Catholic University Journal of Law and Technology

Volume 25 | Issue 1 Article 6

1-18-2017

Autonomous Cars: Navigating the Patchwork of Data Privacy Laws That Could Impact the Industry

Anthony Jones
Catholic University of America (Student)

AUTONOMOUS CARS: NAVIGATING THE PATCHWORK OF DATA PRIVACY LAWS THAT COULD IMPACT THE INDUSTRY

Anthony Jones*

INTRODUCTION

Over the past several years, the development of new technology has drastically changed how society functions. Mobile smartphones and online social networks are prime examples of technologies that have become ubiquitous in many people's lives. While these technologies have become invaluable to their consumers and citizens, they have also created a host of new privacy law challenges. A similar dynamic is playing out in the transportation sector. Just as the train and the automobile have revolutionized the way consumers travel, many believe that the autonomous car will cause similar disruption in today's transportation market.[1] Autonomous cars could present substantial legal challenges within the realm of privacy law, in the same way that Smartphones have affected how society stores and uses personal data.

Some forecasts predict that millions of autonomous cars could be on the road within the next several years.[2] Given this prospect, governments should establish a regulatory scheme that balances the need to protect personal privacy while allowing this burgeoning industry to flourish without excessive govern-

*J.D. Candidate 2017, The Catholic University of America, Columbus School of Law; St. John's University, B.S.; I would like to thank my family and friends for all their love, support and encouragement. I would also like to thank my professors at Columbus School of Law for their valuable wisdom and insight throughout my law school journey.

1 *See* Michele Bertoncello & Dominik Wee, *Ten ways autonomous driving could redefine the automotive world*, MCKINSEY & CO. (June 2015), http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/ten-ways-autonomous-driving-could-redefine-the-automotive-world; *see also* Stefan Burgstaller, *Cars 2025: Change in the Fast Lane*, GOLDMAN SACHS (Dec. 2015), http://www.goldmansachs.com/our-thinking/pages/cars-2025-change-in-the-fast-lane.html.

2 John Greenough, *10 million self-driving cars will be on the road by 2020*, BUS. INSIDER (July 29, 2015), http://www.businessinsider.com/report-10-million-self-driving-cars-will-be-on-the-road-by-2020-2015-5-6.

ment intervention. While some existing laws will affect the industry's development, there is no uniform federal law governing autonomous cars. Furthermore, only a handful of state legislatures have passed bills aimed at regulating them.[3] Several car and tech companies are moving swiftly to introduce these vehicles to the consumer marketplace in the interim.[4] Google, for example, has spent the last several years testing a self-driving car by having it drive millions of miles in an effort to help it eventually become fully autonomous.[5] Additionally, the ride-sharing service Lyft recently partnered with General Motors to produce a service where autonomous cars will be able to provide consumers with on-demand car service.[6] Toyota, Audi, and Mercedes have already begun testing first generation autonomous vehicles.[7]

These are important developments. In the same way that the smartphone became an essential daily tool for both businesses and consumers, it appears that autonomous cars have the potential to reach just as far.

Some estimates predict that there could be over 10 million fully autonomous vehicles on the road within the next 10 years.[8] Other forecasts are even higher, estimating that "85 million autonomous-capable vehicles are expected to be sold annually around the world by 2035."[9] This raises the question of whether the federal regulatory scheme is prepared to adequately regulate in this area, particularly with respect to privacy and related constitutional protections. As demonstrated by legal rulings relating to smartphones, courts and lawmakers are regularly confronted with digital privacy challenges that accompany the latest technological capabilities found in consumer products.[10] Autonomous

---

3 Gabriel Weiner & Bryant Walker Smith, *Automated Driving: Legislative and Regulatory Action*, CTR. FOR INTERNET AND SOC'Y, http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action (last updated Sept. 8, 2016).

4 *See* Hal Hodson, *The firms who will beat Google to get us into self-driving cars*, NEW SCIENTIST (Jan. 11, 2016), https://www.newscientist.com/article/dn28749-the-firms-who-will-beat-google-to-get-us-into-self-driving-cars/.

5 *Id.*

6 *See* Alex Davies, *GM and Lyft are Building a Network of Self-Driving Cars*, WIRED (Jan. 4, 2016, 8:30 AM), http://www.wired.com/2016/01/gm-and-lyft-are-building-a-network-of-self-driving-cars/.

7 *See* Abby Haglage, *Google, Audi, Toyota, and the Brave New World of Driverless Cars*, THE DAILY BEAST (Jan. 16, 2013, 4:45 AM), http://www.thedailybeast.com/articles/2013/01/16/google-audi-toyota-and-the-brave-new-world-of-driverless-cars.html.

8 Press Release, IHS, Self-Driving Cars Moving into the Industry's Driver's Seat (Jan. 2, 2014) (on file with author).

9 Press Release, Navigant Research, Annual Sales of Autonomous-Capable Vehicles Are Expected to Reach 85 Million by 2035 (Sept. 1, 2015) (on file with author).

10 *See* Eric Lichtblau & Nick Wingfield, *F.B.I. Chief Presses Congress to Act on Data Privacy*, NYTIMES.COM (Feb. 25, 2016), http://www.nytimes.com/2016/02/26/technology/fbi-chief-presses-congress-to-act-on-data-

cars are going to present their own set of challenges to be resolved.

These challenges could become much more common with the rise of the "Internet of Things (IoT)"[11] and the growing array of products that will rely on personal information to function – including autonomous cars.[12] As with any nascent and promising industry,[13] it is crucial that regulators and policymakers ensure that appropriate privacy protections are in place as products enter the consumer marketplace. Moreover, this should be done in a way that does not unduly restrict the natural development of the industry. Doing so could help ensure that regulation does not interfere with bringing consumer benefits and efficiencies to the marketplace. Ultimately, the storage and processing of personal information by autonomous cars could be subject to a variety of laws that govern the use of electronic communications.

With this background, this Note will examine a variety of privacy laws to consider how they will apply to the autonomous car industry. Part I will provide background, historical, and technical information regarding autonomous cars. It will show the speed with which this technology has developed as computing power became more advanced, beginning in the 1980s. Part II will discuss the regulatory structure that currently governs this nascent industry, including recent proposals by the Department of Transportation to provide guidance. Part III will discuss privacy laws that affect autonomous cars, including the Drivers Privacy and Protection Act (DPPA) and the Electronic Communications Protection Act. Part IV will delve deeper into digital privacy laws designed to protect consumer information from third parties, with a specific focus on the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC). Finally, Part V will build off of the current regulatory structure and propose reforms that balance the need to protect consumer privacy, while allowing this promising and game-changing industry to develop.

---

privacy.html?_r=0.

11 *Internet of Things Global Standards Initiative*, ITU (July 2015), http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

12 Natasha Lomas, *The FTC Warns Internet Of Things Businesses To Bake In Privacy And Security*, TECHCRUNCH (Jan. 8, 2015), http://techcrunch.com/2015/01/08/ftc-iot-privacy-warning/.

13 *See* Matthew Claudel & Carlo Ratti, *Full speed ahead: How the driverless car could transform cities*, MCKINSEY & CO. (Aug. 2015), http://www.mckinsey.com/business-functions/sustainability-and-resource-productivity/our-insights/full-speed-ahead-how-the-driverless-car-could-transform-cities.

