Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars

Chasel Lee *

TABLE OF CONTENTS

* J.D. candidate, The George Washington University Law School, 2017. Senior Managing Editor, *Federal Communications Law Journal*, 2016–17. B.A., University of California, Berkeley.

I. INTRODUCTION

On October 9, 2010, the *New York Times* revealed that Google had been secretly testing driverless cars for almost a year.[1] This project, consisting mainly of modified Toyota Priuses, had already logged over 140,000 miles.[2] Resembling the company's Street View cars, seven prototypes had been twisting through San Francisco's steep and curvy Lombard Street, traversing the streets of the company's suburban hometown of Mountain View, and speeding down scenic Highway 1 to Los Angeles over 400 miles away.[3] The cars detected and announced upcoming crosswalks, could be driven cautiously or aggressively at the occupant's discretion, and had several mechanisms for the occupant to take manual control.[4]

While the driverless car concept has been tested since the 1920s with varying levels of success, news of Google's foray into autonomous vehicles electrified the world.[5] With the concept reintroduced into the popular consciousness, public and industry interest in driverless cars has grown immensely and allowed autonomous vehicles to gain mainstream traction. Since the *New York Times* article was published, Google has added more features, the vehicles have ventured farther, and the prototypes have been tested by various audiences, including the blind.[6] Hoping to grab a head start in this nascent market and garner publicity, traditional car companies such as Toyota and Audi have joined the fray by developing driverless car prototypes and incorporating automated parking functions into existing cars.[7] Tesla has also contributed its own innovations, such as transforming traditional human-controlled vehicles to autonomous cars simply via software updates to the car's onboard computers.[8] The company has already begun testing full-fledged self-driving cars in California and elsewhere since late 2016.[9]

---

1. John Markoff, *Google Cars Drive Themselves, in Traffic*, N.Y. TIMES (Oct. 9, 2010), http://www.nytimes.com/2010/10/10/science/10google.html [https://perma.cc/U8EQ-DYZU].

2. *See id*.

3. *See id*.

4. *See id*.

5. *See* Emma Poole, *Navigating Driverless Cars*, WIPO MAG. (Dec. 2014), http://www.wipo.int/wipo_magazine/en/2014/06/article_0003.html [https://perma.cc/ZWS6-YRTD].

6. *See* Angela Moscaritolo, *Google's Self-Driving Car Takes Blind Man for a Ride*, PC MAG. (Mar. 29, 2012, 1:12 PM EST), http://www.pcmag.com/article2/0,2817,2402340,00.asp [https://perma.cc/TT92-4H3V].

7. Ian Scherr & Mike Ramsey, *Toyota, Audi Move Closer to Driverless Cars*, WALL ST. J. (Jan. 3, 2013, 10:17 PM ET), http://www.wsj.com/articles/SB10001424127887323374504578220081249592640 [https://perma.cc/B29M-46S6].

8. Ken Yeung, *Tesla Launches Its Long-Awaited Driverless Car Update in Beta*, VENTUREBEAT (Oct. 14, 2015, 2:21 PM), http://venturebeat.com/2015/10/14/tesla-launches-its-long-awaited-driverless-car-update-in-beta/ [https://perma.cc/B8SH-6GPU].

9. Dana Hull, *Tesla Is Testing Self-Driving Cars on California Roads*, WIRED (Feb. 1, 2017, 1:21 PM EST), https://www.bloomberg.com/news/articles/2017-02-01/tesla-is-testing-self-driving-cars-on-california-roads [https://perma.cc/N8XE-P8PN]; Fred Lambert, *Tesla*

Despite the optimistic outlook on the technological development of driverless cars, difficult legal and policy issues lurk in the background and emerge at every turn. For example, the 2010 *New York Times* article noted potential liability concerns between vehicle manufacturers and human passengers in cases of car crashes.[10] Other writers have discussed outdated state laws presuming human control of the car.[11] Additional concerns have turned on safety problems, whether arising from current technological limitations (such as bike lanes or left turns in oncoming traffic), the inability of vehicles to deal with certain weather conditions, and unpredictable driver behavior.[12] Transparency and reporting of malfunctions and other incidents to authorities, especially when crashes occur, have become salient issues.[13] Also, ethics has become a major flashpoint in the driverless car debate, as software programmers must now grapple with situations such as the Trolley Problem,[14] which would now be decided by artificial intelligence and engineer-preset choices rather than human proclivities or simple error.[15]

Driverless cars also raise questions involving cybersecurity and privacy.[16] By their nature, driverless cars must collect and process a substantial amount of data to determine their surroundings, find the best route to a destination, and interact with other vehicles (autonomous or otherwise).[17]

Hints at Testing Self-Driving Car Prototypes Outside of California, ELECTREK (Feb. 6, 2017, 5:27 AM ET), https://electrek.co/2017/02/06/tesla-testing-self-driving-car-prototypes-outside-california/ [https://perma.cc/AY8F-XC9W].

10. Markoff, *supra* note 1.

11. *Id.*; *see* Nathan A. Greenblatt, *Self-Driving Cars Will Be Ready Before Our Laws Are*, IEEE Spectrum (Jan. 19, 2016, 4:00 PM GMT), http://spectrum.ieee.org/transportation/advanced-cars/selfdriving-cars-will-be-ready-before-our-laws-are [https://perma.cc/R9ZR-5NAB].

12. *See, e.g.*, Sam Levin, *Uber Admits to Self-Driving Car "Problem" in Bike Lanes as Safety Concerns Mount*, GUARDIAN (Dec. 19, 2016, 17:42 EST), https://www.theguardian.com/technology/2016/dec/19/uber-self-driving-cars-bike-lanes-safety-san-francisco [https://perma.cc/XJ5A-T33E]; Alex Davies, *Google's Self-Driving Car Causes Its First Crash*, WIRED (Feb. 29, 2016, 2:04 PM), https://www.wired.com/2016/02/googles-self-driving-car-may-caused-first-crash [https://perma.cc/7PJC-MZVV]; Lauren Keating, *The Driverless Car Debate: How Safe Are Autonomous Vehicles?*, TECH TIMES (July 28, 2015, 9:00 AM EDT), http://www.techtimes.com/articles/67253/20150728/driverless-cars-safe.htm [https://perma.cc/73RF-LHEG].

13. *See* Justin Pritchard, *Google Acknowledges 11 Accidents with Its Self-Driving Cars*, ASSOCIATED PRESS (May 12, 2015, 12:46 AM EDT), http://bigstory.ap.org/article/297ef1bfb75847de95d856fb08dc0687/ap-exclusive-self-driving-cars-getting-dinged-california [https://perma.cc/A2C8-SQPK].

14. The Trolley Problem, a thought experiment devised by philosopher Philippa Foot, envisions a runaway trolley, helmed by the reader, barreling towards a fork in the tracks. If nothing is done, the trolley will run over five people working on the tracks and kill them, while if the trolley is turned onto a side track, it will run over one person working on it and kill him. The ethical dilemma rests on what action the reader should take. *See* Judith Jarvis Thomson, *The Trolley Problem*, 94 YALE L.J. 1395, 1395 (1985).

15. Ben Ellman, *Your Driverless Car Could Be Programmed to Kill You*, N.Y. MAG. (Oct. 28, 2015, 9:40 AM), http://nymag.com/scienceofus/2015/10/driverless-cars-might-be-programmed-to-kill-you.html [https://perma.cc/8Z8Q-GL4J].

16. *See* Keating, *supra* note 12.

17. *See* Ucilia Wang, *Driverless Cars Are Data Guzzlers*, WALL ST. J. (Mar. 23, 2014, 4:36 PM ET),

Among other conceivable privacy implications, this data collection raises numerous issues regarding the location of the vehicle, actions by passengers within the car, and common destinations.[18] Cybersecurity concerns include how and what data is stored onboard and for how long, how and what data is shared with others, and what defensive mechanisms are used to protect this data from hackers.[19] Does the consumer have control over what data is collected or shared? More importantly, can governments access this data, and if so, how?[20]

This Note explores the legal aspects and ramifications of cybersecurity and privacy issues regarding driverless cars. Section II of this Note proceeds with a brief discussion of the history of driverless cars, focusing especially on the developments made in the past ten years, before exploring the history of cybersecurity and privacy law in the United States and its relation, or lack thereof, to driverless cars. Section II will also examine legislative and regulatory efforts aimed at driverless cars, such as those recently launched by the National Highway Traffic Safety Administration (NHTSA).[21] This Note proposes in Section III that privacy and cybersecurity concerns should be analyzed, addressed, and regulated under a federal framework, while allowing the states and private industry leeway to engage in experimentation and innovation regarding regulation and promulgation of standards. Lastly, Section IV proposes that regulators collaborate with major players in the industry to craft new rules under their existing authority and set uniform consumer protection baselines for the private sector to follow. This legal regime would apply to both government surveillance and actions by private parties, such as manufacturers and third-party agents.

II. BACKGROUND

Despite the breakneck speed of driverless cars' technological advances, legislation and regulation are still plodding along at a glacial pace. Legislators and regulators, seemingly blindsided by the surge of recent public interest in driverless cars, are still slowly figuring out the path forward to foster

---

http://www.wsj.com/articles/SB10001424052702304815004579417441475998338 [https://perma.cc/3LA6-P7CG].

18. *See, e.g.*, Stuart Dredge, *We Should Question and Challenge Google, but Not as Haters*, GUARDIAN (May 14, 2014, 7:20 AM EDT), http://www.theguardian.com/technology/2014/may/14/driverless-cars-google-data-privacy [https://perma.cc/P7NK-N923].

19. *See, e.g.*, *id.*; Jason Koebler, *Driverless Cars Are Giant Data Collection Devices, Say Privacy Experts*, VICE (Mar. 14, 2014, 4:30 PM EST), https://motherboard.vice.com/en_us/article/driverless-cars-are-giant-data-collection-devices-say-privacy-experts [https://perma.cc/85SP-TZB3].

