12-19-2018

Evolving Autonomous Vehicle Technology and the Erosion of Privacy

Raquel Toral

Evolving Autonomous Vehicle Technology and The Erosion of Privacy

Raquel Toral*

* Articles and Comments Editor, *University of Miami Business Law Review*; Juris Doctor Candidate 2019, University of Miami School of Law; International Arbitration Legum Magister Candidate 2019, University of Miami School of Law; Bachelor of Arts in Political Science 2014, Florida State University. The author thanks Professor Donald M. Jones for his comments, suggestions and guidance. The author would also like to thank the editors of the *University of Miami Business Law Review* for their exemplary edits and work on this Note.

INTRODUCTION

The transition from automated vehicles to self–driving cars is fast approaching. Autonomous vehicles have already transformed the global technological landscape—and are only beginning. The United States' "SELF DRIVE Act"[1] will allow up to 100,000 autonomous vehicles on its roads by 2020.[2] Relatedly, the U.S. Transportation Secretary has actively encouraged states to reevaluate their traffic laws and regulations to guarantee compatibility with autonomous technology.[3]

However, autonomous vehicles' plethora of benefits comes at a substantial cost, namely the evisceration of individual privacy and autonomy. Given the amount of data to be managed by IT companies, "self–driving cars could very well turn automotive suppliers into glorified IT companies, with telematics becoming as important as the hardware these companies traditionally specialize in."[4]

This begs the question of what is private information? What information is likely to become public through autonomous driving systems? What information is likely to be admissible as evidence? Does the data streaming from an autonomous vehicle deserve warrant protection under the Fourth Amendment?[5] More specifically, is this data protected under the theory of an individual's reasonable expectation of privacy?[6] Is there any difference between a digital record and a physical document that might otherwise fall under the "papers" protection of the Fourth Amendment?[7] Put simply, the increased and prevalent use of autonomous

---

1 Self Drive Act, H.R. 3388, 115th Cong. (as passed by House, Sept. 6, 2017) (The bill requires the Department of Transportation to "[c]omplete research to determine the most cost effective method and terminology for informing consumers about the capabilities and limitations of each automated vehicle or each vehicle that performs partial driving automation; and determine whether such information includes terminology as defined by SAE International in Recommended Practice Report J3016.").

2 *See House Passes Bipartisan Legislation Paving the Way for Self-Driving Cars on America's Roads*, ENERGY & COM. COMMITTEE https://energycommerce.house.gov/selfdrive/ (last visited Jan. 22, 2018).

3 *See Federal Automated Vehicle Policy*, U.S. DEP'T. OF TRANSPORTATION (Sept. 2016), https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016.

4 Stephen Edelstein, *LG and Here Team Up on Self-Driving Car Telematics*, THE DRIVE (Dec. 17, 2017), http://www.thedrive.com/news/17208/lg-and-here-team-up-on-self-driving-car-telematics.

5 *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547 (2017).

6 *Id.*

7 *Id.* (quotations omitted).

vehicles will place fundamental privacy interests at stake concerning access, use and policy issues.

This Note examines Fourth Amendment implications regarding data collected and stored by autonomous vehicles. Whether this data is protected by the Fourth Amendment is critical to answer the threshold question of whether there has been a Fourth Amendment search.[8] Part I of the Note explains what an autonomous vehicle is, including its capabilities and development. Part II examines the present state of autonomous vehicle technology and its relation to the current laws and regulations in place. This Note identifies several issues with respect to the disparity between our current legal framework, the Fourth Amendment, and privacy. Part III discusses the hidden dangers associated with autonomous vehicle ("AV") technology and explains why the information collected by a self–driving car serves as a nexus to unrecognized violations of privacy under the Fourth Amendment. Part IV describes the existing laws and proposes modifications to account for autonomous vehicle technology that focuses specifically on issues regarding privacy and the collection of data. Part V concludes the data streaming from an autonomous vehicle warrants protection under Fourth Amendment and the present need for a new theory to protect the data trails an autonomous vehicle leaves behind.[9] This Note has sought to highlight for courts and scholars the need for the development of a new theory to account for the principle of informational security that underlies the Fourth Amendment doctrine.

I. THE RISE OF AUTONOMOUS VEHICLES

A. A Radically Changing Consumer World

Progressing from Motor Vehicles to Autonomous Vehicles

Today's advanced technologies have made autonomous vehicles a reality.[10] As the current crash avoidance technology continues to develop in conjunction with autonomous driving systems, vehicles will drive autonomously.[11] In fact, car manufacturers, from Mazda to Maserati, are working to incorporate these technologies into a larger part of their

---

8 *Id.* at 550 n.13 (citing James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 324–26 (2002)) (discussing the importance of threshold questions).

9 *See generally* Ferguson, *supra* note 5 (alterations added).

10 Stephen P. Wood et al., *Symposium Article: The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles*, 52 SANTA CLARA L. REV. 1423 (2012) (quotations omitted).

11 *Id.* (alterations added).

operational fleet of vehicles.[12] Car manufacturers are not the only ones who want your hands off the wheel—dozens of technology companies, big and small, have designs on the drive as well.[13] Key industry experts, such as Delphi Technologies, share a similar confidence in vehicle–to–vehicle ("V2V") technology, which allows automakers to "[r]eap the rewards of wide–scale data collection."[14] In support of the potential capabilities of V2V technology, studies conducted by the National Highway Traffic Safety Administration ("NHTSA") conclude "[v]ehicle communications have the potential to act not only as enabling technology for autonomous motor vehicles, but also as a technology that can enhance an autonomous vehicle's ability to identify potential problems and take appropriate actions to avoid them."[15]

Notwithstanding the rapid advancements being made, several technological roadblocks remain before the public can expect widespread use of autonomous vehicles.[16] Chris Urmson, a self–driving car pioneer, identifies two key issues inhibiting the use of autonomous vehicles. First, getting the technology so that it deals with those hard problems of driving, specifically by dealing with these rare events where the system gets pushed to really have to perform well.[17] Second, "manufacturing and bringing

---

[12] Jeremy Kaplan, *Here's Every Company Developing Self-Driving Car Tech at CES 2018*, DIGITAL TRENDS (Jan. 7, 2018, 7:30 PM), https://www.digitaltrends.com/cars/every-company-developing-self-driving-car-tech-ces-2018/.

[13] *See id.* (quotations omitted) ("[T]here's a fleet of companies with new interfaces to facilitate how you interact with your car [human-machine interaction, or HMI]." For example, the company Aptiv, which was once part of Delphi—and once a part of General Motors—is allegedly "[t]he biggest name in automotive components" according to Kaplan) (alterations added).

[14] Katie Burke, *Making a Case for V2V, Suppliers Push Automakers to Take Lead*, AUTOMOTIVE NEWS (Jan. 8, 2018, 12:01 AM), http://www.autonews.com/article/20180106/MOBILITY/180109888/vehicle-to-vehicle-communication-tech (Burke explains that "[t]he industry doesn't need to wait for self-driving vehicles to tap into that data stream; it could use V2V [technology] that is market ready" because "[s]elf-driving vehicles are expected to be a boon to data collection, using sensors and cloud connections to feed data about traffic and unexpected obstacles to other vehicles on the road." In fact, experts opine that, when V2V data can be extracted and used in real time, then we will be "more efficient in how we travel.").