PART I - THE HISTORICAL BACKDROP AND TECHNICAL INFORMATION

The scientific community has imagined autonomous cars for nearly 100 years.[14] It was not until General Motors, at their 1939 Futurama Exhibit, that they began to see more public exposure.[15] There was then a degree of realization that these vehicles could eventually find their way into the consumer marketplace.[16] This was, in some sense, the autonomous car's first stage of entry into the marketplace. The second stage occurred when German and Japanese engineers successfully created autonomous car prototypes in the late 1970s .[17] In 1977, Tsukuba Mechanical Engineering Laboratory, led by S. Tsugawa, developed what experts deem as the first truly autonomous car.[18] Unlike a conventional car, this vehicle utilized cameras and sensors in order to function, and was capable of traveling over 30 MPH.[19]

About a decade later, German engineers, led by Ernst Dickmanns of Bundeswehr University Munich, completed a series of projects that would help revolutionize the autonomous car industry.[20] This team developed cars in which guidance did not rely on signals from buried cables, but rather on signals from camera sensors placed on the vehicle itself.[21] What made this different from the earlier prototype was its ability to travel at speeds reaching 112 MPH, making it capable of traveling on a modern freeway.[22] The third stage occurred in 1994, with the completion of a cross-country journey by an autonomous Pontiac transport developed by students at Carnegie Mellon University.[23] In keeping with the tradition of previous autonomous vehicles, this model supplemented the camera capabilities with a Global Positioning System (GPS), allowing it to travel from Pittsburgh to Los Angeles with minimal human interference.[24]

---

14 Marc Weber, *Where to? A History of Autonomous Vehicles*, COMPUTERHISTORY.ORG (May 8, 2014), http://www.computerhistory.org/atchm/where-to-a-history-of-autonomous-vehicles/.

15 Tom Vanderbilt, *Autonomous Cars Through the Ages*, WIRED (Feb. 6, 2012, 6:30 AM), http://www.wired.com/2012/02/autonomous-vehicle-history/.

16 *Id.*

17 *Id.*

18 *Id.*

19 *Id.*

20 *Id.*

21 *Id.*

22 *Id.*

23 *See* Todd Jochem et al., *PANS: A Portable Navigation Platform*, *in* IEEE SYMPOSIUM ON INTELLIGENT VEHICLES 107-122 (1995) (describing PANS (Portable Navigation Support) as "a simple, yet powerful platform, designed to work on any passenger vehicle" to make vehicle and computer systems, which assist in research for self driving vehicles, more feasible).

24 *Id.*

The fourth stage of market entry was reflected by the 2004 DARPA Grand Challenge, where the Department of Defense held a competition that required teams to build an autonomous vehicle capable of driving in traffic, performing complex maneuvers such as merging, passing, parking, and negotiating intersections.[25] Spurred in part by these competitions, and enabled by the development of more advanced computing power and devices, several companies were able to design prototypes of first generation autonomous vehicles for the open road.[26] Perhaps the most well-known of these prototypes is the Google self-driving car, which began testing on the open road in 2008.[27] Other companies, such as Toyota and Audi, followed suit five years later by introducing their autonomous cars plans at the annual Consumer Electronics Show (CES) trade show in Las Vegas.[28] Today, many leading car manufacturers have developed prototypes that could reach the market within the next several years.[29]

Autonomous car technology generally relies on "advanced sensors to gather information about the world, increasingly sophisticated algorithms to process sensor data and control the vehicle, and computational power to run them in real time."[30] Most of the vehicles utilize an on-board Global Positioning Satellite (GPS) system to, in effect, learn the roads and the environment around them as manufacturers continue to test these vehicles on the open road.[31] Some also use laser-sensing technology, known as LIDAR, which "measures distance by pointing lasers at targets surrounding the car and analyzing the light that's reflected."[32] In considering various autonomous car prototypes, it is important to recognize the distinction between cars that are fully autonomous and those that are semi-autonomous, because the different designs will have different effects on privacy.[33] As some have pointed out, many use the term "auton-

---

25 Marsha Walton, *Robots fail to complete Grand Challenge*, CNN (May 6, 2004, 10:44 AM), http://www.cnn.com/2004/TECH/ptech/03/14/darpa.race/.

26 Weber, *supra* note 14.

27 *Id.*

28 JAMES M. ANDERSON ET AL., AUTONOMOUS VEHICLE TECHNOLOGY: A GUIDE FOR POLICYMAKERS, xix (2016) (ebook).

29 *See Forecasts*, DRIVERLESS CAR MARKET WATCH, http://www.driverless-future.com/?page_id=384 (last visited Sept. 7, 2016).

30 ANDERSON ET AL., *supra* note 28, at 58.

31 *See* John Patrick Pullen, *You Asked: How Do Driverless Cars Work?*, TIME.COM (Feb. 24, 2015), http://time.com/3719270/you-asked-how-do-driverless-cars-work/ (explaining how scientists have utilized GPS systems to help autonomous cars learn the road).

32 *See* Stephen Hall, *Elon Musk says that the LIDAR Google uses in its self-driving car 'doesn't make sense in a car context'*, 9TO5GOOGLE.COM (Oct. 16, 2015), http://9to5google.com/2015/10/16/elon-musk-says-that-the-lidar-google-uses-in-its-self-driving-car-doesnt-make-sense-in-a-car-context/.

33 *See generally* Dorothy J. Glancy, *SYMPOSIUM: Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J.L. SCI. & TECH. 619, 631-34 (2015).

omous" "to refer to part-time operation of vehicles by intelligent systems capable of independently controlling some or all vehicle operations for part of a journey, or in specific roadway contexts."[34] Others have echoed this view, describing these semi-autonomous cars as vehicles that can "drive autonomously in certain operating conditions—e.g., below a particular speed, only on certain kinds of roads—and will revert to traditional, manual driving outside those boundaries or at the request of a human driver."[35]

There are several examples of this type of technology in the marketplace today. Examples include features such as cruise control and automatic parking that are found in cars produced by Tesla, Audi, and others.[36] Fully autonomous cars, on the other hand, will provide consumers with mobility absent human intervention.[37] They can do so because of their ability to store and utilize vast amounts of data, such as location information gathered from GPS and insurance information.[38]

While experts may apply varying definitions to these vehicles, the most consequential set of explanations was provided by the government agency with jurisdiction over motor vehicle safety. That issue is addressed in the next section.

PART II - THE CURRENT REGULATORY STATE OF AUTONOMOUS CARS

The National Highway Traffic Safety Administration (NHTSA), part of the Department of Transportation (DOT), is the federal government entity tasked with developing safety standards for self-driving cars.[39] Established by the Highway Safety Act of 1970, NHTSA's mission is to "achiev[e] the highest standards of excellence in motor vehicle and highway safety."[40] They do so "by setting and enforcing safety performance standards for motor vehicles and motor vehicle equipment, and through grants to state and local governments to enable them to conduct effective local highway safety programs."[41] In 2013,

---

34 *Id.* at 629.

35 ANDERSON ET AL., *supra* note 28, at 68.

36 Haglage, *supra* note 7.

37 Glancy, *supra* note 33, at 630.

38 *Id.* at 636-38.

39 *See* Letter from Paul A. Hemmersbaugh, Chief Counsel, NHTSA, to Chris Urmson, Director, Self-Driving Car Project, Google, Inc. (Feb. 4, 2016) (on file with author); *see also* John Markoff, *Google Car Exposes Regulatory Divide on Computers as Drivers*, NYTIMES.COM (Feb. 10, 2016), http://www.nytimes.com/2016/02/11/technology/nhtsa-blurs-the-line-between-human-and-computer-drivers.html.

40 *See About NHTSA*, NHTSA, http://www.nhtsa.gov/About (last visited Feb. 15, 2016).