20. *See* Timothy B. Lee, *Self-Driving Cars Are a Privacy Nightmare. And It's Totally Worth It*, WASH. POST (May 21, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/05/21/self-driving-cars-are-a-privacy-nightmare-and-its-totally-worth-it/ [https://perma.cc/EH2Z-YTL2].

21. *See* Heather Caygle, *White House Pushes to Make Driverless Cars a Reality*, POLITICO (Jan. 14, 2016, 3:22 PM EST), http://www.politico.com/story/2016/01/white-house-driverless-cars-reality-217778 [https://perma.cc/Q6YY-5C3K].

innovation and incorporate consumer protections.[22] However, the current situation stems from the trajectory of development of driverless cars and the ossified nature of American cybersecurity and privacy laws.

A. Today's Driverless Car Revolution Has Made Great Advances, but State Governments Have Only Begun to Touch the Issue.

For the most part, research into driverless cars was an under-the-radar affair in the 20th century. The history of driverless cars begins in the 1920s, when daring entrepreneurs built radio-controlled prototypes, the precursor to today's radio-controlled toy cars.[23] In 1958, General Motors (GM) tested a customized Chevrolet using pick-up coils to sense inductive signals from wires embedded in a test road to propel and turn itself.[24] The 1960s saw the Stanford Cart, a rudimentary buggy with a video camera and a remote control, while the 1970s ended with the first truly autonomous car, a Japanese model equipped with two cameras and analog computers and guided by an elevated rail.[25] The 1980s witnessed German aerospace engineer Ernst Dickmanns and his team build various models with cameras and microprocessors that could navigate in standard European traffic, and the 1990s saw roboticists at Carnegie Mellon University drive NavLab 5, a Pontiac minivan with cameras and an onboard computer, almost 3000 miles from Pittsburgh to Los Angeles in a trip called "No Hands Across America."[26] Prototypes slowly incorporated numerous advances such as installing cameras to use visual-based cues rather than wire loops locating induced signals, using increasingly sophisticated onboard computers, and integrating GPS for navigation.[27]

The driverless car revolution in the United States had a major breakthrough in March 2004, when the U.S. Department of Defense, through the Defense Advanced Research Projects Agency (DARPA), held a Grand Challenge for fully autonomous cars in the California desert.[28] While no

22. *See, e.g.*, Melanie Zanona, *House Gets Serious About Driverless Cars*, HILL (Feb. 14, 2017, 12:32 PM EST), http://thehill.com/policy/transportation/319450-house-lawmakers-weigh-driverless-car-laws [https://perma.cc/5GBB-F5GE]; Pui-Wing Tam, *Daily Report: Regulators Catching Up with Driverless Cars*, N.Y. TIMES: BITS (Sept. 20, 2016), https://www.nytimes.com/2016/09/21/technology/daily-report-regulators-catching-up-with-driverless-cars.html [https://perma.cc/N2WH-V7GD].

23. *See* Poole, *supra* note 5.

24. Tom Vanderbilt, *Autonomous Cars Through the Ages*, WIRED (Feb. 6. 2012, 6:30 AM), http://www.wired.com/2012/02/autonomous-vehicle-history/ [https://perma.cc/NC2T-X4CG].

25. *Id.*

26. *Id.*; *see* NO HANDS ACROSS AMERICA, https://www.cs.cmu.edu/afs/cs/usr/tjochem/www/nhaa/nhaa_home_page.html [https://perma.cc/TE2X-HKFZ] (last visited Mar. 29, 2016).

27. *See* Vanderbilt, *supra* note 24.

28. *See* Denise Chow, *DARPA and Drone Cars: How the US Military Spawned Self-Driving Car Revolution*, LIVE SCIENCE (Mar. 21, 2014, 2:27 PM ET), http://www.livescience.com/44272-darpa-self-driving-car-revolution.html [https://perma.cc/ZL8X-NQCW].

vehicles in that year's challenge succeeded in the mission,[29] it created a budding community interested in the concept of self-driving cars and revealed the staggering amount of work needed to bring the idea to fruition.[30] This coming-together of disparate, formerly scattered groups of inventors, programmers, designers, and innovators saw its first taste of success in 2005, when DARPA held its second Grand Challenge.[31] That year, five vehicles successfully completed the event, with one team winning a $2,000,000 prize.[32]

The Grand Challenge laid the groundwork for the current rush of developments. Self-driving vehicles began to climb mountains and navigate urban-like environments.[33] They began to cross countries and continents, even (almost) getting ticketed by traffic police.[34] In 2011, Nevada became the first state to pass laws allowing autonomous vehicles to drive on public roads.[35] Other states, including California and Michigan, have since followed Nevada in passing or implementing laws and regulations permitting the same.[36]

B. The Rapid Advance of Driverless Car Technology Has Created and Magnified Problems Regarding Cybersecurity and Privacy.

As driverless cars gain prevalence in our cultural conversation, so too do a myriad of concerns and legal issues.[37] Addressing these concerns will have immense impact on consumer confidence in this emerging technology.[38] Some of the most important concerns involve cybersecurity and privacy measures surrounding driverless cars.[39]

---

29. To win the Grand Challenge, a vehicle had to navigate a 142-mile course from Barstow, California to Primm, Nevada in 10 hours. The most successful vehicle managed to travel only 7.5 miles. *See id.*

30. *See id.*

31. *See id.*

32. *See id.*

33. *See* Vanderbilt, *supra* note 24.

34. The errant driverless car evaded the ticket due to the police officer "not knowing in what name to issue the ticket." *Id.*

35. Alex Knapp, *Nevada Passes Law Authorizing Driverless Vehicles*, FORBES (June 22, 2011, 5:29 PM), https://www.forbes.com/sites/alexknapp/2011/06/22/nevada-passes-law-authorizing-driverless-cars/ [https://perma.cc/7V24-UTS7]; *see also* NEV. REV. STAT. § 482A.010-200 (2016).

36. *Autonomous | Self-Driving Vehicles Legislation*, NAT'L CONF. ST. LEGISLATURES (Nov. 11, 2016), http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx [https://perma.cc/Z2MB-48TU]; *see, e.g.*, CAL. VEH. CODE § 38750 (West 2016); MICH. COMP. LAWS § 257.663–66 (2016).

37. *See, e.g.*, Keith Kirkpatrick, *The Moral Challenges of Driverless Cars*, 58 COMM. ACM 19 (2015); Keating, *supra* note 12; Markoff, *supra* note 1.

38. *See* Ashiq JA, *Security Nightmare of Driverless Cars*, TRIPWIRE (Oct. 25, 2015), http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/security-nightmare-of-driverless-cars/ [https://perma.cc/W67G-8EXC].

39. *See* Ellen S. Pyle, *The Connected Car and the Race to Keep Consumers in the Driver's Seat on Data Privacy*, BLOOMBERG BNA (Feb. 2, 2016), http://www.bna.com/connected-car-race-n57982066853/ [https://perma.cc/QQ5F-SVVY].

The adoption of increasingly sophisticated technology in cars has accentuated cybersecurity as a major concern. For example, one concern involves tricking a car's sensors with low-powered lasers, which can disorient the vehicle's computer systems.[40] Hackers can point the laser at a sensor, which tricks the car into taking needless evasive action or simply paralyzing itself to avoid phantom obstacles.[41]

Even before the advent of driverless cars, cybersecurity was a pressing issue impacting human-driven vehicles. Hackers have demonstrated an ability to wirelessly grab control of the vehicle and remotely control it via the car's software and connectivity systems.[42] Those with ill intent can find access paths through Bluetooth, remote keyless entry systems, cellular signals, or any wireless connection a car can make with the outside world.[43] Malware attacking critical car components such as brakes and transmission can be unwittingly introduced into a car's system at auto dealerships by mechanics.[44] With the continued addition of various digital systems and amenities to cars, especially driverless cars, such methods of unauthorized entry will only increase.

While hacking into a car is still difficult, requiring some level of physical access or long, arduous study of a car's programs,[45] the voluminous data gathered and used by these cars makes the effort valuable to hackers.[46] This data can include many types of information stored by the vehicle or

---

40. *See* Ashiq JA, *supra* note 38.

41. *See* Samuel Gibbs, *Hackers Can Trick Self-Driving Cars into Taking Evasive Action*, GUARDIAN (Sept. 7, 2015, 6:28 AM EDT), http://www.theguardian.com/technology/2015/sep/07/hackers-trick-self-driving-cars-lidar-sensor [https://perma.cc/VXK7-PDLS].

42. *See* Angelo Young, *Car Hacking: Security Experts Caution Automakers on Greater Need for Cybersecurity and Anti-Hacking Measures*, INT'L BUS. TIMES (July 28, 2015, 8:26 AM), http://www.ibtimes.com/car-hacking-security-experts-caution-automakers-greater-need-cybersecurity-anti-2026472 [https://perma.cc/TVL4-XCLF] (hacking into a regular Jeep and subsequent recall); *see also* Ashiq JA, *supra* note 38 (other examples).

43. *See* 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/ [https://perma.cc/EH6E-K45J] (listing various vulnerable vectors permitting unauthorized entry into a car's systems).

44. *See* Andy Greenberg, *Car Hack Technique Uses Dealerships to Spread Malware*, WIRED (Oct. 1, 2015, 7:00 AM), http://www.wired.com/2015/10/car-hacking-tool-turns-repair-shops-malware-brothels/ [https://perma.cc/CSZ4-Z8TX].

45. *See* David Pogue, *Why Car Hacking Is Nearly Impossible*, SCI. AM. (Oct. 23, 2015), http://www.scientificamerican.com/article/why-car-hacking-is-nearly-impossible/ [https://perma.cc/EVU4-4H86]. *But see* Jonathan Vanian, *Security Experts Say Hacking Cars Is Easy*, FORTUNE (Jan. 26, 2016, 6:47 PM EST), http://fortune.com/2016/01/26/security-experts-hack-cars/ [https://perma.cc/LT2P-NJG4] ("With cars containing multiple computers coupled together through a maze of networks, it's also possible to break into the car's command center without having to physically plug something into the port. Hackers just have to find a hole somewhere within one of the networks to sneak in.").