[15] *See* Wood et al., *supra* note 10, at 1434 (noting "V2V communications have the potential to provide additional information to the autonomous motor vehicle (covering areas beyond the range of the on-board sensors) and enable more robust performance of autonomous driving technologies.").

[16] *Q&A with Self-Driving Car Pioneer Chris Urmson*, WHEELS 24 (January 7, 2018, 09:11), https://www.wheels24.co.za/News/Gear_and_Tech/qa-with-self-driving-car-pioneer-chris-urmson-20180107.

[17] *See id*. (alterations added).

[autonomous vehicles] to market at scale" or, in other words, how to build the *right* self–driving system.[18]

But the industry faces other pressures. In the United States, for example, the proposed federal mandate to equip cars with V2V technology has been stalled by the Trump Administration, which dissuades automakers from adopting V2V technology.[19] In support of the U.S. Department of Transportation's ("DOT") broader self–driving push, NHTSA announced in October 2018 that it is actively seeking input from companies to guide the new AV test projects where the Agency could temporarily lift rules that pose obstacles to those tests.[20]

Autonomous Vehicles and Wireless Communication Technologies

In order to properly allocate, assign, and manage the technological capacities of an autonomous vehicle, the regulatory framework must ensure it's utilized in a manner that serves the public interest.[21] It's no secret that AV startups and other companies are in the race for data to "teach" the artificial intelligence ("AI") systems—given the amount of data you have affects how much a person can rely on the system—and, in order to get the right level of safety, requires a lot of data. For example, startups such as Blue Vision Labs have developed virtual maps that allow multiple users to see the same virtual objects and interact with each other in that virtual space with spatial accuracy.[22] Accordingly, a stable and secure radio–frequency ("RF")[23] environment is a key component to any system deploying autonomous vehicles and more advanced systems such as V2V communications.[24] To provide "turn–by–turn" location information, transmit real–time data between vehicles to avoid collisions, and identify objects in the roadway, an AV can rely on a combination of

---

18 *Id.* (alterations added).

19 Burke, *supra* note 14.

20 Ryan Beene, *Self-Driving Car Industry Needs Better Metrics, DOT Official Says*, BLOOMBERG, https://www.bloomberg.com/news/articles/2018-10-23/self-driving-car-industry-needs-better-metrics-dot-s-kan-says (last visited Oct. 24, 2018) (alterations added).

21 *See* Robert B. Kelly & Mark D. Johnson, Symposium, *Defining a Stable, Protected and Secure Spectrum Environment For Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1271 (2012).

22 Ingrid Lunden, *Blue Vision Labs, Which Builds 'Collaborative' AR, Emerges From Stealth With $14.5M Led By GV*, TECH CRUNCH, https://techcrunch.com/2018/03/15/blue-vision-labs-which-builds-collaborative-ar-emerges-from-stealth-with-14-5m-led-by-gv/ (last visited Oct. 24, 2018) (quotations omitted).

23 Kelly et al., *supra* note 21, at 1279 n.12 (Radio-frequency "[r]efers to the range of electromagnetic waveforms that carry radio signals . . . [a] 'frequency band' or 'spectrum band' are essentially used interchangeably and refer to the range of frequencies that a certain class of radio communications service operates within.").

24 *Id.* (alterations added).

wireless technologies operating on different spectrum bands.[25] Each band has distinct characteristics, procedural requirements and limitations.[26]

As a result, the success of AVs is contingent on the availability of a reliable spectrum and the spectrum's capacity to meet current and future use.[27] The United States Federal Communications Commission ("FCC") regulates spectrum allocation usage by the private sector and local governments.[28] Alternatively, the National Telecommunications and Information Administration of the United States Department of Commerce ("NTIA") regulates usage by the federal government.[29]

Existing production vehicles are currently assembled with a myriad of wireless communications applications such as GPS, telematics, cellular, land–mobile and Bluetooth.[30] Autonomous vehicles depend on GPS because of its ability to provide accurate location, navigation, and tracking information,[31] which is critical to the viability of an AV's ability to provide real–time, dynamic location and mapping information.[32] Current prototypes for autonomous vehicles have a vehicle radar that identifies and tracks the presence and movement of obstacles, including nearby vehicles.[33] Autonomous vehicles may also be equipped with dedicated short–range communications ("DSRC"), which acts as a short–range wireless service that enables the "wireless link" to the V2V infrastructure.[34]

This technological landscape gives rise to pressing vulnerabilities: the government could easily track the movement of any person in an autonomous vehicle and invade their individual privacy, which calls for federal and state regulators to amend or create laws in order to fill the gaps between AV technology and the Fourth Amendment.

How Autonomous is "Autonomous"?

There are two types of AV models—interconnected and self–contained autonomous vehicles—which can be distinguished in the way they operate.[35] Self–contained autonomous vehicles rely on information

---

25 *Id.* at 1273.

26 *Id.*

27 *Id.* (alterations added).

28 *Id.*

29 Kelly et. al, *supra* note 21, at 1273.

30 *Id.* (quotations omitted) (alterations added).

31 *See generally Global Positioning System,* WIKIPEDIA, https://en.wikipedia.org/wiki/Global_Positioning_System (last visited Jan. 22, 2018) (quotations omitted).

32 *See* Kelly et. al, *supra* note 21 (quotations omitted).

33 *See id.* at 1281. (quotations omitted).

34 *Id.* at 1281–83.

35 Dorothy J. Glancy, *Symposium Article: Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1176 (2012) ("Interconnected autonomous vehicles are characterized by participating in such a vehicular network over which they both send and receive data.

solely programmed into the vehicle.[36] Conversely, interconnected autonomous vehicles, are wirelessly connected to a communication network where it can be externally controlled.[37] A self–contained AV is a concept distinct from an interconnected AV (a vehicle that communicates with other vehicles or infrastructure).[38] An indistinguishable feature of all types of autonomous vehicles, however, is their nature of operation by replacing human drivers with AI systems.[39] Specifically, their reliance on internally facing sensors that collect and feed data on how a vehicle is operating distinguishes them from an interconnected AV.[40] These internally facing sensors have the ability to collect data from various operational parts of the vehicle.[41] For example, when a vehicle records internal sensor data, the vehicle is essentially recording an individual's personal information, including user location and driving behavior.[42] Notwithstanding the differences between the capabilities of a vehicle that uses sensor–based crash avoidance technologies as compared to V2V communications, both types of vehicles present similar legal issues given the Safety Act's broad definition of "motor vehicle equipment" and ability to share data through a variety of ways.[43]

An autonomous vehicle is defined by its level of autonomy. Accordingly, there are five levels to vehicle autonomy.[44] Level four, known as "high automation,"[45] is performance by an automated driving system of all aspects of the driving task, even if a human driver does not respond appropriately to a system request or warning for human intervention.[46] Similarly, level five—"full automation"—is where the

---

Self-contained autonomous vehicles do not participate in the network at all and therefore retain within the vehicle all of its internal and external data, as well as full control over the operation of the vehicle.").

36 *Id.*

37 *Id.*; *see also*, Jeffery K. Gurney, *Driving Into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles*, 5 WAKE FOREST J.L. & POL'Y 393, 399–400 (2015) (quotations omitted).

38 *See* Wood et al., *supra* note 10, at 1432.