41 *Who We Are and What We Do*, NHTSA, http://www.nhtsa.gov/About+NHTSA/Who+We+Are+and+What+We+Do (last visited Feb.

the NHTSA released its *Preliminary Statement of Policy Concerning Automated Vehicles*, which represented the first major step by federal regulators in defining and categorizing the different types of autonomous cars in the marketplace.[42] As noted in NHTSA's official press release, the guidance had three main objectives. First was to explain the different classifications of vehicles and how they could provide tangible safety benefits to drivers.[43] Second was to provide the public with a summary of research that the agency had conducted on the issue and its research plans for the future .[44] Third was to give "recommendations to states that have authorized operation of self-driving vehicles, for test purposes, on how best to ensure safe operation as these new concepts are being tested on highways."[45] The policy statement defines autonomous vehicles as "those in which at least some aspects of a safety-critical control function (e.g., steering, throttle, or braking) occur without direct driver input."[46] The policy statement also establishes five levels of automation, each describing the degree to which a vehicle utilizes artificial intelligence in order to function.[47] These five levels are as follows:

> No-Automation (Level 0): "The driver is in complete and sole control of the primary vehicle controls – brake, steering, throttle, and motive power – at all times."[48]
>
> Function-specific Automation (Level 1): "Automation at this level involves one or more specific control functions. Examples include electronic stability control or pre-charged brakes."[49]
>
> Combined Function Automation (Level 2): "This level involves automation of at least two primary control functions designed to work in unison to relieve the driver of control of those functions."[50]
>
> Limited Self-Driving Automation (Level 3): "Vehicles at this level of automation enable the driver to cede full control of all safety-critical functions under certain

---

15, 2016).

42 Foley & Lardner LLP, *NHTSA Issues Long Awaited Policy Statement on Driverless Car Technology*, AUTOINDUSTRYLAWBLOG.COM (June 13, 2013), https://www.autoindustrylawblog.com/2013/06/13/nhtsa-issues-long-awaited-policy-statement-on-driverless-car-technology/.

43 Press Release, NHTSA, U.S. Department of Transportation Releases Policy on Automated Vehicle Development (May 30, 2013) (on file with author) [hereinafter NHTSA Press Release].

44 *Id.*

45 *Id.*

46 NHTSA, PRELIMINARY STATEMENT OF POLICY CONCERNING AUTOMATED VEHICLES 3 (2013) [hereinafter NHTSA PRELIMINARY STATEMENT], *available at* http://www.autoalliance.org/index.cfm?objectid=CC9678B0-A415-11E5-997E000C296BA163.

47 *Id.* at 4.

48 *Id.*

49 *Id.*

50 *Id.*

> traffic or environmental conditions and in those conditions to rely heavily on the vehicle to monitor for changes in those conditions requiring transition back to driver control."[51]
>
> Full Self-Driving Automation (Level 4): "The vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip. Such a design anticipates that the driver will provide destination or navigation input, but is not expected to be available for control at any time during the trip. This includes both occupied and unoccupied vehicles."[52]

In the Obama Administration's fiscal year 2017 budget proposal, the Department of Transportation requested $4 billion in funding "to fund research projects and infrastructure improvements tied to driverless cars."[53] Furthermore, the agency is expected to release guidance laying out the "functions that autonomous vehicles must be able to perform to be considered safe."[54] The budget proposal demonstrates the rapid development of industry. It could also signify a sense of urgency among regulators in issuing standards to car producers ahead of mass vehicle introduction to the marketplace.[55]

Cars that are semi-autonomous and fully autonomous (i.e., those that fall within NHTSA's levels 3 and 4) have been the focus of state laws that have been passed thus far and are the basis for most of the proposals released by NHTSA.[56] With respect to level 4 vehicles, both government and non-governmental forecasts say that consumer utilization of these types of cars is not likely to occur in the near future.[57] As a result, most near-term policy proposals and rulemaking will be geared towards cars within level 3, since many of the prototypes we see today are already in this category.[58] Once level 4 prototypes are developed, however, many expect them to be more data-intensive and reliant on real-time data tracking than the level 3 models seen today.[59] It is expected that these vehicles will become "connected" to external wireless networks, such as mobile phones or WiFi connections, in order to take advantage of the Internet of Things. As this occurs, the risks to privacy these vehicles

---

51 *Id*.

52 *Id*.

53 Bill Vlasic, *Administration Proposes Effort on Driverless Cars*, N.Y. TIMES, Jan. 15, 2016, at B3.

54 *Id*.

55 *See* Mark Bergen, *Obama's $4 Billion Plan for Self-Driving Cars Will Make Google Very Happy*, RECODE (Jan. 14, 2016, 10:30 AM), http://recode.net/2016/01/14/obamas-4-billion-plan-for-self-driving-cars-will-make-google-very-happy/.

56 *Id*.; *Autonomous: Self-Driving Vehicles Legislation*, NCSL (July 1, 2016), http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx.

57 *See* Peter Bigelow, *Don't hold your breath waiting for fully autonomous vehicles*, AUTOBLOG (Jan. 20, 2016, 5:45 PM), http://www.autoblog.com/2016/01/20/autonomous-self-driving-vehicles-2030/.

58 *Id*.

59 Ellen Hall, *Self-Driving Cars: Can We Really Trust Them?*, ESURANCEBLOG (June 12, 2013), http://blog.esurance.com/self-driving-cars-can-we-really-trust-them/#.VvCyiRIrImp.

create will increase.[60]

The NHTSA recently issued a notice of proposed rulemaking concerning vehicle-to-vehicle (V2V) communications.[61] It defines V2V as "crash avoidance technology, which relies on communication of information between nearby vehicles."[62] V2V is made possible through "devices, installed in vehicles, that use dedicated short-range radio communication (DSRC) to exchange messages containing vehicle information."[63] In theory, this could enable a system in which data transferred vehicle-to-vehicle or vehicle-to-roadside-objects could be used to greatly improve traffic management, safety, and allow more seamless integration of self-driving cars on the road.[64] Given the DOT's heavy emphasis on the public safety benefits of autonomous cars, coupled with its industry guidance, it is easy to imagine V2V being a crucial element in the ongoing development of first generation models. At the same time, the government is also cognizant of how concerns about privacy, coupled with V2V's perhaps limited short-term benefits, could adversely impact the public perception of this technology.[65] This is demonstrated by recent public opinion polls indicating that many consumers are wary of allowing their cars to do most of the driving.[66]

In addition to V2V technology, some companies have developed specialized car antennas with satellite connectivity, allowing the cars to utilize high-speed broadband access.[67] These links permit the download of satellite data at speeds

---

60 Jason Koebler, *Driverless Cars Are Giant Data Collection Devices, Say Privacy Experts*, MOTHERBOARD (Mar. 14, 2014, 4:30 PM), http://motherboard.vice.com/read/driverless-cars-are-giant-data-collection-devices-say-privacy-experts.

61 Press Release, NHTSA, U.S. Dep't of Trans. Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Comm. Tech. (Aug. 18, 2014) (on file with author) [hereinafter Press Release Advanced Notice].

62 U.S. DEP'T. OF TRANSP., VEHICLE-TO-VEHICLE COMMUNICATION TECHNOLOGY 1 (2014), http://www.safercar.gov/staticfiles/safercar/v2v/V2V_Fact_Sheet_101414_v2a.pdf [hereinafter VEHICLE-TO-VEHICLE].

63 *Id*.

64 Margaret Rouse, *vehicle-to-vehicle communication (V2V communication)*, TECHTARGET, http://internetofthingsagenda.techtarget.com/definition/vehicle-to-vehicle-communication-V2V-communication (last visited Sept. 9, 2016); Will Knight, *Car-to-Car Communication: A simple wireless technology promises to make driving much safer*, MIT TECH. REV., https://www.technologyreview.com/s/534981/car-to-car-communication/ (last visited Sept. 8, 2016).

65 U.S. GOV'T ACCOUNTABILITY OFF., GAO-14-13, INTELLIGENT TRANSPORTATION SYSTEMS: VEHICLE-TO-VEHICLE TECHNOLOGIES EXPECTED TO OFFER SAFETY BENEFITS, BUT A VARIETY OF DEPLOYMENT CHALLENGES EXIST 29 (2013).