46. *See* INST. OF ENG'G & TECH., AUTOMOTIVE CYBER SECURITY: AN IET/KTN THOUGHT LEADERSHIP REVIEW OF RISK PERSPECTIVES FOR CONNECTED VEHICLES 12 (2014), http://www.theiet.org/sectors/transport/documents/automotive-cs.cfm [https://perma.cc/DLK2-B2DY] (citing foreseeable motives of hacking into connected vehicles, with data theft ranking first). Immobilization of the vehicle and mischief ranked sixth and seventh among potential motivations, respectively.

utilized by onboard applications.[47] As driverless cars grow in the automobile market and the "Internet of Things" joins the mainstream,[48] these vehicles will only store and transmit more data, including lifestyle information, credit card usage, and medical records, thus making them attractive targets for hackers.[49]

To identify and understand these cybersecurity threats, the NHTSA has crafted a model looking at factors such as entry points into a vehicle's systems, access methods used to penetrate the systems' defenses, types of attacks on a vehicle's systems, and potential consequences of these attacks.[50] For example, if a type of car receives numerous cases of outside interference with use of its brakes, a manufacturer or regulator can use the above factors to establish patterns and respond accordingly.[51] Using this model, data on the ease, prevalence, and potential for various cybersecurity threats can be analyzed to inform standardization and regulatory decisions by governments and private industry.[52]

Like cybersecurity, privacy is becoming an increasingly prominent concern as driverless cars take to the road.[53] As previously discussed, a driverless car collects an immense amount of data in order to ascertain its surroundings, propel itself, move around on the roads, and cater to its passengers' needs.[54] This data can be sufficiently comprehensive that it may enable those who get their hands on the information to form a detailed profile of the car's user.[55] Even if the collection of such information is legal, it may cause users to believe the car is "spying" on them, which is usually not good optics from a public relations perspective.[56]

Moreover, much of the data collected can be connected to a specific user. Even the most innocuous and necessary data for the proper functioning of a driverless car, such as the information collected from the car's sensors or

---

47. *See id.* at 12 (listing examples such as banking records, passwords, insurance information, and vehicle location information).

48. The Internet of Things is the "the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other)." For example, cars can access online calendars or control the thermostat at home. Jacob Morgan, *A Simple Explanation of "The Internet of Things,"* FORBES (May 13, 2014), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#6def3b916828 [https://perma.cc/V66S-7AKB].

49. *See* INST. OF ENG'G & TECH., *supra* note 46, at 12.

50. *See* CHARLIE MCCARTHY ET AL., NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., CHARACTERIZATION OF POTENTIAL SECURITY THREATS IN MODERN AUTOMOBILES: A COMPOSITE MODELING APPROACH 9 (2014), https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf [https://perma.cc/98D8-97VV].

51. *Cf. id.* at 16–18 (filling out a detailed threat matrix using the brake disconnect example).

52. *See id.* at iii.

53. *See* Adrienne LaFrance, *How Self-Driving Cars Will Threaten Privacy*, ATLANTIC (Mar. 21, 2016), http://www.theatlantic.com/technology/archive/2016/03/self-driving-cars-and-the-looming-privacy-apocalypse/474600/ [https://perma.cc/98TW-KFXX].

54. *See* INST. OF ENG'G & TECH., *supra* note 46, at 7–8.

55. *See* Samantha Sayers & Sabba Mahmood, *Connected Cars: An Approach to Dealing with the Privacy Risks*, PRIVACY & DATA PROT. J., Sept. 2015, at 3 (2015).

56. *See id.*

from communicating with other vehicles in order to avoid collisions, can be used to identify people.[57] Data-mining techniques can take any data stripped of unique identifying markers to identify a car and, in turn, its users.[58] Thus, while vehicular data collection may enable a range of attractive consumer features, it is only steps away from surreptitious surveillance and untoward influence of consumer behavior, especially by companies looking to profit from such valuable information.[59]

C. Despite Cybersecurity and Privacy Concerns Surrounding Driverless Cars, There Is Currently a Dearth of Applicable Federal or State Law to Address These Concerns.

Despite some movements by states to pave the road for the anticipated driverless car revolution and protect consumers from wayward excesses, the newly passed driverless car legislation in Nevada and other states merely permit the *testing or use* of autonomous vehicles on the road. Complementary laws and regulations needed to address safety, liability, cybersecurity, and privacy concerns are either nonexistent[60] or stuck in the rulemaking process.[61] Various commentators have described recent guidelines from the NHTSA as unhelpfully vague.[62] The lack of clarity in the law addressing these complex

57. *See* 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, 120–21 (2015).

58. *Id.*

59. LaFrance, *supra* note 53.

60. Aaron M. Kessler, *Hands-Free Cars Take Wheel, and Law Isn't Stopping Them*, N.Y. TIMES (May 2, 2015), http://www.nytimes.com/2015/05/03/business/hands-free-cars-take-wheel-and-law-isnt-stopping-them.html [https://perma.cc/M7SK-3TXM].

61. *See* Alex Davies, *California's New Self-Driving Car Rules Are Great for Texas*, WIRED (Dec. 17, 2015, 11:00 AM), https://www.wired.com/2015/12/californias-new-self-driving-car-rules-are-great-for-texas/ [https://perma.cc/DX9X-EFHN] ("The DMV will host public forums to discuss the regulations, which won't be finalized before later next year."); Samantha Masunaga, *California's Proposed DMV Rules for Driverless Cars Could Change in the Wake of Federal Guidelines*, L.A. TIMES (Sept. 20, 2016, 4:40 PM), http://www.latimes.com/business/la-fi-hy-dmv-driverless-rules-20160920-snap-story.html [https://perma.cc/DU7G-FHP7]. As of January 2017, the California rules are still in draft form. Russ Mitchell, *California Regulations for Driverless Cars Stall as Other States Speed Ahead*, L.A. TIMES (Jan. 26, 2017, 12:10 PM), http://www.latimes.com/business/autos/la-fi-hy-driverless-regulations-california-20170126-story.html [https://perma.cc/T4V7-EE8U].

62. *See, e.g.*, Ian Adams, *The New Federal Safety Guidelines for Self-Driving Cars Are Too Vague . . . And States Are Already Making Them Mandatory*, TECHDIRT (Oct. 14, 2016, 1:11 PM), https://www.techdirt.com/articles/20161006/00202435725/new-federal-safety-guidelines-self-driving-cars-are-too-vague-states-are-already-making-them-mandatory.shtml [https://perma.cc/2WYE-BAQP]; Russ Mitchell and Samantha Masunaga, *Government Paves Way for Driverless Cars to Hit the Roads*, L.A. TIMES (Sept. 20, 2016, 6:45 PM), http://www.latimes.com/business/la-fi-hy-driverless-car-guidelines-20160920-snap-story.html [https://perma.cc/9G76-9CYQ] ("Joan Claybrook, a consumer advocate who ran NHTSA in the Carter administration, called the guidelines 'a definite improvement' but says they're too vague.").

issues must be urgently addressed, as these concerns have only become more important as driverless cars become an impending reality.[63]

Beyond murky or nonexistent laws, certain concepts that are salient to driverless car regulation lack coherent legal definitions. For example, the term "cybersecurity" can mean slightly different things depending on the agency or party using the term.[64] Eric A. Fischer, Senior Specialist in Science and Technology for the Congressional Research Service, defined the term to mean "measures intended to protect information systems—including technology (such as devices, networks, and software), information, and associated personnel—from various forms of attack."[65] CTIA, the industry trade group representing the wireless industry, shares this methods-based orientation, focusing on the methods by which information or systems are protected from attack.[66] The Committee on National Security Systems (CNSS), an intergovernmental agency that sets standards for systems critical to national security,[67] uses a subtly different definition, with "cybersecurity" meaning "the ability to protect or defend the use of cyberspace from cyber attacks."[68] Still other applications treat "cybersecurity" as a synonym for "information security," a statutory term meaning "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction."[69]

Privacy is an even more nebulous legal concept than cybersecurity.[70] Samuel D. Warren and Louis Brandeis famously saw privacy as "the right to

63. *See generally* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1172 (2012) (listing various privacy concerns).

64. *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 1 n.1 (2013), https://www.fas.org/sgp/crs/natsec/R42114.pdf [https://perma.cc/KN2V-3KHT] (noting that cybersecurity is "a broad and arguably somewhat fuzzy concept for which there is no consensus definition").

65. *Id.*

66. *See* CTIA, *Today's Mobile Cybersecurity: Blueprint for the Future* 4 (2013), http://www.ctia.org/docs/default-source/default-document-library/cybersecurity_white_paper.pdf [https://perma.cc/M8U9-Y54F] (defining cybersecurity as "'how' to protect" information).

67. *See* COMM. ON NAT'L SEC. SYS., https://www.cnss.gov/cnss/ [https://perma.cc/4W3Z-G29Z] (last visited Apr. 5, 2016) ("CNSS[] sets national-level Information Assurance policies, directives, instructions, operational procedures, guidance and advisories . . . for the security of National Security Systems (NSS).").

68. *See* COMM. ON NAT'L SEC. SYS., NATIONAL INFORMATION ASSURANCE (IA) GLOSSARY 22 (2010), http://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf [https://perma.cc/U4FL-HSPJ]. "Cyberspace" is defined by the CNSS as "[a] global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." *Id.*

69. FISCHER, *supra* note 64, at 1 n.1 (citing 44 U.S.C. § 3532(b)(1) (2012)).

70. *See* William M. Beaney, *The Right to Privacy and American Law*, 31 L. & CONTEMP. PROBS. 253, 255 (1966) ("[E]ven the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right.").

be let alone,"[71] an approach that Brandeis later grounded in constitutional law and brought with him to the Supreme Court.[72] William Prosser, former dean of the University of California, Berkeley School of Law, and a "giant of tort law,"[73] distilled privacy into four distinct torts,[74] which are recognized in the Restatement of Torts.[75] Daniel Solove, a professor at the George Washington University Law School and a leading expert in privacy law,[76] refers to privacy as "the practices we want to protect and to the protections against disruptions to these practices,"[77] which are drawn from "a common pool of similar elements" such as the "right to be let alone," personhood, and intimacy, among others.[78] On a less philosophical front, CTIA defines privacy as more of a determination of what information should be free from unauthorized intrusion or use (i.e., the "what" to protect).[79] Despite the vagueness of these terms legally and conceptually, it is important to note that privacy and cybersecurity are intertwined in the digital realm: "privacy cannot exist without cybersecurity," and cybersecurity is a moot point without privacy.[80]

Despite the cybersecurity threats facing today's and tomorrow's cars, there is still a dearth of laws and regulations addressing these issues, especially at the federal level. A major reason is the inability of the law to advance as rapidly as the technology, whether due to political uncertainty or inertia, and the inability to address concerns in a "regulatory void."[81] There is no overarching federal legal framework in place for cybersecurity issues, while a patchwork of laws addresses scattered aspects of this field.[82] In fact, until the enactment of several cybersecurity-related bills in late 2014, which shuffled around administrative agencies and codified existing actions and initiatives,[83] there had been no major federal cybersecurity legislation since

---

71. *See* Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("[N]ow the right to life has come to mean the right to enjoy life, – the right to be let alone . . . .").

72. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("The protection guaranteed by the Amendments is much broader in scope. . . . They conferred, as against the Government, the right to be let alone – the most comprehensive of rights, and the right most valued by civilized men.").

73. Christopher J. Robinette, *The Prosser Notebook: Classroom as Biography and Intellectual History*, 2010 U. ILL. L. REV. 577, 579, 581.

74. The four torts are (1) intrusion upon seclusion, (2) public disclosure of embarrassing private facts, (3) false light, and (4) appropriation of name or likeness. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

75. RESTATEMENT (SECOND) OF TORTS §§ 652A(2)(a)–(e) (AM. LAW INST. 1977).

76. *See Daniel Justin Solove*, GW LAW, https://www.law.gwu.edu/daniel-justin-solove [https://perma.cc/68WJ-4TJT] (last visited Apr. 5, 2016).

77. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1093 (2002).

78. *Id* at 1091, 1099.

79. *See* CTIA, *supra* note 66, at 4.

80. *See id*.

81. *See* Kessler, *supra* note 60 ("Part of why federal and state officials have struggled to define autonomous rules is that the issue cuts across traditional legal turf.").

82. *See* FISCHER, *supra* note 64, at 2.

83. *See In a Surprising Move, Congress Passes Four Cybersecurity Bills*, HUNTON & WILLIAMS: PRIVACY & INFO. SECURITY L. BLOG (Dec. 12, 2014), https://www.huntonprivacyblog.com/2014/12/12/surprising-move-congress-passes-four-cybersecurity-bills/ [https://perma.cc/69Y5-VU6S].

2002.[84] Recent guidelines issued by the NHTSA in September 2016 say little about cybersecurity other than to encourage documentation of risks and developments and encouragement of industry sharing.[85] In 2015, Senators Ed Markey and Richard Blumenthal introduced the Security and Privacy in Your Car Act (SPY Car Act) to address cybersecurity issues in driverless cars and to kickstart a rulemaking process at the Federal Trade Commission (FTC),[86] but the bill languished in committee.[87] In 2017, Representatives Joe Wilson and Ted Lieu introduced a more restrained Security and Privacy in Your Car Study Act (SPY Car Study Act),[88] but its prospects of passage are similarly uncertain.

In the face of federal inaction and growing public concern, states have taken some leadership and made more efforts to address cybersecurity along with many other issues surrounding the integration of driverless cars into society.[89] For example, many jurisdictions, such as California and the District of Columbia, have data security breach notification laws in place for other purposes that could be extended to driverless cars.[90] Several states also have laws requiring businesses to have minimum data security standards to prevent

---

84. *See* H.R. REP. NO. 113-33, at 37 (2013). The Senate counterpart of the House bill, the Cybersecurity Enhancement Act of 2014, S. 1353, was signed into law on December 18, 2014. Press Release, White House Office of the Press Secretary, Statement by the Press Secretary – Bills Signed into Law (Dec. 18, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/12/18/statement-press-secretary-bills-signed-law [https://perma.cc/WDK4-K2NQ].

85. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., FEDERAL AUTOMATED VEHICLES POLICY 21 (2016).

86. Security and Privacy in Your Car Act of 2015 (SPY Car Act of 2015), S. 1806, 114th Cong. (2015); *see also* Thomas Fox-Brewster, *SPY Car Act Hopes to Save American Cars from Digital Disaster*, FORBES (July 21, 2015, 1:07 PM), http://www.forbes.com/sites/thomasbrewster/2015/07/21/senators-launch-spy-car-act/ [https://perma.cc/GL4B-952F]. Provisions of the bill include mandating that all motor vehicles comply with software system isolation and data security standards within two years of FTC-promulgated regulations, requiring that a "cyber dashboard" label detailing the car's cybersecurity and privacy measures be affixed to each vehicle, and compelling disclosure of how data is collected and retained by the vehicle. S. 1806 §§ 2(a)(2), 3(a), 4(a).

87. *See All Bill Information (Except Text) for S. 1806 – SPY Car Act of 2015*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/senate-bill/1806/all-info [https://perma.cc/5WDE-4LKS] (last visited Feb. 17, 2017).

88. Security and Privacy in Your Car Study Act of 2017 (SPY Car Study Act of 2017), H.R. 701, 115th Cong. (2017). In contrast with the previous bill, this bill merely requires the NHTSA to conduct a study with other government agencies and the private sector to develop and recommend cybersecurity standards. *Compare id. with* text accompanying *supra* note 86.

89. *See* Kessler, *supra* note 60; Maggie Clark, *States Take the Wheel on Driverless Cars*, USA TODAY (July 29, 2013, 1:47 PM EDT), http://www.usatoday.com/story/news/nation/2013/07/29/states-driverless-cars/2595613/ [https://perma.cc/X6DD-NCKK].

90. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Feb. 24, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/T9K8-KUFE]; *see, e.g.*, CAL. CIV. CODE § 1798.29(a) (West 2015) (mandating notification "following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."), D.C. CODE § 28-3852(a) (2015) (affording similar protections for District of Columbia residents).

breaches in the first place.[91] However, even these states have offered few or no regulations on cybersecurity issues specifically tailored to driverless cars.

Unlike the lack of cybersecurity laws, there are more privacy laws and protections at the federal and state level,[92] especially those addressing more general issues such as digital and Internet privacy.[93] These laws protect minors' library records and online information from disclosure, and create standards for business privacy policies and Internet service providers (ISPs).[94] Like cybersecurity, however, these laws have yet to be applied in the driverless car context. While there are some laws that address privacy concerns related to "traditional" driver-controlled cars,[95] there are also a multitude of privacy concerns surrounding driverless cars where existing privacy laws may be inadequate for the task. There is also a need to adapt existing (and worthwhile) protections and laws such as the Driver's Privacy Protection Act into the uncharted world of self-driving cars.[96] These additional concerns include ensuring secure interaction with external networks, interactions with other vehicles, and proper storage of gathered information.[97] Underlying these concerns are potential issues related to determining control of the information, protecting driver and passenger anonymity, and ensuring informed consent to gather information from passengers.[98]

Privacy concerns can extend not only to what private parties can do with the information, but also to what governments can do to acquire it or analyze it.[99] While such concerns have long existed—spanning the advent of

91. Corey M. Dennis, *Data Security Laws & the Rising Cybersecurity Debate*, LEXOLOGY (Jan. 28, 2013), http://www.lexology.com/library/detail.aspx?g=cc5c9a56-7a60-46ab-9cf4-f36cada0cafa [https://perma.cc/KL6J-EL2B]; *see, e.g.*, CAL. CIV. CODE § 1798.81 (West 2015) (requiring businesses to "take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business").

92. *See, e.g.*, U.S. CONST. amend. IV; Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (1986).

93. *State Laws Related to Internet Privacy*, NAT'L CONF. ST. LEGISLATURES (Jan. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/78P9-GX3H].

94. *See generally id.* (listing examples).

95. *See, e.g.*, Driver's Privacy Protection Act of 1994, Pub. L. 103-322, Title XXX, 108 Stat. 2099 (forbidding the disclosure of driver license information by state DMVs without the consent of the license holder except under certain circumstances).

96. *See* Glancy, *supra* note 63, at 1192; *see also supra* text accompanying note 95.

97. Glancy, *supra* note 63, at 1179–80.

98. *Id.* at 1191, 1195.

99. *See* Kohler & Colbert-Taylor, *supra* note 57, at 120–32; *see also generally* Glancy, *supra* note 63.

police detention,[100] telephone wiretapping,[101] and car searches[102]—driverless cars have created new opportunities and avenues for law enforcement and other government agencies to engage in mass surveillance or, even more troubling, surreptitious and warrantless tracking.[103] States have made tentative efforts to rein in such acts through new laws and regulations, but they have been few and far between.[104] Some of these efforts have stalled or been stymied due to the driverless car companies themselves.[105]

However, federal and state governments, along with interest groups, have begun to make initial steps to lay the groundwork for some regulation regarding privacy protections for driverless cars.[106] In 2016, the Obama administration aimed to bolster these efforts by including $4 billion in funding for driverless car pilot programs in its fiscal 2017 budget presented to Congress.[107] After soliciting comment from the public and private industry,[108] the NHTSA also issued some guidelines on "automated cars" in September 2016.[109]

---

100. Terry v. Ohio, 392 U.S. 1, 38 (1968) (Douglas, J., dissenting) (quoting Henry v. United States, 361 U.S. 98, 100–02 (1959) ("This immunity of officers [to search without a warrant] cannot fairly be enlarged without jeopardizing the privacy or security of the citizen.").

101. Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting) ("Subtler and more far-reaching means of invading privacy [such as telephone wiretapping] have become available to the government."); *see* Katz v. United States, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth . . . .").

102. United States v. Ross, 456 U.S. 798, 804 (1982) ("In every case [of a car search] a conflict is presented between the individual's constitutionally protected interest in privacy and the public interest in effective law enforcement."); United States v. Ortiz, 422 U.S. 891, 896 (1975) ("A search, even of an automobile, is a substantial invasion of privacy.").