39 *See id.*

40 *Id.* at 1487.

41 Glancy, *supra* note 35, at 1175 ("Internal sensors can also collect continuous data about vehicle status that is potentially useful to vehicle manufacturers, traffic engineers, insurance companies, and the like. When vehicle status and operation information [are] associated with an identifiable individual, the data becomes personal information.").

42 *See* Glancy, *supra* note 35, at 1175–76.

43 *See id.*

44 *Id.* at 1428–29.

45 *A Brief History of Autonomous Vehicle Technology*, WIRED, https://www.wired.com/brandlab/2016/03/a-brief-history-of-autonomous-vehicle-technology/ (last visited Nov. 16, 2018).

46 *Id.*

driving is fully performed by an automated driving system under all roadway and environmental conditions.[47] Level five "full automation" can also be managed by a human driver; however, unlike level four, human intervention is not needed.[48] Essentially, the vehicle replaces the driver and operates itself.

Moreover, connected vehicles derive certain advantages from the number of communication technologies that facilitate the vehicle's ability to wirelessly communicate with the driver, other cars on the road (V2V), roadside infrastructure (V2I), bikes, pedestrians or others (V2X). Relatedly, self–driving cars are expected to rely heavily on digital maps to orient themselves.[49] As with any digital map, these will need to be constantly updated to accurately detail real–time traffic changes, including accidents, construction, and the like.[50] Because the machine learning technology that enables autonomous vehicles remains dependent on data collection to improve, there are unpredictable privacy risks.

II. THE CHANGING NATURE OF THE CITIZEN AND STATE RELATIONSHIP

As currently applied, the Fourth Amendment legal framework does not address data trails from autonomous vehicles.[51] Developments in the vehicle industry are progressing at light speed to create advanced driver–assistance systems.[52] In fact, key industry players in the United States market—such as General Motors, Ford, Chrysler, Volkswagen, BMW, Honda, Nisan, Mercedes–Benz, and, of course, Telsa—are already in the process of developing self–driving technology.[53] The "SELF DRIVE Act" [54] ("Act") seems to have alleviated concerns that technology may outpace

---

47 *Id.*

48 *Id.*

49 Edelstein, *supra* note 4.

50 *Id.*

51 *See* Ferguson, *supra* note 5, at 553 (alterations added) (noting that the current legal framework does not provide an answer to the question of data trials from smart devices and argues that, despite "insights and arguments [that] can be drawn from precedent, real gaps remain.").

52 *See* Glenn McDonald, *Here's What You Need to Know About the Status of Autonomous Vehicles*, SEEKER, https://www.seeker.com/transport/heres-what-you-need-to-know-about-the-status-of-autonomous-vehicles (last visited Jan. 11, 2018) (quotations omitted).

53 *Id.*

54 H.R. 3388, (The bill defines "(1) 'a highly automated vehicle' as a motor vehicle, other than a commercial motor vehicle, that is equipped with an automated driving system; and (2) an 'automated driving system' as the hardware and software of a vehicle that are collectively capable of performing the entire dynamic driving task on a sustained basis, regardless of whether such system is limited to a specific operational design domain.").

the law in the realm of autonomous vehicles and aims to make several changes to federal law impacting autonomous vehicles. Relatedly, the National Conference of State Legislatures ("NCSL"), along with other state groups, issued letters as the bill made its way through the House. The bill included four main sections: expansion of federal preemption; updates to federal motor vehicle safety standards ("FMVSS"); exemptions from FMVSS; and a federal automated vehicles advisory council.[55] The Senate Commerce Committee also unveiled legislation regarding autonomous vehicles—"the American Vision for Safer Transportation Through Advancement of Revolutionary Technologies" ("AV START Act").[56] The AV START Act, although similar to the House passed SELF DRIVE Act, contains some significant differences.[57]

Under the "Federal Automated Vehicle Policy,"[58] a safety assessment letter to NHTSA identifies "privacy" as an area covered by the SELF DRIVE Act. More specific, to ensure that the policy has been followed, the DOT will request manufacturers and other entities to voluntarily provide reports detailing their compliance with the NHTSA's updated guidance.[59] This mandate is expected to require manufacturers and other entities to submit a safety assessment to NHTSA's Office of the Chief Counsel for each highly automated vehicle ("HAV")[60] system.[61] The policy renders manufacturers responsible for ensuring and protecting consumer privacy.[62] With the rise of competition, lawmakers hope the legislation will strike a balance between allowing technology and

---

55 *Autonomous Vehicles|Self-Driving Vehicles Enacted Legislation*, NCSL, http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx (last visited Oct. 25, 2018) (quotations omitted).

56 *Id.*

57 *Id.*

58 U.S. Dep't. of Transportation, *supra* note 3 (The purpose of the Federal Automated Vehicle Policy according to the Secretary Anthony Foxx of the U.S. Department of Transportation is to formally seek public comment on the Policy and "[t]o establish a foundation and framework upon which future Agency action will occur."); *see also*, Federal Motor Vehicle Safety Standards; V2V Communications, 82 Fed. Reg. 3854-01 (to be codified at 49 C.F.R. pt. 571) (The regulations proposed in January specify what type of information vehicles are required to share and the method for sharing that information).

59 *See id.* (alterations added).

60 *Id.* (A "highly automated vehicle" (HAV) represents the SAE International (SAE) definitions for levels of automation.)

61 *Id.* (alterations added).

62 *Id.* (Moreover, "[t]he Department and the Administration strongly believe[s] in protecting individuals' right to privacy." Given the available resources, such as, the White House Consumer Privacy Bill of Rights, the Federal Trade Commission's privacy guidance, and the alliance of Automobile Manufacturers and the Association of Global Automakers published Privacy Principles for Vehicle Technologies and Services, "HAV manufacturers and other entities, either individually or as an industry, should take steps to protect consumer privacy.").

permitting car companies to conduct tests and collect data to ensure driver safety.

A. Steering the Wheel: NHTSA's General Authority Over Motor Vehicle Safety[63]

In 1966, Congress enacted the National Traffic and Motor Vehicle Safety Act (the "Safety Act") with the purpose of reducing deaths and injuries as a result of motor vehicle crashes and non–operational safety hazards.[64] To achieve this objective, the Safety Act authorizes NHTSA to "[s]et motor vehicle safety standards for new motor vehicles and motor vehicle equipment and requires the recall and remedy of vehicles and equipment that do not comply with the standards in place at the time of manufacture."[65] The Safety Act mandates that the standards issued by NHTSA be "[p]racticable, meet the need for motor vehicle safety and stated in objective terms."[66] Notwithstanding NHTSA's seemingly broad authority, the agency does not have the power to regulate the actions of vehicle owners, the operation of motor vehicles on public roads, or the maintenance or repair of vehicles in use.[67] However, as previously mentioned, NHTSA has the ability to regulate autonomous vehicles because of its broad statutory authority over motor vehicles and motor vehicle equipment.[68] Ultimately, as motor vehicle control systems become increasingly automated, NHTSA will continue to have regulatory authority over all systems, parts and components installed on new motor vehicles under the Safety Act.[69]

---

63 Wood et al., *supra* note 10.

64 *Id.* at 1435 n.30.

65 *Id.*; *see generally*, 49 U.S.C. § 30111(a) (2006).