66 Amir Nasir & Fawn Johnson, *Voters Aren't Ready for Driverless Cars, Poll Shows*, MORNING CONSULT (Feb. 8, 2016), https://morningconsult.com/2016/02/voters-arent-ready-for-driverless-cars-poll-shows/.

67 Press Release, Intelsat, Kymeta and Intelsat Bring Terabyte Connectivity to the Cars

of 50MB per second, which is "better than most 4G LTE mobile services."[68] Developers of this technology believe that it will become the norm in connected-cars and will be able to provide broadband connectivity to locations that aren't typically reached by other communication networks.[69] Furthermore, the FCC has proposed a rule[70] that would advance 5G wireless technology, which could also be utilized by autonomous cars.[71]

These advanced technological capabilities raise questions about how they will be regulated and which federal agencies would be in charge of doing so. How would the ability of these vehicles to make use of broadband wireless connection capabilities be viewed by the FCC, the agency with general responsibility for spectrum usage and broadband Internet access?[72] With respect to information privacy and data security regulations, would ensuring consumer protections also fall within the purview of the FTC? Or, given their core nature as automobiles, would jurisdiction over the privacy and communications aspects of autonomous cars fall mainly to the Department of Transportation, despite its relative lack of expertise in the digital space? Questions remain as to which agencies will take the lead in regulating a product represents a meld between automobiles, wireless devices, and high speed Internet.

PART III - CARS AND BASIC PRIVACY PROTECTIONS

The first and least complicated law to apply to autonomous vehicles is the Driver's Privacy Protection Act (DPPA). The DPPA was originally enacted in 1994 to protect the privacy of personal information assembled by State Departments of Motor Vehicles (DMVs).[73] The Act was subsequently amended in 1999 to provide more consumer protections.[74] Specifically, it required state

---

of the Future (Jan. 12, 2016) (on file with authors) [hereinafter Press Release Intelstat]; *see also* Alan Boyle, *A satellite antenna on your car: Toyota and Kymeta aim to make it so*, GEEKWIRE (Jan. 16, 2016, 4:00 AM), http://www.geekwire.com/2016/a-satellite-antenna-on-your-car-toyota-and-kymeta-aim-to-make-it-so/.

68 Press Release Intelstat, *supra* note 67; *see also* Boyle, *supra* note 67.

69 *Id*.

70 Use of Spectrum Bands Above 24 GHz for Mobile Radio Service, 81 Fed. Reg. 1801 (proposed Jan. 13, 2016) (to be codified 47 C.F.R. pts. 1, 2, 15, 25, 30 and 101).

71 *Id*.

72 *See* Cecilia Kang, *Court Backs Rules Treating Internet as Utility, Not Luxury*, NYTIMES.COM (June 14, 2016), http://www.nytimes.com/2016/06/15/technology/net-neutrality-fcc-appeals-court-ruling.html (explaining that the FCC now has the authority to regulate Internet service providers as common carriers).

73 *See* Driver's Privacy Protection Act, 18 U.S.C. §§ 2721 (2012); *The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record*, EPIC, https://epic.org/privacy/drivers/ (last visited Mar. 22, 2016) [hereinafter *DPPA and Privacy*].

74 *DPPA and Privacy*, *supra* note 73.

agencies to "obtain a driver's express consent [of the driver] before releasing any personal information, regardless of whether the request is made for a particular individual's information or in bulk for marketing purposes."[75] Some states challenged this law, arguing to the Supreme Court that it violated the principles of federalism.[76] The Court ultimately upheld the law, and it remains in effect today, with many states going further and passing state law strengthening privacy safeguards for personal information collected by the DMVs.[77]

As it stands today, DPPA prohibits the release or use by any State DMV (or any officer, employee, or contractor thereof) of personal information about an individual obtained by the department in connection with a motor vehicle record, and also sets penalties for those who violate it.[78] Covered information includes an individual's photograph, social security number, driver identification number, name, address, telephone number, and medical or disability information.[79] However, the DPPA contains several exceptions permitting this information to be accessed. These include legitimate needs by any government agency in carrying out its functions,[80] and when there is a "use in connection with matters of motor vehicle or driver safety and theft."[81] Another exception is when the information is used for "motor vehicle market research activities."[82]

Assuming that State DMV processes remain the same, regardless of whether someone owns a level 2 or level 3 car; it is likely that this statute would apply to autonomous vehicles.[83] In a broad sense, the NTSHA will have a leading role in the many regulatory aspects of the industry, including, but not limited to helping establish guidance to states as they continue to pass laws piece-by-piece. Regulations involving consumer privacy protections from commercial parties, on the other hand, could also end up being shared with other agencies like the FTC and FCC. This will be especially true if manufacturers produce autonomous cars that have wireless mobile network capabilities. As to privacy protections from government access, recent Supreme Court precedent and federal laws could provide some degree of protection.

---

75 *Id.*

76 *Id.*

77 *Id.*

78 18 U.S.C. §§ 2721(a) (The statue also sets penalties for those who are found liable in violating it).

79 *Id.* at § 2725(3).

80 *Id.* at § 2721(b)(1).

81 *Id.* at § 2721(b)(2).

82 *Id.*; *see, e.g.*, Tim Cushing, *Texas DMV Sells Personal Information To Hundreds Of Companies; Drivers Not Allowed To Opt-Out*, CBS (Feb. 13, 2013), http://dfw.cbslocal.com/2013/02/11/cbs-11-investigates-your-personal-information-for-sale-you-cant-opt-out/.

83 Glancy, *supra* note 33, at 676-77.

A. Government Access and Autonomous Cars

Autonomous cars implicate laws pertaining to "government access to and use of locational and other personal data" and "the private, primarily commercial, use of the personal data."[84] Concern over government access to personal data is rooted in the Fourth Amendment.[85] In this regard, police procedure applicable to autonomous vehicles would likely be guided by several recent Supreme Court decisions regarding surveillance and the reasonable expectation of privacy one has in their vehicle.[86] In *United States v. Jones*, for example, which involved placing a GPS tracker on a suspect's car, the majority focused on the physical intrusion onto private property involved, but the concurring opinion placed emphasis on the "mosaic theory" with respect to car GPS searches.[87] That is, the concurrence was focused on the notion that over time a GPS tracking device placed on a car would harvest enough information to disclose an amount of private information that many citizens could find unreasonable.[88] That same logic would appear to apply to data stored by an autonomous vehicle about where the car had gone, at what speeds, etc.

Data stored within an autonomous car could also bring it within the scope of the Electronic Communications Privacy Act of 1986 (ECPA). The Act regulates when electronic communications can be intercepted, monitored, or reviewed by third parties, making it a crime to intercept or procure electronic communications unless otherwise provided for under law or an exception to ECPA.[89] The Act is divided into three parts. Title I generally outlaws the unauthorized interception of wire, oral, or electronic communications.[90] It does, however, provide procedures for federal, state, and other government officers to obtain judicial authorization for intercepting such communications, and regulate the use and disclosure of information obtained through authorized wiretapping.[91] Title I also states that a judge may issue an order authorizing interception of communications for up to 30 days upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has

84 William J. Kohler & Alex Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles*, 31 SANTA CLARA COMPUTER & HIGH TECH. L.J. 99, 121 (2015).

85 *Id.* at 123-24.

86 *Id.* at 124-25.

87 United States v. Jones, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, J., concurring).

88 Kohler & Colbert-Taylor, *supra* note 84, at 124-25.

89 *Electronic Communications Privacy Act (ECPA)*, EPIC, https://epic.org/privacy/ecpa/ (last visited Sept. 8, 2016) [hereinafter EPIC *ECPA*].