103. Glancy, *supra* note 63, at 1211–12.

104. *See, e.g.*, S.B. 178, 2015-2016 Leg., 1st Sess. (Cal. 2015) (prohibiting law enforcement "from compelling the production of or access to electronic communication information or electronic device information . . . without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant under specified conditions, except for emergency situations . . . .").

105. *See, e.g.*, Koebler, *supra* note 19 (discussing Google's lobbying to strip privacy protections from California's driverless car legislation).

106. *See* Tom Risen, *How Safe Is a Self-Driving Car?*, U.S. NEWS & WORLD REP. (Oct. 8, 2015, 3:54 PM), http://www.usnews.com/news/articles/2015/10/08/nhtsa-volvo-seek-cybersecurity-privacy-for-driverless-cars [https://perma.cc/4PT3-GJSU] (referencing the federal Grow America Act, a transportation funding bill that would criminalize hacking a vehicle).

107. *Id.*

108. Caygle, *supra* note 21.

109. *See generally* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 85. The NHTSA gave guidance on various issues surrounding autonomous vehicles with varying specificity. *Compare id.* at 19–20 (the privacy section with seven detailed aspects that manufactures "should ensure") *with supra* discussion accompanying note 85 (sparse cybersecurity section).

D. Existing Cybersecurity and Privacy Laws Are Ill-Suited to Regulate Driverless Cars.

When there is a cybersecurity or privacy law on the books, it is often outdated and inadequate to shield consumers and systems from new risks.[110] Faced with intractable legislative gridlock and the demands of modernity, some courts have broadened legal definitions in preexisting laws to afford some protection to new technologies in the absence of more relevant legislation. For example, courts have deemed cellphones to be "computers" in order to qualify them for the cybersecurity protections in the Computer Fraud and Abuse Act (CFAA),[111] which criminalizes the use of "computers" to commit acts such as hacking or defrauding resulting in damages exceeding $5000.[112]

With the lack of federal laws covering cybersecurity generally, the FTC has resorted to using Section 5 of the Federal Trade Commission Act ("Section 5") to assert its jurisdiction over some cybersecurity issues.[113] Section 5 prohibits the use of "unfair or deceptive acts or practices in or affecting commerce."[114] According to the FTC and the courts, "unfair or deceptive acts or practices" can include failure to "maintain reasonable and appropriate data security" and/or loss of sensitive personal information as a result.[115] The FTC often relies on the "deceptive" legal term to penalize data security transgressors upon finding that companies have misrepresented or violated their own privacy policies.[116] To its credit, the FTC has made some efforts to examine cybersecurity issues related to connected cars,[117] but has

---

110. *See* Eddie Schwartz, *It's Time to Update Antiquated Cybersecurity Legislation*, WASH. EXAMINER (Feb. 23, 2015), http://www.washingtonexaminer.com/its-time-to-update-antiquated-cybersecurity-legislation/article/2560412 [https://perma.cc/J8HT-8WWZ]; Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. TIMES (Jan. 9, 2011), http://www.nytimes.com/2011/01/10/technology/10privacy.html [https://perma.cc/8AZZ-43X3].

111. *See, e.g.*, United States v. Hill, 783 F.3d 842, 845 (11th Cir. 2015) (per curiam); United States v. Kramer, 631 F.3d 900, 902–03 (8th Cir. 2011).

112. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2), (4) (2012).

113. HANOVER RESEARCH, THE EMERGENCE OF CYBERSECURITY LAW 13–14 (2015), https://sm.asisonline.org/ASIS%20SM%20Documents/The-Emergence-of-Cybersecurity-Law.pdf [https://perma.cc/687T-XCY6].

114. Federal Trade Commission Act § 5, 15 U.S.C. § 45(a)(1) (2012).

115. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 236 (3rd Cir. 2015); *see also Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the S. Comm. on Banking, Hous., & Urban Affairs*, 109th Cong. 14, 15 (2005) (statement of Deborah Platt Majoras, Chairman, Fed. Trade Comm'n) ("In addition to deception, the FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.")

116. *See* HANOVER RESEARCH, *supra* note 113, at 14; *see also Identity Theft*, *supra* note 115, at 14 n.41 (listing examples of deceptive claim actions).

117. *Examining Ways to Improve Vehicle and Roadway Safety: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. 2 (2015) (statement of Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., Bureau of Consumer Prot., Fed. Trade Comm'n) ("[A]t its Internet of Things workshop in November 2013, the Commission specifically examined privacy and security issues relating to the different technologies in connected cars . . . .").

not initiated any enforcement actions related to connected, let alone driverless, vehicles.

In the absence of federal action to plug gaping loopholes in federal law, many states have used computer crime laws on their books to offer some cybersecurity protections.[118] For example, California's computer crime laws ban hacking on statutorily defined "computer networks," replete with prescribed criminal sanctions.[119] Michigan also has computer crime provisions criminalizing hacking to defraud or to "acquire, alter, damage, delete, or destroy property," among other purposes.[120] While California's and Michigan's definitions are sufficiently broad to encompass mobile devices within their reach,[121] little or no commentary exists on whether a driverless car or its components qualify as "computers" under this statute.

As is the case with cybersecurity, privacy laws were enacted in a different era for a different world. For example, the Electronic Communications Privacy Act of 1986 (ECPA) prohibits any act or attempt to "intercept" or "disclose . . . any wire, oral, or electronic communication."[122] The ECPA expanded a preexisting narrow prohibition on certain wiretapping acts on telephone lines to include other modes of electronic communication, including email.[123] However, this law does not apply to any data, such as geolocation; in fact, with the exception of the FTC's nebulous standard of "unfair or deceptive acts or practices," there are very few federal limitations on private sector use of personal data outside of statutory protections for children, credit reporting, and health information.[124]

---

118. *Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES (Dec. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx [https://perma.cc/Q257-ZZZ8]; *see, e.g.*, People v. Childs, 164 Cal. Rptr. 3d 287, 301 (Ct. App. 2013) (applying California's statute to defendant for malicious disruption and denial of access by authorized users into their computer systems); People v. Schlike, No. 253117 (Mich. Ct. App. May 3, 2005) (unpublished decision) (applying Michigan's statute to defendant for maliciously entering company's network remotely and deleting almost everything).

119. CAL. PENAL CODE §§ 502(b)(2), (c), (d) (West 2015) ("'Computer network' means any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities.").

120. *See* MICH. COMP. LAWS §§ 752.794–.795 (2015).

121. *See* Patrick E. Corbett, *Cyberharassment, Sexting and Other High-Tech Offenses Involving Michigan Residents—Are We Victims or Criminals?*, 88 U. DETROIT MERCY L. REV. 237, 250 (2010) (citing MICH. COMP. LAWS § 752.792(3) (2000)) ("Michigan's computer crime laws appear to include broad enough definitions so that a cell phone would be considered a 'computer' for purposes of the law."). California's law includes "mobile devices" in its definition of "computer networks."); CAL. PENAL CODE § 502(b)(2).

122. 18 U.S.C. § 2511(1)(a), (c) (2012).

123. *See generally* Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–2521 (2012); U.S. DEPT. OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE ASSISTANCE, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 [https://perma.cc/9M9F-LSKK] (last visited Jan. 19, 2016).

124. Kohler & Colbert-Taylor, *supra* note 57, at 127–28 (citing the Children's Online Privacy Protection Act, 15 U.S.C. §§ 86501–86506 (2012), Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2012), Health Insurance Portability and Accountability Act of 1996 Title II, 42 U.S.C. §§ 1320d to 1320d-9 (2012), and the Federal Trade Commission Act § 5, 15 U.S.C. § 45(a)(1) (2012)).

The Fourth Amendment of the U.S. Constitution has served as an important linchpin for privacy protections restraining the government. For example, the 2014 Supreme Court case of *Riley v. California* required law enforcement to obtain a warrant to search the information on a cellphone of someone who has been arrested.[125] In 2015, the Supreme Court struck down a municipal ordinance mandating that hotels open their registries for warrantless law enforcement inspection as an unconstitutional search,[126] a potential legal harbinger for any potential requirement to permit government searches in large databases such as those drawn on by mobile devices or driverless cars. However, like statutes, much of this case law restricts warrantless government collection of cell phone data during or after an arrest, rather than private or government collection under different circumstances, leaving those concerned about data collection in other technologies (such as driverless cars) in a legal gray area.[127]

States have attempted to plug some of the legal holes in federal privacy protection legislation.[128] The most comprehensive effort came from California in 2015, when the state passed its own Electronic Communications Privacy Act (ECPA).[129] California's ECPA, which went into effect in 2016, requires law enforcement agencies to obtain a warrant in order to search for a device's location data, content, metadata, and search history.[130] This applies to information held by either the device's owner or by service providers.[131] Some states, such as Minnesota, require warrants only for location data,[132] while other states have few or no protections at all.[133] However, there are currently multistate efforts to pass privacy protection laws,[134] but whether they are broad enough to encompass driverless cars remains to be seen.

125. *See generally* Riley v. California, 134 S. Ct. 2473 (2014).

126. Los Angeles v. Patel, 135 S. Ct. 2443, 2452 (2015).

127. *Riley*, 134 S. Ct. at 2489 n.1 (2014) ("[T]hese cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.").

128. Some states, such as California, have the right to privacy ingrained in their constitutions. *See, e.g.*, CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining . . . privacy.").

129. Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), http://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/ [https://perma.cc/WF2D-UREM]; *see generally* Electronic Communications Privacy Act, CAL. PENAL CODE §§ 1546–1546.4 (West 2015).

130. Zetter, *supra* note 129; *see* CAL. PENAL CODE §§ 1546–1546.1.

131. CAL. PENAL CODE § 1546.1.

132. MINN. STAT. § 626A.28 subd. 3(d) (2015).

133. *See* Peter Cihon, *Status of Location Privacy Legislation in the States: 2015*, ACLU: FREE FUTURE (Aug. 26, 2015, 1:15 PM), https://www.aclu.org/blog/free-future/status-location-privacy-legislation-states-2015 [https://perma.cc/H7NW-H8JD].