66 *Id.* (quotations omitted) (citations omitted).

67 *Id.* (alterations added).

68 Wood et al., *supra* note 10, at 1441 (asserting that the broad construction of the statutory term "motor vehicle equipment" "[d]oes not depend on the type of technology or its mode of control (mechanical or electronic) or whether an item is tangible or intangible.").

69 *Id.*

B. Don't Get Too Ahead of Yourself: The Self–Driving Bubble is Nowhere Near Bursting[70]

During the week of January 9, 2018, auto manufacturers gathered at the CES tech conference ("CES")[71] and revealed their plans to produce the first true self–driving cars by 2021.[72] For example, Ford announced its plan to initiate a fleet of self–driving cars and sell those vehicles to service businesses, but no one should expect to see a self–driving car on any dealership lots in 2021.[73] Ford's business model differs from an automaker's traditional business model, however.[74] Companies such as BMW, who adhere to the traditional business model, will continue to sell cars directly to consumers and simultaneously sell "transportation as a service," meaning consumers would have the ability to rent "[f]ree–floating cars, hail a car with a driver," or perhaps "[o]rder a car without a driver."[75]

Despite the apparent global movement towards transportation as a service, (i.e. consumers would no longer purchase cars and would only purchase Uber rides or Zipcar rentals or the like) a looming difficulty remains in striking a balance between letting the industry guide regulation and allowing regulation dictate what the industry decides to build.[76] As seen in November 2017, the Trump administration began amending the framework for self–driving cars that was first issued by the Obama administration.[77] The proposal put forth by the Obama administration in

---

70 Doug Newcomb, *The Self-Driving Bubble Is Nowhere Near Bursting*, PC MAGAZINE (Dec. 30, 2017), https://www.pcmag.com/news/358201/the-self-driving-bubble-is-nowhere-near-bursting?source=google-editors-picks.

71 *See The Global Stage for Innovation*, CES, https://www.ces.tech (last visited Jan. 12, 2018) (describing the CES tech conference as "[t]he world's gathering place for all those who thrive on the business of consumer technologies [and] has served as the proving ground for innovators and breakthrough technologies for 50 years.").

72 *See* JC Reindl, *First True Autonomous Cars Won't Be For Sale*, DET. FREE PRESS, https://www.freep.com/story/money/cars/2018/01/11/first-true-autonomous-cars-wont-sale/1021656001/.

73 *Id.* (Sherif Marakby, Ford's vice president for autonomous vehicles and electrification commenting that the first truly autonomous Ford would not be available for consumers to buy).

74 *See id.*

75 *See* S. Somasegar, *Business Models Will Drive the Future Vehicles*, TECH CRUNCH (Aug. 25, 2017), https://techcrunch.com/2017/08/25/business-models-will-drive-the-future-of-autonomous-vehicles/.

76 *Id.*

77 Melanie Zanona, *Trump Administration Working to Update Driverless Vehicle Guidance*, THE HILL (Nov. 11, 2017), http://thehill.com/policy/transportation/358482-trump-administration-working-to-update-driverless-vehicle-guidance (last visited Jan. 9, 2018) (alteration maintained).

December 2016 would have required all new cars and light trucks be equipped, by 2023, with technology that facilitates communication and exchange data—such as a vehicle's location, speed, and direction—between vehicles up to ten times per second.[78] As a result of the loosening of standards by the Trump administration, however, V2V communication between vehicles has transitioned from being the centerpiece in the future of transportation to a mere secondary safety measure.[79]

In support, Elaine Chao, Secretary of the DOT, announced that the Trump administration would offer incentives, rather than public dollars, to private companies that are developing the next wave of transportation technology at CES in January 2018.[80] More importantly, just before Chao's speech, DOT's website began soliciting public comment on how to remove regulatory barriers and integrate automated vehicles into the national highway system.[81] The DOT vowed to continue their commitment to forward the new era of transportation and safety and solicited support from the technology and transportation industry, including state and local governments and other key stakeholders as they consider and design practices relative to the testing and deployment of automated vehicle technology.[82]

NHTSA's policy and guidance for automated vehicles continues to evolve. In October 2018, NHTSA published its third iteration of its policy and guidance ("Vision for Safety 3.0") and its primary focus is the safe performance of automated vehicles. The second version sought to clarify federal and state roles in autonomous vehicle rulemaking and veered away from the concept of safety oversight, focusing more on the promotion of AVs.[83] In guidance 3.0, NHTSA described its future role and the ability

---

78 Colin Wood, *Trump Administration Expected to Nix Vehicle-to-Vehicle Communications Mandate*, STATE SCOOP (Nov. 2, 2017), http://statescoop.com/pushing-for-autonomous-trump-may-abandon-of-vehicle-to-vehicle-mandate (last visited Jan. 9, 2018).

79 *Id.* (Commentators in support of moving away from V2V communication technology, such as the Competitive Enterprise Institute, praised the Trump administration's initiative, noting the Obama administration's rule "[w]ould have imposed large public infrastructure costs, in addition to the substantial costs on every American who purchased a new automobile.") (alteration maintained).

80 *See* Art Marroquin, *Trump Infrastructure Plan to Include Shift Toward Driverless Vehicles*, L. V. REV. J. (Jan. 10, 2018), https://www.reviewjournal.com/business/trump-infrastructure-plan-to-include-shift-toward-driverless-vehicles/.

81 *See id.* (quotations omitted); *see generally*, *USDOT Automated Vehicles*, U.S. D'PT OF TRANS., https://www.transportation.gov/AV (last visited Jan. 12, 2018) (commenting that "[t]he Department of Transportation is committed to facilitating a new era of transportation innovation and safety ensuring that our country remains a leader in automation.").

82 *See id.*

83 Zanona, *supra* note 77 (alteration maintained).

for manufacturers to obtain waivers of compliance with existing safety standards, as related to automated vehicles without steering wheels and foot pedals, which cannot meet existing standards. The most alarming modification under guidance 2.0, and sustained in guidance 3.0, concerns the removal of the suggestion that obligated automakers to consider ethical and privacy issues.[84] As a result, auto manufacturers, rather than lawmakers, retain control of the future of autonomous vehicles,[85] and NHTSA has taken on the role of promoting and facilitating the deployment of AVs no matter the cost.

The auto industry may be ready, but are we?[86] Nixing the requirement for automakers to consider ethical and privacy issues is troublesome, especially when security researchers have repeatedly demonstrated how easy it is to wirelessly hijack a car's electronic instrumentalities.[87] Because of the software's level of complexity, the degree of injury to an individual is unquantifiable.[88] Clifford Neuman, director of the Center for Computer Systems Security at USC Viterbi, urges developers of these systems to "[p]rovide much more attention to their software architecture to ensure that basic safety constraints are embedded deep in the system and cannot be subverted."[89]

The question here is not what but who. Who would have the ability to cause irreparable harm to the driver or passengers of an autonomous vehicle by subverting the system? Does the government have the authority to use the information collected and stored by the system?