90 *Electronic Communications Privacy Act of 1986 (ECPA)*, OJP.ORG, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last visited Nov. 3, 2016) [hereinafter *ECPA of 1986*].

91 Electronic Communications Privacy Act, 18 U.S.C. § 2518(9) (2012).

committed, or is about to commit a "particular offense" listed in § 2516."[92] Title II focuses on the privacy of stored electronic communications through the Stored Communications Act (SCA).[93] Title III focuses on government conduct with respect to the installation and use of pen registers and trap devices.[94]

Courts have found that the ECPA "protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility" and that it "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility."[95] While the original intent underlying ECPA may have been admirable, the rise of cloud computing and mobile email has raised concerns about whether the SCA reflects the current reality of stored electronic communications such as emails and text messages. Under Section 2703(a), the government is required to obtain a warrant if it seeks access to the content of a communication from an ECS provider that has been in "electronic storage" for 180 days or less.[96] However, under Section 2703(d), the government only needs to obtain a subpoena or a court order in order to access that content.[97] The ECPA of 1968 was originally geared primarily towards the interception of data transferred between telephones and has not been subject to a major overhaul despite the ubiquity of mobile smartphones.[98] This could result in diminished privacy protections when it comes to cloud computing, which has been increasingly utilized by autonomous car manufacturers. Furthermore, privacy advocates point out that while "an e-mail stored on a home computer would be fully protected by the 4th Amendment warrant requirement, only the Sixth Circuit has ruled that all e-mail stored on a remote, cloud computing server is protected."[99] Applied to autonomous cars, which are essentially mobile computers, the circuit split could leave gaps in privacy protections from the government.

As mentioned, autonomous cars rely heavily on gathering and processing of location data, using methods such as GPS tracking and LIDAR.[100] The concurrence in *United States v. Jones* stated that:

GPS monitoring generates a precise, comprehensive record of a person's

---

92 *Id.* at § 2518(1)(b); *Id.* at § 2518(5).
93 *EPCA of 1986*, *supra* note 90.
94 *Id.*
95 Theofel v. Farey-Jones, 341 F.3d 978, 982 (9th Cir. 2003).
96 CHARLES DOYLE, CONG. RESEARCH SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 1 (2012).
97 *Id.*
98 *ECPA of 1986*, *supra* note 90.
99 EPIC *ECPA*, *supra* note 89.
100 Pullen, *supra* note 31.

public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations . . . . Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.[101]

As noted above, this idea is better known as the "mosaic theory," or the idea that over time, disclosing simple location data can yield a large amount of personal information.[102] While the majority of the Court did not rely on the "mosaic theory" in ruling that placing a GPS device on a car for an extended period of time required a warrant under the 4th Amendment, the theory appears to have had some influence in the appellate courts.[103] For example, there is currently a circuit split on whether inspecting historical cellular phone data, through data mining of data from cell tower usage, constitutes a search under the Fourth Amendment.[104] In *United States v. Graham*, the Fourth Circuit also ruled that such a search does indeed constitute a "search" for 4th Amendment purposes.[105] However, both the Fifth Circuit and Eleventh Circuit are in conflict with *Graham*, which could lead the Supreme Court to eventually resolve it.[106] In the context of autonomous cars, the rule described in *Jones* may not be the most applicable. While the case did involve GPS tracking, the device was placed externally on the vehicle and was limited to gathering basic locational data.[107] Autonomous cars, by contrast, can process and gather vast amounts of information in addition to basic GPS information.[108] Many will have voice recognition software, the ability to store text messages and contacts, and high speed broadband capabilities.[109] A more applicable 4th Amendment case is *Ri-*

---

101 Jones, 132 S. Ct. at 955-56 (2012) (Sotomayor, J., concurring).

102 Orin Kerr, *Fourth Circuit adopts mosaic theory, holds that obtaining "extended" cell-site records requires a warrant*, VOLOKH CONSPIRACY (Aug. 5, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/05/fourth-circuit-adopts-mosaic-theory-holds-that-obtaining-extended-cell-site-records-requires-a-warrant/.

103 *Id.*

104 *Id.*

105 United States v. Graham, 796 F.3d 332, 349-50 (4th Cir. 2015).

106 Kerr, *supra* note 102; *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 603-04 (5th Cir. 2013).

107 Jones, 132 S. Ct. at 946.

108 Alexis C. Madrigal, *The Trick That Makes Google's Self-Driving Cars Work*, THE ATLANTIC (May 15, 2014), http://www.theatlantic.com/technology/archive/2014/05/all-the-world-a-track-the-trick-that-makes-googles-self-driving-cars-work/370871/.

109 *See generally* Michael Romer et al., *How Automakers Can Survive the Self-Driving Era*, A.T. KEARNEY 8 (2016), https://www.atkearney.com/documents/10192/8591837/How+Automakers+Can+Survive+the+Self-Driving+Era+%282%29.pdf/1674f48b-9da0-45e8-a970-0dfbd744cc2f (discussing the need and integration of mobile broadband technology to make autonomous cars successful); *see generally* Ryan Dube, *Do Everything in the Car Hand Free With Google Now*, MAKE USE OF (Nov. 24, 2015), http://www.makeuseof.com/tag/do-everything-car-hands-

ley v. California, which held that the police generally may not, without a warrant, search digital information on a cellphone seized from an individual who has been arrested.[110] The aforementioned features of autonomous cars (voice recognition, broadband capabilities) are analogous to the capabilities of the modern smartphone.[111] This suggests that *Riley* may come to govern how courts view warrantless searches of these vehicles.

Riley and *Jones* provide some guidance about how courts would view government access to their data with respect to autonomous cars, given that they involved similarly related technologies (e.g., GPS, mobile broadband access). At the same time, however, they did not specifically involve autonomous cars. The body of precedent regarding the 4th Amendment in relation to autonomous cars is sparse. If and when the Supreme Court confronts this issue, the aforementioned cases will likely be heavily cited. What they likely won't confront is how federal regulatory agencies will deal with protections against the use of consumer information by commercial parties, as opposed to by the government.[112]

Absent congressionally passed legislation dealing specifically with autonomous cars, digital privacy protections should fall to the FTC and FCC with varying degrees.

PART IV – CONSUMER PRIVACY: FEDERAL LAWS IN THE LEAD

A. The FTC and Section 5 Authority

The autonomous car industry could come under the purview of the Federal Trade Commission Act, a consumer protection law that prohibits deceptive and unfair trade practices.[113] The Act empowers the Federal Trade Commission to: "prevent persons, partnerships, or corporations… from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce";[114] conduct investigations relating to the organiza-

---

free-google-now/ (reviewing Google's new hands free technology that allows current automobile drivers to perform tasks such as inquiring about the weather, asking sports scores, obtaining foreign language translations while traveling, and sending SMS text messages, all through voice recognition technology).

110 Riley v. California, 134 S. Ct. 2473, 2485 (2014).

111 *See Smartphones on wheels*, THE ECONOMIST, Sept. 6, 2014, at 16.

112 Kohler, *supra* note 84, at 127 ("While some limited protections exist preventing the government from unrestrained access to vehicle users' private data, very little regulation exists preventing private parties from collecting, aggregating, analyzing, marketing, and monetizing individuals' private data in whatever creative ways they might imagine.").

113 Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2012).