134. Rachel Levinson-Waldman & Michael Price, *Multi-State Privacy Push Paves the Way for National Reform*, HUFFINGTON POST (Jan. 20, 2016, 2:24 PM ET), http://www.huffingtonpost.com/rachel-levinsonwaldman/multi-state-privacy-push_b_9031692.html [https://perma.cc/TY4X-WH22].

III. A NEW COHERENT REGULATORY REGIME IS NEEDED TO GUIDE AND FOSTER THE DRIVERLESS CAR REVOLUTION.

Today's patchwork of state-based regulation, combined with the inadequacy of existing federal laws, has fueled calls for new regulations and regulatory structures.[135] The rapid rate of technological advancement for driverless cars, combined with increasing globalization, is rendering this approach untenable. Instead, the federal government should take charge and institute a comprehensive nationwide regulatory framework for driverless cars to follow.

A. Given the Interstate Nature of Driverless Cars and Communications, Cybersecurity, and Privacy Pertaining to These Vehicles, Foundational Regulation Should Take Place at the Federal Level.

Highway safety and wireless communications represent two contexts in which a federalized regulatory approach has been pursued over a state-dominant status quo.[136] The concerns regarding safety requirements for driverless vehicles, and the privacy and security of transmitted data between vehicles and between a vehicle and some other infrastructure, are all attendant aspects of these key channels of interstate commerce. As forms of interstate commerce, both highway safety and wireless communications fall under the purview of the Commerce Clause of the U.S. Constitution, making them subject to federal regulation.[137]

Both human-driven vehicles and driverless cars are already regulated at the federal level. Motor vehicle safety in general is regulated by the NHTSA pursuant to the National Traffic and Motor Safety Act of 1966.[138] Wire and radio communication is regulated by the Federal Communications Commission (FCC) pursuant to the Communications Act of 1934.[139] As previously discussed, privacy and cybersecurity have become growing concerns for, and increasingly the province of, the FTC.[140] The FCC has

---

135. *See, e.g.*, Laura Putre, *Speed Up Self-Driving Regulation, Says Volvo CEO*, INDUSTRYWEEK (Oct. 9, 2015), http://www.industryweek.com/regulations/speed-self-driving-regulation-says-volvo-ceo [https://perma.cc/SVU4-RYXG].

136. *Cf.* 49 U.S.C. § 30101 (2012) (stating that the purpose of Chapter 301 of Title 49 of the United States Code is "to prescribe motor vehicle safety standards for motor vehicles and motor vehicle equipment in interstate commerce"); 47 U.S.C. § 151 (2012) (stating that the creation of the Federal Communications Commission is "[f]or the purpose of regulating interstate and foreign commerce in communication by . . . radio so as to make available, so far as possible, to all the people of the United States . . . .").

137. *See* U.S. CONST. art. I, § 8, cl. 3.

138. National Highway Traffic Safety Act of 1966, 49 U.S.C. § 30101 (2012).

139. Communications Act of 1934, 47 U.S.C. § 151 (2012).

140. *See* Federal Trade Commission Act § 5, 15 U.S.C. § 45(a)(1) (2012); Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMMISSION (Aug. 31, 2016, 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc [https://perma.cc/55N6-CHCG] ("As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the

recently directed its attention toward cybersecurity and privacy issues, especially those involving telecommunications networks and the Internet.[141] Other federal agencies have also played a hand in regulation. For example, the National Institute of Standards and Technology (NIST) has promulgated certain cybersecurity standards, and the Intelligent Transportation Systems (ITS) office in the U.S. Department of Transportation has researched privacy protections for connected cars.[142]

Practical concerns also tip the scales toward preferring federal regulation of driverless cars over state regulation. The most important reason counseling against a state-based framework is the risk of inconsistency among state and local regulatory regimes, a concern echoed by the NHTSA.[143] An oddball patchwork of state and local regulations would result in confusion, inefficiency, and stifled innovation.[144] Overarching federal regulation facilitates a commonly understood vocabulary and a uniform regulatory model for driverless car companies and innovators to follow,[145] and, if done right, can foster sustained growth and development.

Leaving driverless car regulation solely to the states also magnifies the harmful impact posed by state regulators' lack of technical expertise, which can lead to uncertainty and hindered innovation due to ineffective legal guidance.[146] This problem is accentuated if poorly conceived laws are enacted in states where the driverless car industry is seeing the most growth. For example, when California proposed regulations requiring self-driving cars to have a human occupant behind a wheel (effectively banning driverless cars), what seemed to be a safety regulation measure on the surface sparked a panic in the driverless car world, given the concentration of companies in that state and its precedent-setting potential.[147] The draft regulations would essentially

---

private sector . . . Section 5 of the FTC Act is the primary enforcement tool that the FTC relies on to prevent deceptive and unfair business practices in the area of data security.").

141. *See generally* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Report and Order*, 31 FCC Rcd 13911, para. 2 (2016).

142. *See* DANIEL J. FAGNANT & KARA M. KOCKELMAN, PREPARING A NATION FOR AUTONOMOUS VEHICLES: OPPORTUNITIES, BARRIERS AND POLICY RECOMMENDATIONS 13 (2013), https://www.enotrans.org/wp-content/uploads/AV-paper.pdf [https://perma.cc/E5MD-GNRF]; Pyle, *supra* note 39.

143. David Shepardson, *U.S. Vows "Nimble, Flexible" Approach on Self-Driving Car Rules*, REUTERS (Dec. 17, 2015, 4:09 PM EST), http://www.reuters.com/article/us-regulations-autos-driverless-idUSKBN0U02XV20151217 [https://perma.cc/FYU3-NFDM].

144. *See, e.g.*, Alex DuFour, *Voice over Internet Protocol: Ending Uncertainty and Promoting Innovation through a Regulatory Framework*, 13 COMMLAW CONSPECTUS 471, 487 (2005) (describing the former state-based regulatory regime of voice over Internet protocol (VoIP) services as increasing uncertainty and compliance costs while decreasing innovation).

145. Putre, *supra* note 135. *But see id.* ("Sam Abuelsamid, an auto industry analyst for Navigant, said that overarching regulation for autonomous vehicles is 'premature' and what the government needs now is to develop 'some minimum performance standards for these systems that can be tested.'").

146. *See* Masunaga, *supra* note 61 ("Jean Shiomoto, director of the California DMV, . . . said . . . that the agency does not have the 'expertise on staff' and has relied on NHTSA for guidance and expertise in autonomous vehicle research.").

147. *Compare* Conor Dougherty, *California D.M.V. Stops Short of Fully Embracing Driverless Cars*, N.Y. TIMES (Dec. 16, 2015), http://www.nytimes.com/2015/12/17/technology/california-dmv-stops-short-of-fully-

ban testing of any driverless vehicle that is "smarter" than currently existing prototypes.[148] Such concerns counsel that federal regulators assume control, perhaps even going so far as to preempt state regulation under the Supremacy Clause of the U.S. Constitution.[149]

The new federal regulatory regime envisioned by this Note should therefore harness the strengths of disparate federal agencies rather than reinvent the proverbial wheel by creating a new agency or forcing an existing agency to leave its comfort zone. A dedicated consortium of government agencies should be created, either through executive order or congressional action, to facilitate the sharing of up-to-date industry information between different entities and to coordinate the crafting of targeted driverless car regulations. At a minimum, this consortium should include the NHTSA, the FTC, the FCC, NIST, and ITS, while other agencies and departments could join the group as circumstances and demands for expertise warrant.

Different agencies should take primary jurisdiction over different aspects of driverless car technologies, with fellow consortium members available to offer additional support. In line with its current jurisdiction over motor vehicle safety,[150] the NHTSA would have responsibility over the hardware aspects of driverless cars and vehicle-specific technologies such as vehicle-to-vehicle (V2V) communications.[151] The FCC would have responsibility over spectrum usage, including consumer protection regulations impacting wireless V2V communications.[152] The FTC could exert jurisdiction over most cybersecurity and data privacy areas, along with enforcement of other consumer protection measures in areas that may not be under FCC jurisdiction, such as onboard software and apps.[153] Meanwhile,

---

embracing-driverless-cars.html [https://perma.cc/VA5J-XL7U], *with* Sarah Buhr, *A Proposed California Law Would Require Drivers for Driverless Cars*, TECHCRUNCH (Dec. 16, 2015), http://techcrunch.com/2015/12/16/a-proposed-california-law-would-require-drivers-for-driverless-cars/ [https://perma.cc/5DR7-XXMY].

148. Davies, *supra* note 61.

149. Dorothy Glancy, *Autonomous and Automated and Connected Cars – Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J.L. SCI. & TECH. 619, 655 (2015) ("Under the Supremacy Clause . . . , such federal autonomous vehicle legislation could preempt varied state laws. . . . If a diversity of state laws regulating autonomous vehicles in different ways appears to stifle the development of autonomous cars, such national law might come under consideration.").

150. *See About NHTSA*, NHTSA, https://www.nhtsa.gov/about-nhtsa [https://perma.cc/86EK-HP4U] (last visited Feb. 21, 2017); *see also* Pyle, *supra* note 39 (citing NHTSA's exerting jurisdiction over V2V technology).

151. V2V communications are a crash-avoidance system in which vehicles sense distances from one another and warn drivers when a crash seems imminent. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., FACT SHEET: IMPROVING SAFETY AND MOBILITY THROUGH VEHICLE-TO-VEHICLE COMMUNICATION TECHNOLOGY 1 (2014), http://www.safercar.gov/staticfiles/safercar/v2v/V2V_Fact_Sheet_101414_v2a.pdf [https://perma.cc/LX8K-9B88].

152. *See* Pyle, *supra* note 39 ("The FCC regulates wireless communication standards used by autonomous vehicles.").

153. *See* Jason Wool, *FTC and FCC Sign Consumer Protection MOU*, ALSTON & BIRD: PRIVACY & DATA SECURITY BLOG (Nov. 30, 2015), http://www.alstonprivacy.com/ftc-and-fcc-sign-consumer-protection-mou/ [https://perma.cc/7ASP-8RKF].