C. Government Piracy of Individual Privacy: Defining the Regulatory Framework for Autonomous Vehicles

Given that parties developing AV technologies and systems are at the will of the United States government and its regulatory agencies, parties must work through the complex welter of critical legal, policy and technical issues that affect the RF spectrum upon which their systems depend.[90] Defining a spectrum environment is contingent on the FCC's allocation to the private sector and state and local governments.[91] NTIA,

---

84 *Id.*

85 Ian Chaffee, *Driverless Cars Are Ready to Hit the Road – But Are We Ready for Driverless Cars?*, USC News (Jan. 1, 2018), https://news.usc.edu/134264/driverless-cars-are-ready-to-hit-the-road-but-are-we-ready-for-driverless-cars/.

86 *Id.*

87 *See id.*

88 *Id.*

89 *See id.*

90 *See* Kelly, *supra* note 21, at 1272 ("This is true regardless of whether the autonomous vehicle operates with existing communications systems and networks.").

91 *See id* at 1273.

on the other hand, oversees the spectrum allocation for use by the federal government.[92] An autonomous vehicle has the ability to rely on a combination of multiple wireless technologies (each of which uses different spectrum bands and operates with distinct technical characteristics, procedural requirements, and limitations).[93]

But how could the FCC not anticipate a significant growth in voice and data usage as a result of current trends in wireless usage after it repealed the network neutrality rules in 2017. The repeal would essentially allow for wireless internet service providers ("ISPs") to offer customized content and media packages but also give preferential treatment to certain websites or block others.[94] All of this creates an exigence on governments, regulators and commercial interests.[95] In fact, Comcast informed the FCC prior to the repeal that network neutrality laws should be repealed to accommodate for high–speed data in autonomous vehicles.[96] Regulators must therefore adopt policies, rules, and technologies that capitalize on the instrumentalities in the already available spectrum to accommodate the increasing demand of autonomous vehicles by devising a new spectrum.[97]

Given the current trend of autonomous vehicle technology, there will be need for a new spectrum allocation to accommodate autonomous vehicle technology.[98] In support, on October 23, 2018, the FCC proposed to expand the available unlicensed spectrum for Wi–Fi communications into the 6 GHz band (5.925–7.125 GHz).[99] The Internet and Television Association asked the Commission to adopt a Notice of Proposed Rulemaking, which would reform current rules that give 5.9 preference to automotive–industry applications and broadening the range of low–power, unlicensed transmissions allowed in the band.[100] The FCC's proposed rules will allow a "[s]pectrum resource to be more intensively used to benefit consumers while allowing the existing licensed uses of the 6 GHz

---

92 Kelly, *supra* note 21, at 1273.

93 *Id.*

94 Cecilia King, *F.C.C. Repeals Net Neutrality Rules*, N.Y. TIMES (Dec. 14, 2017), https://www.nytimes.com/2017/12/14/technology/net-neutrality-repeal-vote.html.

95 Kelly, *supra* note 21, at 1285.

96 King, *supra* note 94.

97 *Id.*

98 Kelly, *supra* note 21, at 1287 (noting and cautioning that if such a need were to arise as autonomous vehicle technology matures and is introduced into commercial markets, "proponents of such an allocation must consider the often lengthy, contentious, and costly allocation process in their planning.").

99 Randy Sukow, *NCTA Call for 5.9 GHz Unlicensed Spectrum Meets Positive FCC Reaction*, NRTC (Oct. 17, 2018), https://www.nrtc.coop/rural-connect/ncta-call-for-5.9-ghz-unlicensed-spectrum-meets-positive-fcc-reaction.

100 *Id.* (quotations omitted).

band to continue uninterrupted."[101] As unlicensed devices that employ Wi–Fi and other unlicensed standards have become indispensable for providing low–cost wireless connectivity as related to autonomous vehicles, it is clear that any shared spectrum environment presents instances of harmful interference by obtaining the location and operation of each autonomous vehicle's service transmitter.[102] The preservation of individual autonomy and absolute privacy will inevitably clash with opposing political forces and the government's law enforcement function.[103] For one thing, the age of autonomous vehicles will usher in sweeping changes, transforming life as we know it.[104] But who is to keep the government and regulatory agencies from lawless invasions of an individual's constitutional rights through unhindered government use of data collected from an AV's service transmitter?

III. HIDDEN DANGERS OF AUTONOMOUS VEHICLES

Privacy interests are inescapably intertwined with the use of autonomous vehicles. With people as the intended users and purchasers of autonomous vehicles, privacy interests will be affected by their increased use. Autonomous vehicles give rise to several types of privacy interests, including (1) technical issues where the sources and modes of attack are unknown, unpredictable, and likely to be ever–changing;[105] (2) legal and practical issues regarding protection from unauthorized intrusions into autonomous driving systems;[106] and (3) data and location privacy.[107] Personal data imported or derived from a vehicle, a user, or the interactions between a user in a vehicle could facilitate the denigration of all individual privacy. Perhaps most significant is the capacity for V2V technology to distribute personal information to other vehicles, municipal signal towers, infrastructure objects such as traffic signs and stoplights, buildings and billboards, and other unmanifested possibilities.[108]

---

101 Action by the Commission October 23, 2018 by Notice of Proposed Rulemaking (FCC 18-147).

102 *See* Kelly, *supra* note 21, at 1313.

103 *See* Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189, 189 (1996).

104 Omri Barzilay, *The Road to the Autonomous Age Will Be Paved by Smart Cities*, FORBES (Jan. 24, 2018, 7:00 AM), https://www.forbes.com/sites/omribarzilay/2018/01/24/the-road-to-the-autonomous-age-will-be-paved-by-smart-cities/#7965bf6168c3.

105 Wood et al., *supra* note 10, at 1467.

106 *Id.* at 1468.

107 *Id.* at 1471.

108 *See* Bryan Clark, *How Self-Driving Cars Work: The Nuts and Bolts Behind Google's Autonomous Car Program*, MAKEUSEOF (Feb. 21, 2015), https://www.makeuseof.com/tag/how-self-driving-cars-work-the-nuts-and-bolts-behind-googles-autonomous-car-

A. Autonomous Vehicles Increasing Vulnerability

Access to electronic communications and files have become the cornerstone to many criminal investigations. The use of computers and cell phones in the aid of criminal activity has expanded in recent years, raising many Fourth Amendment questions.[109] The legislature has played a significant role in establishing the procedures through which law enforcement may investigate a crime. However, relying on the legislature to regulate communication networks and criminal investigations involving digital records does not necessarily mean the Fourth Amendment will provide protection. What happens if there isn't a statute to fill the void? Without judicial interference, there may be nothing to limit the volume or substance of information the government could gather.

In the last few decades, the Supreme Court has endeavored to craft an expansive view of digital communications and Fourth Amendment individual privacy protections. Electronically stored information is more susceptible to abuse because of its ability to be stored for an infinite amount of time.[110] More specific, all communications will inevitably be recorded because of the difficulty associated with tapping into a communication without compromising other communications that are being transmitted across the same fiber optic line.[111]

It is no new phenomenon that the government has the means to monitor Americans' online activity. What information can we reasonably expect to remain private under the Fourth Amendment if we store and access more information online from autonomous vehicles?

What Type Information is Being Collected?

In the background of self–driving vehicles' capability "to drastically reduce accidents, travel time, the environmental impact of road travel," and their profound impact on labor demand,[112] is a particular concern

---

program/ (explaining that Google's autonomous vehicle software "processes . . . data in real-time [and] model[s] dynamics of other drivers, pedestrians, and objects.").