114 *Id.* at § 45(a)(2).

tion, business, practices, and management of entities engaged in commerce;[115] and issue reports of persons, partnerships, and corporations.[116] These broad statutory directives give the FTC the potential to play an increasingly active role in trying to shape the regulatory atmosphere by focusing on autonomous V2V technology.[117]

This potential is illustrated by several recent enforcement actions where the agency alleged the failing to take reasonable and appropriate steps to protect personal information constituted an "unfair act or practice."[118] For example, the FTC charged Nomi Technologies with violating Section 5 of the Act for tracking consumer's physical locations within their stores without notifying them.[119] In 2014, the FTC settled charges against Snapchat based on Snapchat collecting geolocation data about its users even though its own privacy policy said that it would not collect such information.[120] These cases followed *Federal Trade Commission v. Wyndam Worldwide Corporation*, where the agency made clear that "inadequate data security practices can form a basis for a claim of deceptive practices under the FTC Act where a privacy policy states that the business had implemented reasonable and appropriate security measures."[121]

In January 2015, the FTC issued a report entitled *The Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*, where the agency recommended concrete steps that businesses can take to help protect consumers' privacy.[122] The report noted that there are currently over 25 billion connected devices around the world and the number of these devices, including cars, is expected to rise significantly.[123] It also described the safety benefits and data security risks associated with the increased prevalence of connected cars.[124] While acknowledging that the "risk to car owners currently may be small," it also mentioned that they could be "ampli-

---

115 *Id.* at § 46(a).

116 *Id.* at § 46(b).

117 *See* Kelley Drye, *FTC Supports NHTSA's Approach to Privacy in V2V Rulemaking*, AD LAW ACCESS (Oct. 27, 2014), http://www.adlawaccess.com/2014/10/articles/ftc-supports-nhtsas-approach-to-privacy-in-v2v-rulemaking/.

118 Ieuan Jolly, *US Privacy and Data Security Law: Overview*, WESTLAW 6-501-4555 (last updated Aug. 2016).

119 Press Release, FTC, FTC Approves Final Order In Nomi Tech. Case (Sept. 3, 2015) (on file with author).

120 Press Release, FTC, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014) (on file with author).

121 Jolly, *supra* note 118; *see also* First Amended Complaint for Injunctive and Other Equitable Relief at 2, Fed. Trade Comm'n. v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012).

122 Press Release, FTC, FTC Rep. on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Sec. Risks (Jan. 27, 2015) (on file with author).

123 *Id.*

124 *Id.*

fied as fully automated cars, and other physical objects, become more prevalent."[125] To be sure, protections from data security breaches, as alluded to in the report, are not necessarily the same as protecting commercial parties from accessing consumer information; however, the fact that the FTC is contemplating some of the data protection aspects surrounding autonomous vehicles indicates that they will play a role in the regulation of these cars. This is also demonstrated by members of the FTC submitting testimony submitted to the House Committee on Energy and Commerce, which mentioned their involvement helping shape the NHTSA's recently proposed rule regarding V2V communications in autonomous cars.[126] Autonomous cars, like many other consumer products within the realm of the 'IoT', are capable of tracking a driver's location and surroundings then using that information to deliver services.[127]

While providing input on these matters to NHTSA is a positive development, an open question remains as to how much authority the FTC will have to actually enforce the FTC Act once autonomous cars become more prevalent. It has been suggested that the FTC's express authority to provide federal protections of personal data outside of health care, credit reporting, and children, is lacking.[128] Moreover, the language in the FTC Act, at least arguably, allows companies to 'contract around' potential liabilities stemming from lax internal privacy standards.[129]

A national framework to regulate autonomous cars will have to be constructed in a way that addresses these potential deficiencies if a role for the FTC under Section 5 of the Act is envisioned as part of the solution. Even if such a framework grants the FTC the tools needed to do so, there remain questions, discussed below, about how much jurisdiction over these issues will be shared with the FCC. Sharing of jurisdiction is not a new concept. But, what has changed over the past few years is the integration of broadband connections into autonomous cars. In this respect, the FCC has clear directives that

---

125 FTC, INTERNET OF THINGS: PRIVACY AND SEC. IN A CONNECTED WORLD 12-13 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

126 *Examining Ways to Improve Vehicle and Roadway Safety: Hearing Before Subcomm. on Commerce, Mfg., and Trade of the H. Comm. On Energy and Commerce*, 114th Cong. 2-3 (2015) (statement of Maneesha Mithal, Associate Director of the Division of Privacy & Identity Protection of the Bureau of Consumer Protection, Fed. Trade Comm'n), https://www.ftc.gov/system/files/documents/public_statements/826551/151021vehiclesafetytestimony.pdf.

127 *See generally* Adrienne Lafrance, *How Self-Driving Cars Will Threaten Privacy*, THE ATLANTIC (Mar. 21, 2016), http://www.theatlantic.com/technology/archive/2016/03/self-driving-cars-and-the-looming-privacy-apocalypse/474600/.

128 *See* Kohler & Colbert-Taylor, *supra* note 84, at 127-28.

129 *Id.* at 128.

might not be matched when it comes to the regulation of broadband-connected devices.

B. The Federal Communications Commission and Section 222 of the Communications Act

One of the key features that differentiates autonomous cars from most current vehicles is their increased reliance on broadband Internet access.[130] In this regard, the FCC may well play a significant role helping to ensure that consumer information is given appropriate privacy protections.

The FCC is an independent federal agency that "regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories."[131] It is the country's "primary authority for communications law, regulation and technological innovation."[132] The FCC was granted this authority in the Communications Act of 1934, which has been amended many times since its enactment.[133] The most recent major overhaul of the Communications Act was the Telecommunications Act of 1996,[134] which was "designed e-regulate aspects of the telecommunications business."[135] These amendments dealt with the ongoing development and increasing technological overlap of innovations such as the cellular phones, cable television, and satellite communications.[136] The Act is broken up into six parts, three of which are most relevant here.[137] Title I lays out general provisions and states the FCC's purpose,[138] while Title V describes the Commission's general rules governing the imposition of penalties against violators of the Act.[139] Title II imposes regulations on providers of telecommunications services, or "common carriers."[140] In the FCC's 2015 Open Internet Order, the

---

130 *See generally Driverless cars: Look, no hands*, THE ECONOMIST (Apr. 20, 2013), http://www.economist.com/news/special-report/21576224-one-day-every-car-may-come-invisible-chauffeur-look-no-hands.

131 *About the FCC*, FCC, https://www.fcc.gov/about-fcc/what-we-do (last visited Mar. 22, 2016).

132 *Id.*

133 *FCC Regulations*, USLEGAL.COM, http://telecommunications.uslegal.com/fcc-regulations/ (last visited Mar. 22, 2016).

134 Telecommunications Act of 1996, 47 U.S.C. § 151-662 (2012).

135 David McCabe, *Bill Clinton's telecom law: Twenty years later*, THE HILL (Feb. 7, 2016), http://thehill.com/policy/technology/268459-bill-clintons-telecom-law-twenty-years-later.

136 *See Telecommunications Act of 1996*, CYBERTELECOM, http://www.cybertelecom.org/notes/telecomact.htm (last visited Sept. 9, 2016).

137 47 U.S.C. §§ 151-621 (2012).

138 *Id.* at § 151.

139 *See generally id.* at §§ 501-510.

140 *See generally id.* at §§ 201-276; *see also* KATHLEEN ANN RUANE, CONG. RESEARCH

agency deemed providers of broadband Internet access services (BIAS) to fall within the purview of Title II.[141] The Order was subsequently challenged by a consortium of telecommunications companies, but was upheld by the D.C. Circuit Court of Appeals in June 2016.[142] While the agency chose not to apply a wide range of Title II "utility-style" regulation to BIAS providers, the agency chose to subject Internet Service Providers (ISPs) to the same general regime governing other common carriers.[143] The common carrier regime includes a variety of consumer protection rules, including those that safeguard the use of customer proprietary network information (CPNI) pursuant to Section 222 of the Communications Act.[144] This could have significant implications on the autonomous cars industry, given how the broadband capabilities of autonomous cars could conceivably bring the entities providing those vehicles within the definition of "common carrier" for purposes of privacy regulation."[145]

Section 222 imposes a duty on telecommunications carriers to maintain the confidentiality of proprietary information, stating "[e]very 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."[146] It goes on to state that "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information."[147] Section 222(f) concerns the use of locational information and, at least conceptually, fits into the core function of broadband connected autonomous cars.[148] It provides:

SERV., R43971, NET NEUTRALITY: SELECTED LEGAL ISSUES RAISED BY THE FCC'S 2015 OPEN INTERNET ORDER 3 (2015).

