(b)(2).

257. *Id.* § 2721(b)(1), (4).

258. *Id.* § 2721(a).

vehicle EDR, GPS, accident reconstruction software, and anything deemed relevant by NAVSA.[259]

Next, consider the information that is retained in private company databases.[260] It is recommended to ask to whom such data might be transmitted, and under what circumstances, as well as to distinguish between the degrees of personally identifiable information.[261] It has been noted that these specific privacy concerns "can be remedied by a combination of private self-regulation, tort law . . . consumer watchdog pressure and press attention."[262]

Finally, there is also information that could remain with the vehicle, which has not been transferred to the local state department because of a possible delay or incident.[263] Access to this information would be outside the scope of the DPPA and likely requires balancing access to the information with that of a reasonable search or seizure under the Fourth Amendment.[264] If, however, that information was required to be transferred to the local state department—where the government could nonetheless access it under chapter 123 of title 18—there would not actually be a violation of a person's reasonable expectation of privacy by accessing the same information under comparable means.[265] Therefore, for this particular case, further specific expansions to the ECPA, CALEA, and Telecommunications Act should be considered but not enacted at this time—it would be too early at this stage to start applying specific solutions to clarify the privacy doctrines for access to vehicle information until it is seen if the technology proceeds as currently expected.[266] This Note's proposed amendments can also have an indirect

259. *Id.* § 2725.

260. *See supra* Part III.B.3.

261. *See* Thierer & Hagemann, *supra* note 17, at 383 (stating that the transmission of very personally identifiable information raises more legitimate privacy concerns).

262. *Id.* at 383-84 (highlighting, for example, that the Future of Privacy Forum launched a Connected Cars Project to promote practices in privacy and data security that would best recognize the benefits of the new vehicle technology).

263. *See* Glancy, *supra* note 134, at 1180 (discussing self-contained autonomous vehicles, where personal information would be concentrated on-board the vehicle). This personal information contained in the vehicle could potentially be accessed by investigators, both private and governmental. *Id.*

264. 18 U.S.C. § 2721. The DPPA only protects personal information gathered by state DMVs. *Id.* Balancing tests (as opposed to bright line tests) have been used in many privacy cases in which the law enforcement need is weighed against an individual's right to privacy, but such tests have never been applied to the situation at hand. *See, e.g.*, Michigan v. Summers, 452 U.S. 692, 704-06 (1981) (considering factors such as the safety of the officer and the preservation of evidence).

265. 18 U.S.C. § 2721.

266. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 27, at 21 (stating that more research needs to be done before enacting a regulatory standard in relation to the cybersecurity issues); *see also* Thierer & Hagemann, *supra* note 17, at 388-89. Forbearance at this stage is suitable. *See id.* Many of the suggested security and privacy concerns may never materialize, and

impact on these doctrines, providing all the more reason to wait and see how this emerging technology will begin to shape the law.[267]

In addition, the recommended policies "should not be converted into a regulatory straitjacket that uniformly mandates data collection and use practices according to a centralized blueprint. In the future, some automakers . . . might craft creative data-sharing policies that provide . . . [a] myriad [of] unanticipated benefits."[268] Flexible and evolving practices for data collection—not just for autonomous vehicles but all developing technology—would ultimately better serve consumers and society.[269] Policymakers need not respond to these issues preemptively and should be mindful that the right answers might not be available at this time.[270] Another real challenge concerning an individual's reasonable expectation of privacy arises when a situation requires law enforcement officials to engage in a vehicle pullover.[271] The AVSA needs to allow some level of permission for certain officials to authorize vehicle pullovers—while avoiding controversial privacy issues, so that important evidence may be quickly obtained or if it would be necessary to stop a live vehicle that may be suspected of being hijacked.[272] Generally, a law enforcement official can pull over the vehicle if she has probable cause to believe a traffic violation has occurred.[273] This Note does not address the question of whether a federal or state official is allowed to pull over and search an autonomous vehicle based on what is potentially a violation of existing federal law. Rather, it recommends autonomous vehicle pullovers be delegated to a specific federal agency and that pullovers and searches be required by owners and operators of autonomous vehicles under a more flexible probable cause standard, as a condition of obtaining an AVL.[274] This would be effective in circumventing, and even solving, the controversial issue of

---

society may very well quickly adapt to a world filled with autonomous vehicles, based on adequate initial regulation or, even, universal acceptance by the public. *Id.*

267. *See* Thierer & Hagemann, *supra* note 17, at 389 (stating that creative solutions may have to be pursued as issues develop since it is impossible to anticipate every possible issue, concern, or scenario in advance).