109 *See* United States v. Jones, 565 U.S. 400, 427, 429–30 (2012) (Alito, J., concurring) ("[T]he *Katz* test rests on the assumption that [the] hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes . . . .In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. (citation omitted) A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.").

110 Singhal, *supra* note 103, at 191.

111 *Id.*

112 David Beede et al., *The Employment Impact of Autonomous Vehicles*, ECON. & STAT. ADMIN. 1, 1 (Aug. 11, 2017), http://www.esa.doc.gov/sites/default/files/Employment%20Impact%20Autonomous%20Vehicles_0.pdf ("In 2015, 15.5 million U.S.

regarding data privacy and security risks.[113] To date, seventeen states have enacted statutes related to data privacy issues of data retrieval from an event data recorder, ("EDR") which serves as a "black box" for recording critical sensor and diagnostic data prior to collisions.[114] For example, an EDR can record an occupant's information in the seconds before, during, and after a vehicular collision.[115] These microcomputer chip sets also have the ability to capture much more than just vehicle collisions, depending on the auto manufacturer.[116] Despite NHTSA's failed mandate that would have required EDR implementation in every new vehicle, as of September 2014 most new vehicles include an EDR.[117] This, in part, is a result of states passing laws imposing standards that specify what auto manufacturers must disclose, who can access EDR information, and when they can access it.[118] According to the NCSL, states that have enacted statutes relating to data retrieval have included a provision that the data collected from a motor vehicle EDR may be downloaded only with the consent of the vehicle owner or policyholder, with certain "exceptions."[119] The statutes, however, make clear that the intent is to allocate ownership to the physical embodiment of data on tangible EDR devices, not create property rights to the information content itself.

The *exceptions* raise serious questions as to whether a company would be required to grant law enforcement access to driver behavior information.[120] More importantly, who owns the driver behavior information—the driver or the company—and what are their respective

---

workers were employed in occupations that could be affected (to varying degrees) by the introduction of automated vehicles.").

113 Christopher Achatz & Ashlee Difuntorum, *Data Privacy Issues of Self-Driving Vehicles*, BRYAN CAVE (July 17, 2017), https://www.bryancave.com/en/thought-leadership/data-privacy-issues-of-self-driving-vehicles.html.

114 *Id.*

115 *Event Data Recorder*, NHTSA, https://www.nhtsa.gov/research-data/event-data-recorder (last visited Jan. 10, 2018) ("For instance, EDRs may record (1) pre-crash vehicle dynamics and system status, (2) driver inputs, (3) vehicle crash signature, (4) restraint usage/deployment status, and (5) post-crash data such as the activation of an automatic collision notification (ACN) system.").

116 Michelle V. Rafter, *Decoding What's in Your Car's Black Box*, EDMUNDS (Jul. 22, 2014), https://www.edmunds.com/car-technology/car-black-box-recorders-capture-crash-data.html.

117 *See id.* (explaining that "96 percent of new cars sold in the United States" have EDRs); *see also* Russ Heaps, *Data Collection for Self-Driving Cars Could be Risking Your Privacy*, AUTOTRADER (Sept. 2016), https://www.autotrader.com/car-shopping/data-collection-for-self-driving-cars-could-be-risking-your-privacy-257144 (explaining that event data recorders have been installed in every new car since 2014).

118 *See* Rafter, *supra* note 116.

119 *Event Data Recorder*, *supra* note 115.

120 Achatz & Difuntorum, *supra* note 113.

rights to its usage?[121] Perhaps the most perplexing question of all—who are the entities watching, monitoring and recording our behavior by collecting this information?—has an even more troublesome answer: anyone.[122] Namely, anyone with a stake to anything with respect to the vehicle.[123]

Is the Problem Collection or Use of the Information Obtained?

Many states' statutes related to the black box require automakers to notify new car buyers that their vehicle contains such.[124] However, disclosure of the black box may be by directing the vehicle owner to the owner's manual.[125] Some states have also enacted laws that explicitly detail the circumstances where auto manufacturers are to disclose data contained in an EDR to law enforcement officials or third parties *without* the owner's consent.[126] But what happens when a state has failed to enact laws to protect a vehicle owner from an unreasonable search and seizure of an EDR by a police officer or third party?[127] Put simply, if they want it, there's nobody saying they can't have it.[128]

Notwithstanding NSCL's enactment of the 1994 federal Driver Protection Privacy Act ("DPPA"),[129] which places limitations on data retrieval from EDRs and establishes that any information collected belongs to the vehicle owner or lessee of the vehicle, information collected by an EDR arguably continues to subject an individual to unreasonable searches and seizures. More specific, the DPPA protects personal information that identifies an individual, including an individual's photograph, Social Security number, driver information number, name, and address, but not the five digit zip code, telephone number, and some medical information.[130] Thus, the DPPA generally prohibits the Department of Motor Vehicles and authorized recipients from knowingly disclosing an individual's personal information.[131]

---

121 *Id.*

122 Heaps, *supra* note 117.

123 *Id.*

124 *See* Rafter, *supra* note 116.

125 *Id.*

126 *Id.*

127 See *id.*

128 *Id.*

129 18 U.S.C. § 2721 (2012) ("A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information . . . about any individual obtained by the department in connection with a motor vehicle record.").

130 *Know About Driver's Privacy Protection Act*, OHIO BAR, https://www.ohiobar.org/ForPublic/Resources/LawYouCanUse/Pages/LawYouCanUse-461.aspx (last visited Jan. 11, 2018).

131 *Id.*; *see generally* 18 U.S.C. § 2725(3) (2012) (defining "personal information").

Despite the DPPA's general prohibition, it's riddled with 14 exceptions and, arguably, the most concerning exception allows for law enforcement agencies to obtain an individual's information relevant to their work.[132] Assuming the data collected can be used against a driver in a legal proceeding, it must be determined what specific information is at issue.

B. Autonomous Vehicles: The Search of Digital Information

Legislation has undoubtedly played a more significant role in setting out the procedures by which law enforcement may investigate a crime.[133] At the same time, however, there can be disadvantages to strictly relying on legislatures, as opposed to courts, to act as the sole decision maker in determining the role in the articulation of the rules that are to regulate criminal investigations involving autonomous vehicles.[134] More specific, these disadvantages may be greater in investigations concerning communication networks and digital records contained in an autonomous vehicle's EDR.[135] Justice Sotomayor, in *United States v. Jones*, observed that "[i]t may be necessary to reconsider the premise that an individual has no reasonable expectation to privacy in information voluntarily disclosed to third parties" as "[i]ll suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[136] Justice Sotomayor's reasoning in *Jones*, that a Fourth Amendment search occurs whenever the government violates a subjective expectation of privacy that society recognizes as reasonable remains, which is of particular importance in the era of autonomous vehicle technology, where physical intrusion is unnecessary to many forms of surveillance.[137] Alternatively, what if the courts are not in the best position to assess and respond to violations related to privacy protection

---

132 *See id.* § 2721(b); *see also Know About Driver's Privacy Protection Act*, *supra* note 130 (highlighting a number of unsettling exceptions to the DPPA, including the ability of insurance companies to "obtain [personal] information to investigate claims"; the disclosing of personal information to "verify a person's identity under certain circumstances"; and the ability of attorneys to obtain personal information "for use in a lawsuit").