141 *See* 47 U.S.C. §§ 201-276 ("The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter."); *see also* RUANE, *supra* note 140.

142 United States Telecom Ass'n v. FCC, 825 F.3d 674, 726 (D.C. Cir. 2016).

143 RUANE, *supra* note 140.

144 47 U.S.C. § 222(a) (2012).

145 *See generally* Natasha Lomas, *As FCC considers new broadband privacy rules, report urges wider user data safeguards*, TECHCRUNCH (Mar. 23, 2016), http://techcrunch.com/2016/03/23/as-fcc-considers-new-broadband-privacy-rules-report-urges-wider-user-data-safeguards/ (discussing how the expansion of the definition has led to reclassification of Google and what that may mean for other technologies that gather information).

146 47 U.S.C. § 222(a).

147 *Id.* at § 222(c)(1).

148 *Id.* at § 222(f); *see, e.g.*, Pullen, *supra* note 31.

> [W]ithout the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to . . . call location information concerning the user of a commercial mobile service . . . or the user of an IP-enabled voice service . . . or . . . automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.[149]

The Commission has used its enforcement power to impose several significant fines on companies for Section 222 violations in recent years.[150] The most notable of these enforcement actions took place in 2015, when the Commission imposed a civil penalty of $25 million on AT&T for failing to protect the confidentiality of 280,000 of their customer's information.[151] This trend could continue given a recent Notice of Proposed Rulemaking (NPRM) that signifies the FCC taking a more proactive role in regulating the use of CPNI by ISPs.[152]

The NPRM is one of the immediate impacts of the Open Internet Order of 2015[153] and provides some insight into how it could affect ISPs.[154] It could by extension affect self-driving cars in light of their potential reliance on high-speed broadband Internet service and suggests what a regulatory framework governing autonomous car privacy might look like. The framework laid out in the NPRM would "require broadband providers to take reasonable steps to safeguard customer information from unauthorized use or disclosure," while also creating an opt-in and opt-out mechanism with respect to sharing consumer data with third parties.[155] The NPRM also specifically mentions how "geo-location" services meet the definition of CPNI;[156] and the FCC has previously held that "[t]he location of a customer's use of a telecommunications service

---

149 § 222(f)(1)-(2).

150 *See, e.g.*, *In re* Terracom, Inc. & Yourtel Am., Inc., Notice of Apparent Liability for Forfeiture, 29 FCC Rcd. 13325, 13332 ¶ 20 (Oct. 14, 2014); *see also* Press Release, FCC, Cox Communications to Pay $595,000 to Settle Data Breach Investigation (Nov. 5, 2015) (on file with author).

151 *See In re* AT&T Mobility, LLC., Order, 30 FCC Rcd. 6613 ¶ 2 (Apr. 8, 2015).

152 *See generally* Lomas, *supra* note 145 (The FCC is "now seeking to further flesh out what's at stake – by profiling in some detail the data harvesting practices of specific ISPs and [CPNIs]...").

153 *See* Allison Grande, *FCC Broadband Privacy Rules Set ISPs Apart On Liability*, LAW360 (Mar. 11, 2016, 10:21 PM), http://www.law360.com/articles/770537/fcc-broadband-privacy-rules-set-isps-apart-on-liability ("The FCC began crafting broadband-specific privacy rules last year, after the commission issued its Open Internet Order that reclassified broadband providers as common carriers...").

154 *See* FCC, CHAIRMAN WHEELER'S PROPOSAL TO GIVE BROADBAND CONSUMERS INCREASED CHOICE, TRANSPARENCY & SECURITY WITH RESPECT TO THEIR DATA 1 (2016), https://www.fcc.gov/document/broadband-consumer-privacy-proposal-fact-sheet.

155 *Id.* at 2.

156 Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, 81 Fed. Reg. 23359, (Apr. 20, 2016) (to be codified at 47 CFR pt. 64) [hereinafter Protecting Privacy].

also clearly qualifies as CPNI."[157] Essentially, the proposal will broaden the scope of Section 222 CPNI rules so that "[i]nternet providers could not, without consent, track customers using a unique number tied to a customer's Internet activity or phone location."[158]

The degree to which the functions of autonomous vehicles will be intertwined with the broadband offerings is not yet clear, but ultimately will be crucial in determining how the autonomous car industry will be affected by the FCC's CPNI rules. Recent developments indicate that there will indeed be a lot of interaction, as several car manufacturers are partnering with mobile broadband providers in integrating high-speed Internet into the cars.[159] This serves to buttress the argument that the FCC's role in protecting privacy with respect to the information generated by the cars should be increased, in light of their established CPNI rules and its proposed privacy rules for ISPs. Even outside of the realm of information privacy, the FCC's involvement in issues affecting autonomous cars would not be an entirely new development.[160] In 1999, the FCC contemplated the allocation of 5.9 GHz spectrum for Dedicated Short-range Communications (DSRC) to "be used by 'intelligent transportation solutions' in the future, such as intersection collision avoidance."[161] The technology that has developed since then has led to an increased recognition that DSCR will play a large role in the autonomous car industry, demonstrated by the fact that V2V systems now rely on the 5.9GHz band.[162] Indeed, FCC Commissioners have aptly pointed out "when DSRC was new, driverless cars were the stuff of science fiction. But autonomous and semi-autonomous vehicles are now not only on display at the Consumer Electronics Show—they are being tested on our roadways."[163] This could signify a greater sense of urgency by regulators in

---

157 *Id.*

158 Julia Angwin, *5 Things You Should Know About the FCC's Proposed Privacy Rules*, PROPUBLICA (Mar. 14, 2016, 11:35 AM), https://www.propublica.org/article/5-things-you-should-know-about-the-fccs-proposed-privacy-rules.

159 *See Connected Car*, AT&T, http://about.att.com/sites/internet-of-things/connected_car (last visited Nov. 7, 2016); *see also* Damon Lavrinc, *Sprint, Chrysler Link Up With 'Velocity' In-Car System*, WIRED (Nov. 27, 2012, 8:00 PM), http://www.wired.com/2012/11/sprint-velocity/.

160 *See generally* Julian Hattem, *Execs pitch FCC on connected cars*, THE HILL (Oct. 29, 2014, 6:18 PM), http://thehill.com/policy/technology/222277-execs-pitch-fcc-on-connected-cars.

161 Owen Williams, *The FCC wants to test sharing 5.9GHz Wi-Fi spectrum with connected cars*, NEXTWEB, http://thenextweb.com/insider/2016/01/12/the-fcc-wants-to-test-sharing-5-9ghz-wi-fi-spectrum-with-connected-cars/#gref (last visited Sept. 7, 2016).

162 *Issues in action*, GLOBAL AUTOMAKERS, https://www.globalautomakers.org/topic/vehicle-vehicle-technology (last visited Sept. 7, 2016).

163 Williams, *supra* note 161.

the autonomous car industry.

The broadband capabilities of autonomous cars, combined with the FCC's increasingly active role in protecting consumer information following the re-classification of BIAS as a telecommunications service, help make the case for the FCC taking a leading role in consumer privacy protections. The FCC has a demonstrated expertise in regulating wireless and wireline communications, and, given the digital footprint of autonomous cars, it makes sense to have the FCC regulate at least the CPNI element of their operations. Section 222 grants them the authority to do so. Indeed, "the Federal Communications Commission itself has a long history of protecting privacy."[164] The privacy protections found in Section 222 could by extension provide at least some degree of consumer privacy protections until Congress takes action to address the issue.