268. *Id.* at 385.

269. *Id.* at 385-86 ("Serendipitous discoveries can only materialize in a policy environment that embraces trial and error experimentation.").

270. *Id.* at 386.

271. *See* Douma & Palodichuk, *supra* note 130, at 1166 (expressing that the prospect of a law enforcement officer having the ability to pull over and track movements of any suspected vehicles will increase public concern).

272. *See* Glancy, *supra* note 15, at 686-90 (hypothesizing that it is possible to establish a body of "federal autonomous vehicle privacy protection requirements," which would preempt state privacy laws that would otherwise apply in the context of autonomous vehicles).

273. *See* Whren v. United States, 517 U.S. 806, 810 (1996).

274. *See infra* Part IV.E.

whether or not it is necessary to bolster Fourth Amendment constraints on governmental attempts to access data from autonomous vehicles.[275]

E. Characterizing the Application and Extent of Autonomous Vehicle Licenses

Much like how licenses have been required to test autonomous vehicles in the past years, it would also be effective, and consistent with present regulation, to require a specific license to operate them.[276] This may potentially resolve privacy concerns operators and owners might have.[277] The license would require all autonomous vehicle operators and owners to comply with the relevant state and federal regulations, including those implemented under AVSA.[278] In the United States, driver licenses are issued individually by each state's DMV rather than by the federal government based on each state having their own domestic laws with regard to driving.[279] However, the national concerns with regard to autonomous vehicles support a recommendation for imposing a more uniform standard for AVLs.[280] Federal requirements can be applied to each state's licensing requirements, requiring those who want to own or operate an autonomous vehicle to meet federal standards for issuance by the state or, perhaps, federal government.[281]

Proceeding from how a license is made a requirement to test an autonomous vehicle, California is wrestling with the question of how it may require motorists to undergo additional instruction or evaluation before they can operate these vehicles.[282] This includes classroom

---

275. *See infra* Part IV.E.

276. *See* Mary Slosson, *Google Gets First Self-Driven Car License in Nevada*, REUTERS (May 8, 2012, 6:39 AM), http://www.reuters.com/article/2012/05/08/uk-usa-nevada-google-idUSLNE84701320120508 (stating that since the DMV licensed a Toyota Prius modified by Google, Nevada plans to eventually license autonomous vehicles owned by members of the public); *see also* S. 343, 217th Leg., Reg. Sess. (N.J. 2016) (proposing legislation to require that "[a] person shall not operate an autonomous vehicle in autonomous mode unless that person has obtained an endorsement on that person's driver's license to operate an autonomous vehicle").

277. *See supra* Part III.A.1.

278. *See supra* Part IV.A.

279. *See Driver's Guide to Licenses, Registration & DMV Locations*, DMV.ORG, http://www.dmv.org/drivers-guide (last visited Dec. 31, 2016).

280. *See supra* Part III.A.

281. *See supra* Part IV.

282. *See* Mark Harris, *Will You Need a New License to Operate a Self-Driving Car?*, IEEE SPECTRUM (Mar. 2, 2015, 10:00 AM), http://spectrum.ieee.org/cars-that-think/transportation/human-factors/will-you-need-a-new-license-to-operate-a-selfdriving-car; *see also* Kirsten Korosec, *Kia Motors' Road to Self-Driving Cars Goes Through Nevada*, FORTUNE (Dec. 15, 2015, 11:10 AM), http://fortune.com/2015/12/15/kia-self-driving-cars; Beth Stebner, *Look, No Hands! Google's Self-Driving Cars Set to Hit the Roads of Nevada After Being Granted Licence*, DAILY MAIL (May 8, 2012, 9:19 AM), http://www.dailymail.co.uk/sciencetech/article-2141308/Google-driverless-car-

lessons on the abilities and limitations of autonomous technologies, computer simulations of failures, and real-world driving sessions—all of which could be made as a pre-requisite for obtaining an AVL.[283] Despite the view that individuals have compared an autonomous vehicle with that of a train or a bus which may eliminate the need for a license completely, individuals that hold this view assume that no driver intervention will be allowed and that no external interference will occur.[284] The California DMV released a set of proposed guidelines: (1) a person may not operate an autonomous vehicle unless that person has a driver's license, and obtains a certificate to operate the vehicle; (2) a licensed operator would be required to sit in the driver's seat, ready to take over should an event that requires immediate attention occurs; and (3) the driver would also be liable for any roadway violations.[285] This sort of a requirement for drivers can be made a national standard, where AVL requirements can be proposed by NAVSA and enforced by federal enforcement agencies or even local state departments.[286]