133 ALLEN ET AL., CRIMINAL PROCEDURE: INVESTIGATION AND RIGHT TO COUNSEL, 754 (3d ed. 2016).

134 *Id.* at 755.

135 *Id.*

136 *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring); *see also* ALLEN ET AL., *supra* note 133 at 755.

137 *See Jones*, 132 S. Ct. at 954–55 (Sotomayor, J., concurring) (alterations added).

in an autonomous vehicle?[138] Perhaps the legislature, as it is elected by the people, may be in a better position to respond to these technological changes.[139]

IV. THE HEART OF THE FOURTH AMENDMENT AND AUTONOMOUS VEHICLES

A. The Fourth Amendment: The Linchpin of Constitutional Protection

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[140] "No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law."[141] It provides protection against government interference. Thus, the inquiry in each case should examine the essence of what the Fourth Amendment seeks to protect: the individual's right to be secure from an unreasonable search and seizure.

Is There Enough Left of Boyd?

In *Boyd v. United States*,[142] the Fourth Amendment undoubtedly applied to the papers at issue. In *Boyd*, the Supreme Court held that the Fourth and Fifth Amendments created a zone of privacy with respect to an individual's person and property.[143] The *Boyd* Court concluded that the Fourth Amendment protects against the invasion into a person's private matters by prohibiting the government from compelling a person to produce private papers though a subpoena.[144] *Boyd*, in essence, created the principle that the Fourth Amendment protects privacy through the unreasonable searches and seizures clause.[145]

---

138 *See* Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring in part and concurring in the judgment).

139 *Id.* at 2497–98 (quotations omitted).

140 U.S. CONST. amend. IV.

141 Terry v. Ohio, 392 U.S. 1, 9 (1968).

142 *See* 116 U.S. 616, 623 (1886).

143 *See id.* at. 630; *See also The Life and Times of Boyd v. United States*, 76 MICH. L. REV. 184 (1977) ("The government, according to Boyd, cannot enter this zone, either by compelling an individual to testify against himself or by subpoenaing or seizing his books and papers for use as evidence against him in criminal or quasi-criminal proceeding.").

144 *Boyd*, 116 U.S. at 630.

145 *See id.*; *See also The Life and Times of Boyd v. United States*, *supra* note 143, at 190 (commenting "[i]n this roundabout way, the fourth amendment in fact became the protector of privacy.").

In the decades that followed, the Supreme Court retreated from defining an unreasonable search in terms of a property interest.[146] The extent of this retreat, as reflected in the decisions following *Boyd*, reduced obstacles to governmental seizure of an individual's property, which, in effect, narrowed his zone of privacy.[147] In light of these decisions, "no zone of privacy now exists that the government cannot enter to take an individual's property for the purpose of obtaining incriminating information."[148] Despite the evisceration of the *Boyd* privacy principle, the Court has refused to overrule it.[149]

The death of *Boyd* raises a pressing concern for drivers of autonomous vehicles, namely, what does *Boyd* mean with respect to the privacy of the driver? More important, how can autonomous driving systems protect the information received, generated and sent by autonomous vehicles, and ensure that information may freely move without being tracked?[150] The increased prevalence of autonomous vehicles and their electronic components undeniably leads to unique challenges regarding the security of vehicle systems.[151] Privacy concerns are not limited to autonomous driving systems and the system's security functions;[152] privacy interests are also raised when the Federal Motor Vehicle Safety Standards ("FMVSS") enacts safety regulations for the purpose of avoiding crashes.[153] For example, when the FMVSS requires crash avoiding technology to be implemented into the autonomous system, it "[will] involve the potential for more sophisticated measuring (and potentially

---

146 *See The Life and Times of Boyd v. United States*, *supra* note 143, at 193.

147 *See generally* Ferguson*, supra* note 5 (quotations omitted); *see*, e.g., Katz v. United States, 389 U.S. 347, 366 (1967) (where Justice Black refused to extend Fourth Amendment protections to eavesdropping:

[I]f they [the framers of the Constitution] had desired to outlaw or restrict the use of eavesdropping, I believe that they would have used the appropriate language to do so in the Fourth Amendment. They certainly would not have left such a task to the ingenuity of language-stretching judges.).

148 *Q&A with Self-Driving Car Pioneer Chris Urmson*, *supra* note 16 at 211 ("In most cases, the zone can be entered by the issuance of a subpoena; in the rest, it can be breached by a search warrant.").

149 *Id.*

150 *See* Wood et al., *supra* note 10, at 1448 (alterations added).

151 *Id*. at 1465-66 (quotations omitted)

("This increased permeation of electronic components into the motor vehicle could expose the vehicle to new safety issues if persons can gain access to these electronic components and can manipulate how these components issue commands or otherwise interact with the vehicle. Through the increased use of wireless connections (whether as a medium for V2V safety communications or for other, non-safety related purposes), it is widely demonstrated that it is possible to obtain unauthorized access to a vehicle's systems without physical access to the vehicle.").

152 *See id*. at 1472.

153 *Id*.

recording) of safety relevant information regarding the driver's behavior[,]" such as, direction and speed.[154] Some commentators opine that the agency may provide the most comprehensive protection against potential security issues.[155] But allowing NHTSA to exercise its authority over unwanted intrusions into a vehicle's electronic system by external sources is essentially playing into the government's hand.

Data and Reasonable Expectation of Privacy

The Fourth Amendment applies to a government searches and seizures.[156] In response to the shift from *Boyd* to the trespass doctrine, the Court created some anomalous rulings, finding a "microphone" placed on a wall to eavesdrop on an adjoining room was not a search because there was no physical intrusion of a protected space,[157] but, alternatively, found a "spike mike" that scarcely pierced an adjoining wall to encapsulate the same conversation would have constituted a search.[158] In response to the criticisms of the limited reading of the trespass doctrine (which undoubtedly failed to capture technological advancements that would soon invade an individuals' privacy without physically intruding in a constitutionally protected space) Justice Harlan's concurrence in *Katz v. United States* established the test known as the "reasonable expectation of privacy." Reasonable expectation of privacy turns on whether an individual has a subjective expectation of privacy that society deems objectively reasonable.[159]

The *Katz* Court found that a conversation picked up by a microphone taped to a public telephone booth was a search despite the lack of a physical invasion into the phone booth.[160] The majority reasoned that Fourth Amendment protects "people, not places."[161] Since the Court's

---

154 *Id.* at 1472 (alterations added).

155 *See id.* at 1468
(noting "[C]oordinated action by NHTSA and other entities (such as state governments) might provide the most comprehensive protection. In their article discussing the security of vehicle electronic systems, [the authors] opine that the priority areas for action in the immediate future should be ensuring that external sources of information for vehicle are authenticated and that interfaces that are exposed to those external sources are properly guarded against unwanted intrusions.").

156 *See* U.S. CONST. AMEND. IV.

157 *See* Ferguson, *supra* note 5, at 570 n.122 (citing Goldman v. United States, 316 U.S. 129, 135 (1942).

158 *Id.* at 570 n.123 (citing Silverman v. United States, 365 U.S. 505, 509-12 (1961)) (alterations added).

159 *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

160 *See* Ferguson, *supra* note 5, at 570–71 (alterations added) (citations omitted).