As the industry continues to develop however, it is doubtless that questions will continue as to how jurisdiction over all aspects of autonomous vehicles will be shared among the various agencies with some claim to authority. There will also be questions about how such regulation will affect participants in the broader Internet ecosystem. After all, broadband-connected cars could be just one such participant, along with "edge" providers who are not subject to the Open Internet Rule's reclassification. In the realm of inter-agency rivalry, the main jurisdictional battle when it comes to digital privacy is between the FCC and the FTC.

PART V – TILTING THE BALANCE TOWARDS AN FCC-LED APPROACH

In late 2015, the FCC and FTC jointly released a Memorandum of Understanding on Consumer Protection.[165] The memorandum was "designed to formalize the existing cooperation between the agencies, outlining how the FCC and FTC will coordinate consumer protection efforts" and "methods by which the agencies will coordinate and share information, and recognizes the agencies' expertise in their respective jurisdictions."[166] The memorandum is important due to the FCC's recently upheld 2015 Open Internet Order, specifically with respect to BIAS. The reclassification of BIAS providers as "common carriers" under Title II[167] has essentially taken ISPs away from the FTC's reach when it comes to consumer privacy protections. This is because under Section

---

164 Protecting Privacy, *supra* note 156.

165 Margaret Harding McGill, *FCC Teaming Up With FTC On Consumer Protection*, LAW360 (Nov. 16, 2015), http://www.law360.com/articles/727540/fcc-teaming-up-with-ftc-on-consumer-protection.

166 Press Release, FCC, FCC and FTC Sign Memorandum of Understanding for Continued Cooperation on Consumer Protection Issues (Nov. 16, 2015) (on file with author).

167 RUANE, *supra* note 140, at 8.

5 of the FTC Act, "*common carriers* subject to the Acts to regulate commerce" – which includes the Communications Act – are exempt from the statute.[168] The D.C. Circuit's clear affirmation of the 2015 Order means that agency could move swiftly to finalize and enforce Section 222 rules with respect to BIAS providers.

Nonetheless, the memorandum makes clear that the "common carrier exception does not preclude the FTC from addressing non-common carrier activities from common-carriers,"[169] which means that the FTC could still play a role if those activities are integrated into broadband-connected cars. Both agencies committed to releasing joint enforcement actions and sharing information about consumer complaints, which is valuable in that it sends at least some guidance to the industry about which agencies will have data privacy jurisdiction.[170] More broadly, the memorandum's objectives are indicative of what an autonomous car regulatory regime could look like where multiple agencies are faced with information and resource sharing in tackling a specific industry.

While such coordination among agencies obviously makes sense where their jurisdictions overlap, it is not clear that these arrangements are the most effective use of federal resources. Arguably, an FCC-led approach to CPNI – including as related to autonomous cars – may be better suited to ensure adequate consumer privacy protections while optimizing efficient use of government resources. In light of the D.C. Circuit's Open Internet Order Opinion, the FCC would appear to have more regulatory authority and thus more ability to provide incentives to those ISPs that provide service to cars, to comply with federal rules. The CPNI rules, despite not mentioning autonomous cars (in their currently proposed form), could reach the industry by virtue of broadband integration into the vehicles. The counter-argument to an FCC-led approach is that it could create a regulatory disparity between "edge providers," which are regulated by the FTC on these matters, and ISPs. This incongruence could result in negative "competitive ripple effects" within the broadband ecosystem."[171] Also, a regulatory approach that is too onerous and complicated could impede the autonomous car industry from progressing and innovating. From this perspective, it would also be possible to simply use the FTC's Section 5 framework regarding unfair and deceptive practices, and apply that framework to ISPs, and then by extension to autonomous cars. This could provide industry

---

168 15 U.S.C. § 45(a)(2) (2012).

169 FCC & FTC, FCC-FTC CONSUMER PROTECTION MEMORANDUM OF UNDERSTANDING 2 (2015).

170 *Id*.

171 Protecting Privacy, *supra* note 156 ("We recognize that edge providers, who may have access to some similar customer PI, are not subject to the same regulatory framework, and that this regulatory disparity could have competitive ripple effects.").

with some predictability, since the FTC has a "rich body of precedent, in enforcement actions and consent orders that measures privacy against the unfair-or-deceptive standard" contained in Section 5.[172]

But the fact still remains that the reclassification of BIAS as common carriers clearly puts them within the jurisdiction of the FCC, and at least with regards to their common carrier activities, beyond the authority of the FTC. Following this interpretation could actually provide more predictability than Section 5 of the FTC, since they provide bright line rules. The Communications Act grants the FCC the authority to "prescribe rules that may be necessary in the public interest to carry out the Act," while also giving the agency the authority to "interpret and implement Section 222's provisions." Also, the FCC could also have authority in Section 705 of the Communications Act, which states that providers of communications services by wire and radio have obligations not to "divulge or publish the existence of, contents, substance, purport, effect, or meaning" of communications that they carry on behalf of others.[173] In either case, it would behoove the industry to realize that the very thing that makes autonomous cars functional (broadband connections) puts them squarely within the FCC's jurisdiction.

Autonomous cars themselves (as opposed to the entities providing communications links between autonomous cars and the Internet) are not likely to be viewed as "edge providers."[174] An autonomous car is, ultimately, a device, more akin to a MacBook than to Facebook.[175] Indeed, current regulations interpret edge providers as entities such as Netflix and YouTube, which are much less analogous to cars compared to a tablets, smartphone, and computers. Most importantly, autonomous cars as they exist today embody the functions of communications devices, similar to cellular phones and computers.

CONCLUSION

Autonomous cars are, in a sense, a microcosm of the larger jurisdictional fight regarding privacy regulation, specifically between the FTC and FCC.

---

172 *Id.*

173 Telecommunications Act, 47 U.S.C. § 605(a) (2012).

174 Protecting and Promoting the Open Internet, 79 Fed. Reg. 37447 (July 1, 2014) (to be codified at 47 C.F.R. pt. 8) (This Note is making a connection in how an autonomous car is analogous to a coffee shop, in terms of how the phone *in* a coffee shop operates as a separate entity to the coffee shop, just as the device *in* the autonomous car operates separately than the car); *see also* Alan Galloway, *The Open Internet Order's Changes Regarding Edge Providers*, OPENINTERNETLAW (June 11, 2015), www.openinternetlaw.com/2015/06/the-open-internet-orders-changes-regarding-edge-providers/.

175 Jamie Condliffe, *Nvidia's Autonomous Car Computer Makes 24 Trillion AI Operations a Second*, GIZMODO (Jan. 5, 2016, 3:42 AM), http://gizmodo.com/nvidias-autonomous-car-computer-makes-24-trillion-deep-1751078739.

However, given the communications element of these cars and the recently upheld reclassification of BIAS, the FCC's regulations under Section 222 should provide a blueprint for regulating privacy in the burgeoning autonomous car industry. To be sure, the FTC should play a collaborative role, as the MOU states. But is nothing in the MOU that precludes the FCC from demonstrating stringent privacy protections standards for the industry to follow as it continues to develop. Doing so would in fact be following the letter of the law. While there could be an argument that privacy laws should develop at the state level, it is doubtful that they would be broad and comprehensive enough to regulate a medium as ubiquitous as the Internet. The Internet provides interstate communications, as opposed to intrastate, which means that a federal approach makes more sense.

The development of autonomous cars is evolving rapidly. Unless and until Congress enacts federal regulations focused specifically on privacy protections in the industry, Section 222 provides a blueprint and helps ensure strong privacy protections. The enforcement of this statute should fall within the purview of the FCC, with the FTC playing an augmenting role in specific cases.