V. CONCLUSION

The most efficient method to address the cybersecurity concerns associated with the hacking of autonomous vehicles is to implement a federal statute that preempts state and common law regulations.[287] The issues that develop from the emergence of autonomous vehicles are too

---

licence-Self-driving-cars-set-hit-Nevada-roads.html (explaining that Google's cars will display red plates and an infinity symbol to represent their status as vehicles of the future).

283. *See* Harris, *supra* note 282 (noting that the car companies themselves can issue the pre-requisite training for its test drivers, rather than the federal or state government—"Google requires that its test drivers complete weeks of in-depth lessons and rigorous exams, while Audi's entire program lasts just a couple of hours").

284. *See* Doug Newcomb, *You Won't Need a Driver's License by 2040*, WIRED (Sept. 17, 2012, 1:42 PM), http://www.wired.com/2012/09/ieee-autonomous-2040 (stating that people do not need a license to sit on a train or a bus).

285. *Autonomous Vehicle Express Terms*, ST. CAL. DEP'T MOTOR VEHICLES (Sept. 30, 2016), https://www.dmv.ca.gov/portal/wcm/connect/ed6f78fe-fe38-4100-b5c2-1656f555e841/AVExpress Terms.pdf?MOD=AJPERES (providing that a person must complete a training program conducted by the manufacturer to obtain a certificate that allows the operation of an autonomous vehicle). The training program includes, but is not limited to, demonstrating "how to engage and disengage the autonomous mode, how to override unauthorized or spurious commands received by the autonomous technology in the event of a cyberattack, and the operator's responsibility to monitor the safe operation of the vehicle at all times." *Id.*; *see* Transp. Mgmt., *Autonomous Vehicles: California to Require Licensed Drivers in Driverless Vehicles*, ROADS & BRIDGES (Dec. 17, 2015), http://www.roadsbridges.com/autonomous-vehicles-california-require-licensed-drivers-driverless-vehicles (explaining that the DMV's actions could lead to better research on autonomous vehicles regarding human behavior and interaction).

286. *See supra* Part IV.A.

287. *See supra* Part IV.A.

prevalent and diverse such that it would be more effective to create and amend patchworks of federal law, rather than state law.[288] Nevertheless, it is crucial to impose requirements on operators and owners of autonomous vehicles since it would grant law enforcement officials a more effective means of prosecuting criminals—the main requirement being that vehicle operators need an AVL, which would automatically subject them to greater transparency regarding their vehicle data under new federal law.[289] These requirements would also ease the development of impending autonomous vehicle regulations, as new technology generally has a great deal of unanticipated consequences on society.[290]

*Christopher Wing**

288. *See supra* Parts II–III.

289. *See supra* Part IV.E.

290. *See supra* Part IV.

* J.D. Candidate, 2017, Maurice A. Deane School of Law at Hofstra University; M.S. Candidate in Physics, 2017, City College of New York; B.S. in Physics, 2013, Brooklyn College. This Note is dedicated to the memory of Natasha A. Lewis, my dear friend who passed away around the time I began writing this piece. You were strong, kind, and beautiful, and the best darn wingman, sidekick, and geologist I have ever known. Thank you for giving me the strength to always strive for something greater and to never give up on my dreams no matter the odds and no matter how hopeless things may seem. Also, thank you to my parents, Gary and Ling Wing, and my sister, Amanda Wing, for your unconditional love, inspiration, and never-ending support. Thank you to my faculty Note advisor, Professor Kevin McElroy, and to my advising Notes Editor, Amanda Regan, for your wisdom and having to put up with my babbling about cars for a whole year. Lastly, I would like to thank the *Hofstra Law Review* Volume 45 Managing Editors, Joseph De Santis, Susan Loeb, and Michelle Malone, as well as the entire Board of Editors, Associate Editors, and Staff without whom this and many other publications would not be possible.

> *If something is important enough you should try, even if [you believe that] the probable outcome is failure[,] . . . [f]ailure is an option here. If things are not failing, you are not innovating enough.*
>
> – Elon Musk