NIST and ITS could continue their work, cooperating with private industry and consumer groups to formulate robust standards for driverless cars.[154]

That a collection of federal agencies would have a hand in regulating driverless cars does not detract from the effectiveness of regulating this industry, nor is this sort of concurrent jurisdiction unheard of. Certain aspects of driverless cars necessarily call for the jurisdiction or expertise of various agencies. For example, NHTSA and the FCC oversee driver-controlled connected vehicles, such as those equipped with GM's OnStar service.[155] While the NHTSA handles many of the vehicle safety implications, the FCC has jurisdictional control over the use of OnStar, most notably when the system transitioned from an analog to digital network in 2008.[156] Another instance of concurrent jurisdiction occurred between the NHTSA and the FTC during GM's ignition switch scandal in 2014.[157] While the NHTSA had responsibility for evaluating the safety of the ignition switch itself, the FTC ultimately probed the company's selling of "certified" used cars with the faulty equipment.[158] The FCC and the FTC have begun to cooperate and share responsibility over areas such as consumer protection, and even signed a memorandum of understanding cementing this relationship in 2015.[159] The two agencies have also engaged in enforcement actions in overlapping jurisdictional areas (but not regarding vehicles), such as when both agencies fined Verizon and Sprint for "mobile cramming," the billing of customers for unauthorized subscriptions and services.[160]

Given these and other past examples of overlapping and/or shared responsibility among multiple federal agencies, it is possible for these agencies to successfully work together in a coherent federal regulatory framework for driverless cars. As noted before, the NHTSA has already taken the lead on establishing guidelines for the burgeoning driverless car industry.[161] The NHTSA has also kept the door open for other agencies to join

---

154. *See generally* FAGNANT & KOCKELMAN, *supra* note 142.

155. Peter Svensson, *Old Cell Network Going Off Air*, USA TODAY (Dec. 21, 2007), http://usatoday30.usatoday.com/tech/wireless/2007-12-21-analog-network_N.htm [https://perma.cc/2WYG-XYQF].

156. *Id.*

157. *See* Melissa Burden, *GM Faces FTC Investigation*, DETROIT NEWS (July 23, 2015, 7:35 PM EDT), http://www.detroitnews.com/story/business/autos/general-motors/2015/07/23/gm-faces-ftc-investigation/30567821/ [https://perma.cc/N5Y2-5BKR]; Bill Vlasic & Rebecca R. Ruiz, *Safety Agency Admits Missing Clues to G.M. Ignition Defects*, N.Y. TIMES (June 5, 2015), https://www.nytimes.com/2015/06/06/business/nhtsa-admits-missing-clues-to-gm-ignition-defects.html [https://perma.cc/JUG5-2NGN].

158. *See* Burden, *supra* note 157; Vlasic & Ruiz, *supra* note 157.

159. *FCC-FTC Consumer Protection Memorandum of Understanding*, FCC (Nov. 16, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-336405A1.pdf [https://perma.cc/9KNQ-C2RZ]. The MOU allows both agencies to exercise oversight over common carriers such as broadband providers and to engage in joint enforcement actions against violators of consumer protection regulations involving common carrier services. Wool, *supra* note 153.

160. Andre Revilla, *Verizon and Sprint Ordered to Pay $158 Million in Fines over Cramming Charges*, DIGITAL TRENDS (May 12, 2015, 2:17 PM), http://www.digitaltrends.com/mobile/verizon-sprint-cramming-charges/ [https://perma.cc/AX8R-6F6V].

161. Caygle, *supra* note 21.

the conversation and develop a workable policy.[162] Indeed, it is optimal to allow each of these agencies to share their expertise rather than confining all jurisdiction and responsibility within a single agency.

Detractors may argue that this system of shared responsibility can lead to duplicative action, inefficiency, or shirking by government agencies.[163] However, as stated above, these agencies already have overlapping jurisdiction over traditional human-controlled vehicles. While federal agency overlap in driverless car regulation may lead to some inevitable inefficiency compared to a single agency with overall control, such a coordinated system is far more efficient than having fifty different state jurisdictions potentially enact over fifty different regulatory regimes with little coordination.

B. Within a Federal Framework, States Should Be Allowed to Experiment with Some Regulation, and Private Industry Should Be Allowed to Engage in Some Self-Regulation.

Despite the appeal of a uniform law across the country, it is important to remember that driverless cars will be driving on state-paved roads, governed by state-based traffic laws, and subject to state-level consumer protection statutes. As time-tested laboratories of democracy and policy development, states are already leading the way in allowing and regulating driverless cars on their roads.[164] Even as a federal regulatory regime takes shape in the coming months and years, states should be able to exercise some power to enact innovative legislation in areas such as licensing and conditions of operation, consistent with their traditional powers and duties.[165]

However, state regulation should be limited, and most aspects of driverless car regulation should ideally be deferred to a federal framework.[166]

---

162. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., "DOT/NHTSA POLICY STATEMENT CONCERNING AUTOMATED VEHICLES": 2016 UPDATE TO "PRELIMINARY STATEMENT OF POLICY CONCERNING AUTOMATED VEHICLES" (2016), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Autonomous-Vehicles-Policy-Update-2016.pdf [https://perma.cc/AGS4-J9KD] ("DOT/NHTSA will continue to work . . . with other governmental entities . . . to help ensure that this testing takes place in a way that protects safety on today's roads while increasing safety for tomorrow.").

163. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-375SP, 2016 ANNUAL REPORT: ADDITIONAL OPPORTUNITIES TO REDUCE FRAGMENTATION, OVERLAP, AND DUPLICATION AND ACHIEVE OTHER FINANCIAL BENEFITS 9 (2016) (noting overlapping agency jurisdiction in financial market regulation, resulting in "regulatory processes [being] sometimes inefficient, regulators oversee[ing] similar types of institutions inconsistently, and consumers [being] afforded different levels of protection"); *see also* Jacob E. Gerson, *Overlapping and Underlapping Jurisdiction in Administrative Law*, 2006 SUP. CT. REV. 201, 214 ("Overlapping jurisdiction also creates a risk of shirking by both agencies when Congress observes only outcomes and not effort.").

164. *See* Clark, *supra* note 89; *see also Autonomous | Self-Driving Vehicles Legislation*, *supra* note 36.

165. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., PRELIMINARY STATEMENT OF POLICY CONCERNING AUTOMATED VEHICLES 10 (2013), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf [https://perma.cc/LL4C-B9GM].

166. *See id.* ("NHTSA has considerable concerns however about detailed state regulation on safety of self-driving vehicles . . . .").

As stated before, wayward or ill-considered rules by states crafted by poorly equipped lawmakers and regulators can chill progress in the entire industry. A well-functioning federal regulatory framework should create a fundamental baseline that binds the entire country, but allows states to tack on laws in areas within their traditional control, such as emissions.

On other issues, the private sector, rather than federal or state regulators, should take charge.[167] This is not new; automakers have already joined together and established the Information Sharing and Analysis Center to craft cybersecurity best practices.[168] These developments should be encouraged. As driverless cars rapidly evolve technologically, the snail-like pace of lawmaking and politics makes it impractical for regulators and lawmakers to keep up with the cutting edge of development. For example, with V2V communications, which implicate cybersecurity concerns,[169] there should be room for the private sector to sort out a wide variety of technological and logistical kinks and arrive at industry-wide standards, rather than having them mandated from above. Since the industry usually has more expertise than federal or state regulators,[170] a robust and flexible regulatory regime should allow informed and cooperative creation of widely-adopted industry standards, which in turn permit further innovation. This self-regulation can, and should, be done in collaboration with governmental agencies such as NIST and ITS, among others.

IV. NEW CYBERSECURITY AND PRIVACY REGULATIONS ARE NECESSARY TO PROTECT CONSUMERS AND PROMOTE FUTURE GROWTH.

Creating a federal regulatory consortium is only a start. Given the patchwork of federal cybersecurity and privacy laws in existence, robust regulations created by the proposed federal driverless car consortium will pave the best way forward in overcoming these collective action problems and growing this nascent technology industry.

---

167. *Cf.* Pyle, *supra* note 39 ("[T]he United States auto industry has made a concerted effort to self-regulate.").

168. *Id.*; Ryan Beene, *Automakers Form Alliance to Bolster Cybersecurity*, AUTO. NEWS (Aug. 24, 2015, 12:01 AM), http://www.autonews.com/article/20150824/OEM06/308249985/automakers-form-alliance-to-bolster-cybersecurity [https://perma.cc/3PVF-WLX9].

169. Interfering with V2V communications can not only cause more collisions, but also capture crucial location data for surveillance or other purposes. *See* Todd B. Benioff, *Automakers Should Not Be Held Strictly Liable for V2V Hacks*, LAW360 (Oct. 29, 2014, 6:04 PM EDT), http://www.law360.com/articles/591695/automakers-should-not-be-held-strictly-liable-for-v2v-hacks [https://perma.cc/3FXJ-UE4U]; *see also* Jake Williams, *NHTSA Begins to Explore Vehicle-to-Vehicle Communications*, FEDSCOOP (Aug. 20, 2014, 11:42 AM), http://fedscoop.com/nhtsa-begins-explore-vehicle-vehicle-communications/ [https://perma.cc/RP95-XHYZ].

170. *See* Matt McFarland, *How Can We Make Sure That Driverless Cars Are Safe?*, L.A. TIMES (Dec. 22, 2015, 5:00 AM), http://www.latimes.com/business/technology/la-fi-1222-thedownload-driverless-car-safety-20151222-story.html [https://perma.cc/TP69-G2KL].

A. Cybersecurity Concerns Regarding Driverless Cars Should Be Addressed Through Regulatory Action.

Determining the cybersecurity risks of autonomous cars is difficult, and applicable cybersecurity laws "are among the most elusive of the many unknowns" when it comes to driverless car regulation.[171] Given the novelty of driverless vehicle technology, it is extremely hard to predict the exact threats that these cars will face. Analogizing threats to ordinary computers to those faced by connected and driverless cars is also problematic because a car's onboard computers require higher physical endurance thresholds with fewer opportunities for physical upgrades or software updates.[172]

Despite these difficulties, there are still ways to craft robust cybersecurity regulations that strike the balance between encouraging innovation and protecting consumers. Such regulations should aim for a "preventative medicine" approach by having manufacturers proactively protect a vehicle's onboard systems and create mechanisms for systems to self-diagnose potential problems.[173] For example, a regulation could require that systems critical to the safety and functions of a driverless car, such as brakes, run separately from entertainment or informational systems, such as navigation. Such a "partition" can limit the reach of malware and other threats that enter a car's systems.[174]

The proposed NHTSA model offers a useful guide for determining what cybersecurity regulations are important and how to best craft them.[175] For example, a driverless car has multiple entry points into its systems, such as Bluetooth, charging ports, GSM wireless signals, and many more.[176] There are also several ways in which a hacker can damage systems, such as tampering with data or denying service.[177] Understanding these variables may lead to regulations such as the separation of core systems, as explained in the context of "preventative medicine."[178] Another example of potential regulation is self-diagnosis, whereby an onboard system periodically monitors its status and warns drivers of any potential issues.[179] Given the vast number of entry points into a driverless car's systems, some basic capacity of a system to fix itself, or even to notify users to fix it, is necessary for reliable operation.[180] Also, if all else fails, driverless cars should have some means of

171. Glancy, *supra* note 149, at 684.

172. *See* Hiro Onishi, *Paradigm Change of Vehicle Cyber Security*, 4 INT'L CONF. ON CYBER CONFLICT 387 (2012) ("[T]he first difficulty of automotive electronics is that online software updates have not prevailed yet . . . . The second difficulty in vehicle cyber security is that automotive electronics have lower computational performance than ordinary computers, because of the high endurance (temperature, humidity, vibration and others) and longer vehicle life cycle (over 10 years) compared to a computers' one (average 3 years).").

173. *See id.* at 389.

174. *See id.*

175. *See generally* MCCARTHY ET AL., *supra* note 50.

176. *Id.* at 10 tbl.3.

177. *Id.* at 11 tbl.5.

178. *See* discussion *supra* Section IV.A.

179. *See* Onishi, *supra* note 172, at 389.

180. *See id.*

mechanical override to ensure passenger safety, such as braking and unlocking doors.[181] Such measures may alleviate consumer fears regarding a complete loss of control of potentially deadly machines.

Cybersecurity regulations issued by different government entities should nonetheless be coordinated through the proposed interagency consortium. For example, rules impacting V2V communications should be under the purview of the NHTSA, which has already taken steps toward regulating such technology in collaboration with private industry.[182] On the other hand, cybersecurity regulations surrounding apps in a car should be under the purview of the FTC, while the FCC and NIST can have some supporting roles to both the NHTSA and the FTC.

Existing federal laws can also offer limited help in alleviating this data security conundrum. The CFAA is the most prominent example.[183] Many cars today already have onboard computers to control their engines, transmission, brakes, and steering.[184] The integration of new technologies into driverless cars means even more computer modules, computer systems, and data storage units.[185] While there is no case law directly relating to unauthorized access to a car's electronic control unit (ECU), cellphones have been classified by some courts as "computers."[186] This expansion of the definition of "computer" serves as a good indication that the ECU can also qualify as a "computer."[187] Just as unauthorized access or use of cellphones leads one to a CFAA violation, unauthorized access or use of a vehicle's ECU could lead to a violation of the CFAA.[188] However, this law has been criticized as outdated and vague, and its potential application to driverless cars may present a double-edged sword.[189] Detractors charge that it may unintentionally stifle needed innovation if someone tinkers with a car's unit, even in furtherance of well-intentioned academic research.[190] At best, the CFAA serves as an inadequate patch until new driverless car-specific regulations are advanced.

---

181. *Id.*

182. Williams, *supra* note 169; *see* discussion *supra* Sections III.A, B.

183. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

184. *See* Dan Goodin, *Tampering with a Car's Brakes and Speed By Hacking Its Computers: A New How-To*, ARS TECHNICA (July 29, 2013, 10:43 AM), http://arstechnica.com/security/2013/07/disabling-a-cars-brakes-and-speed-by-hacking-its-computers-a-new-how-to/ [https://perma.cc/QS2M-FCK3].

185. Lisa Vaas, *Warning Issued by FBI over Dangers of Car Hacking*, SOPHOS: NAKED SECURITY (Mar. 21, 2016), https://nakedsecurity.sophos.com/2016/03/21/warning-issued-by-fbi-over-dangers-of-car-hacking/ [https://perma.cc/D6QV-H6MK].

186. *See, e.g.*, United States v. Kramer, 631 F.3d 900 (8th Cir. 2011).

187. Cheryl Dancey Balough & Richard C. Balough, *Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?*, AM. BAR ASS'N: BUS. L. TODAY (Nov. 2, 2013), https://www.americanbar.org/publications/blt/2013/11/02_balough.html [https://perma.cc/EN8M-2V8U].

188. *Id.*

189. *See* Jeff Kosseff, *Congress Looks at Car Hacking*, HILL (Oct. 26, 2015, 9:30 AM EDT), http://thehill.com/blogs/congress-blog/technology/257936-congress-looks-at-car-hacking [https://perma.cc/N55Q-R7Y6].

190. *Id.*

B. New Privacy Laws, Regulations, and Guidance Are Also Needed to Address Concerns Specific to Driverless Cars.

Like cybersecurity, yesterday's privacy laws are also woefully inadequate for the task of protecting today's consumers, let alone tomorrow's driverless cars.[191] These laws handle technology such as answering machines instead of smartphones, and intranet mail instead of apps.[192] Consumer protections take the hit as more people transition to newer technologies without appropriate safeguards against surveillance or government disclosure requests.[193]

However, it is also important to acknowledge and understand some countervailing interests. Companies have an interest to sell to potential customers, and they want detailed user information in order to target them with individualized advertising, similar to that encountered on the Internet and on social media.[194] Law enforcement has public safety in mind, along with national security at the federal level.[195] Governments have continually expressed interest in source-identifiable information to discover and stop threats to the public.[196] However, as the documents disclosed by former National Security Agency (NSA) contractor Edward Snowden have shown, there is immense public interest and desire in keeping collected metadata private from both government and business.[197] These concerns apply to driverless cars in much the same way that they do to personal data from cellphones, Internet use, and other forms of modern technology, suggesting that vehicular data may therefore be treated under similar legal principles.[198]

To balance these interests, this Note urges the adoption of privacy regulations by the proposed consortium based on the findings of the U.S. Government Accountability Office's (GAO) 2014 In-Car Location-Based Services report.[199] The report details ten connected car companies' commitments to privacy practices in disclosures, consent and controls, safeguards and retention, and accountability.[200] Respecting these commitments as industry-adopted best practices,[201] the proposed consortium

---

191. *See* Helft & Miller, *supra* note 110.

192. *See id.*

193. *See id.*

194. Kohler & Colbert-Taylor, *supra* note 57, at 122.

195. *See* Helft & Miller, *supra* note 110.

196. *See id.*

197. *See, e.g.*, Susan Page, *Poll: Most Americans Now Oppose the NSA Program*, USA TODAY (Jan. 20, 2014), http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551/ [https://perma.cc/L3QS-ZSS2]; Daniel J. Galligan, *What About Private Sector Data Collection?*, U.S. NEWS & WORLD REP. (Jan. 4, 2014), http://www.usnews.com/opinion/blogs/world-report/2014/01/06/compared-to-private-sector-data-collection-nsa-surveillance-is-nothing [https://perma.cc/DM2Y-4Y8J].

198. Kohler & Colbert-Taylor, *supra* note 57, at 121.

199. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., GAO-14-81, IN-CAR LOCATION-BASED SERVICES: COMPANIES ARE TAKING STEPS TO PROTECT PRIVACY, BUT SOME RISKS MAY NOT BE CLEAR TO CONSUMERS (2013).

200. *Id.* at 6–7 tbl.1.

201. *Id.* at 6 (citing U.S. GOV'T ACCOUNTABILITY OFF., GAO-12-903, MOBILE DEVICE LOCATION DATA: ADDITIONAL FEDERAL ACTIONS COULD HELP PROTECT CONSUMER PRIVACY

should enact regulations and further guidance to detail, cement, and build on these baselines and encourage industry compliance therewith. Such regulations should include: (1) requiring companies to disclose information regarding data collection, use, disclosure, and destruction; (2) requiring companies to gain consumer consent to use data; (3) laying out baseline metrics for storing data; and (4) crafting enforcement mechanisms for companies that breach these obligations. Formalizing these protections will help improve consumer perceptions and confidence regarding connected and driverless car technology.[202]

Statutory and regulatory restraints are also required in order protect consumer privacy and to hinder government agencies, such as the NSA and law enforcement, from overzealous collection of identifiable data. Legislation such as the Geolocational Privacy and Surveillance Act (GPS Act) have been proposed to curtail the government's collection of locational data from both cellphones and other sources, potentially including driverless cars.[203] Such efforts should continue in order to garner and cement consumer trust in emerging technologies such as driverless cars.

V. CONCLUSION

The world of driverless cars is still new, and many aspects of cybersecurity and privacy remain to be explored. Even today, decision makers in both government and private industry are grappling with how an impending brave new world should be regulated. To balance the competing needs of full-throated innovation and gradual integration with our lives, a robust federal regulatory framework with some state and industry participation will yield the flexibility and predictability that government, industry, and society need to help this this exciting new technology thrive.

(2012)) ("Mobile industry associations and privacy advocacy organizations have recommended practices that companies can take to better protect consumers' privacy; we determined that these recommended practices can be applied to the companies discussed in this report.").

202. *See* GAO-12-903, *supra* note 201, at 37 ("Without clearer expectations for how industry should address location privacy, consumers lack assurance that the aforementioned privacy risks will be sufficiently mitigated.").

203. *See* Geolocational Privacy and Surveillance Act, S. 395, 115th Cong. (2017); Geolocational Privacy and Surveillance Act, H.R. 1062, 115th Cong. (2017).