161 *Katz*, 389 U.S. at 351.

decision in *Katz*, the reasonable expectation of privacy analysis governs the threshold question of whether a Fourth Amendment search and seizure has occurred.[162] Generally, if an individual has a reasonable expectation of privacy, a search warrant must be obtained to constitute a lawful search.[163] Over time, the Court has allowed for case–specific exemptions to the warrant requirement, including the well–established vehicle exception.[164] Fourth Amendment principles, such as the search incident to arrest exception and the doctrine governing the search of a closed container, can also be relevant to the vehicle exception inquiry. An autonomous vehicle's mobility, therefore, is not necessarily dependent on the decisions made by an individual occupying it. In other words, the fact an AV can drive itself would not render the automobile exception inapplicable. Thus, the mobility threshold is arguably moot.

The question remains, however, whether a reasonable expectation of privacy exists in an object, area, or thing.[165] Admittedly, the data stored in an autonomous vehicle's system, although not incriminating in itself, may lead law enforcement to develop suspicion.[166]

The reasonable expectation of privacy test singularly controlled Fourth Amendment questions of whether there had been a search until the *United States v. Jones* decision.[167] The Court's decision in *Jones* represents the gradual retreat from *Katz* and the traditional "reasonable expectation of privacy." After *Jones*, courts faced with Fourth Amendment questions about locational data or other information analyze whether a search occurred under both the "reclaimed" physical intrusion theory and the reasonable expectation of privacy theory.[168] The Court's decision in *Riley v. California*,[169] only adds to the uncertainty of which theory is to govern technological cases, especially when faced with the question of AVs.

Would a police officer need a warrant to search a smartphone incident to arrest?[170] The Court answered in the negative in *Riley*, which was the Court's first attempt to reconcile the Fourth Amendment and smartphone

---

162 *See* Ferguson, *supra* note 5 at 571 (alterations added).

163 Singhal, *supra* note 103, at 196 (quotations omitted).

164 *See* Arizona v. Gant, 556 U.S. 332 (2009).

165 *See* Ferguson, *supra* note 5, at 571 (quotations omitted); *see, e.g.,* Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 583 (1990) ("If the fourth amendment was intended to promote a sense of personal security, it must extend to the protection of informational privacy.").

166 *See* Ferguson, *supra* note 5, at 562 (quotations omitted).

167 Ferguson, *supra* note 5, at 571–72 (alterations added) (quotations omitted).

168 *Id.* at 573 (alterations added) (quotations omitted).

169 Riley v. California, 134 S. Ct. 2473, 2484 (2014).

170 *Jones*, 132 S. Ct. at 945–47.

data.[171] In *Riley*, the Court found that smartphone data was quantitatively and qualitatively different from searching a cigarette pack or even a wallet or address book recovered from an arrested suspect, and the police did not need a warrant before searching the smartphone data.[172]

The Court made several relevant statements as to how the Fourth Amendment might conceptualize data trials arising from AVs. The Court reasoned that data distorts the traditional application of legal precedent based on physical objects because ordinary physical constraints and physical limitations fall away in a digital world.[173] And it further recognized the threat digital technology poses to invade "the privacies of life,"[174] as actions, thoughts, and patterns become reflected in digital form.[175] Despite the Court's recognition in *Riley* of a need to restructure the Fourth Amendment to extend its protections to digital technology, the decision provided an incomplete answer. *Riley* began reimaging a digital Fourth Amendment, but it provided an incomplete picture.[176]

Government Interception of Communications, Title III, and Reasonable Expectation of Privacy

Title III was enacted in the wake of the Supreme Court's decision in *Katz*.[177] Title III regulates the "nonconsensual" interception of any wire, oral, or electronic communications through use of any electronic, mechanical, or other device of the contents.[178] The statute sets out to accomplish at least four things:

> First, in permitting investigators to obtain court authorization to wiretap or eavesdrop[,] [Congress] sought to provide law enforcement officials with a much–needed weapon in their fight against crime, particularly organized crime. Second, it sought to safeguard the privacy of . . . communications. Third, Congress endeavored to satisfy the procedural and substantive requirements previously enunciated by the . . . Supreme Court in *Berger* and *Katz* as constitutional prerequisites to lawful court–authorized interception of private

---

171 *See* Ferguson, *supra* note 5, at 573 (alterations added).

172 *Riley*, 134 S. Ct. at 2489.

173 *Id.* at 2489 ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.").

174 *Id.* at 2495 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

175 *Riley*, 134 S. Ct. at 2490.

176 Ferguson, *supra* note 5, at 575 (quotations omitted).

177 *Katz*, 389 U.S. at 348.

178 18 U.S.C. §2510(4) (2012).

> communications. Finally, it attempted to define on a uniform basis the circumstances and conditions under which the interception of . . . communications may be authorized.[179]

Despite Title III's detailed legislative scheme, its procedural safeguards do not warrant comfort in its ability to protect an individual's Fourth Amendment rights. In fact, the procedural and substantive safeguards implemented by Congress in Title III are not constitutionally mandated and are not applicable to conventional search warrants.[180]

Title III contains a "minimization" requirement that addresses the reality of law enforcement agents executing an intercept order to gain access to communications that are unrelated to the crimes under investigation.[181] In *United States v. New York Telephone Company*,[182] the Supreme Court relied on Title III's legislative history and statutory language in establishing the definition of "intercept" under Title III.

The "third party doctrine" creates additional problems for the Fourth Amendment.[183] As currently understood, communications provided to a third party (e.g., a phone company, friend, or any of the companies providing devices in the Internet of Things) are not protected under the reasonable expectation of privacy theory.[184] These communications fall outside of a reasonable expectation of privacy because the act of giving the information to another prohibits the giver from claiming privacy over the information.[185] A broad reading of the third party doctrine undermines Fourth Amendment protection because data stored in an autonomous vehicle's software will be held by another entity as well as the owner.[186]

As such, if there is no Fourth Amendment protection for the data trails that an autonomous vehicle creates, law enforcement officials would be

---

179 *Id.* (citations omitted).

180 Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,* 102 MICH. L. REV. 801, 855 (2004) (As Professor Kerr accurately observed, in the wake of Title III's enactment, "wiretapping law remained 'constitutional in theory' but [became] statutory in practice.").

181 *See* 18 U.S.C. § 2518(5) (2012) (dictating Title III requires that surveillance "be conducted in such a way to minimize the interception of communications not otherwise subject to interception under this chapter . . . .").

182 *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 166–68 (1977) (distinguishing the definition of *intercept* from the operation of a *pen register*, which the Court characterized as "[decoding] outgoing telephone numbers by responding to changes in electrical voltage cause by the turning of the telephone dial and present[ing] the information in a form to be interpreted by sight rather than by hearing.").

183 Ferguson, *supra* note 5, at 575.

184 *Id.* (quotations omitted).

185 *Id.* at 575–76.

186 *Id.* at 576.

able to collect and use these data trails.[187] Contrarily, if the Fourth Amendment does protect data trials created by an autonomous vehicle, then the third party doctrine may facilitate a loop hole for law enforcement to obtain the same information indirectly (via the third party).[188] Thus, how can one trespass or physically intrude on data trials which have no physical being?[189] More specific, how does one define a threshold line for a reasonable expectation of privacy test around an intangible, instantaneous, mutable representation of digital code?[190]

The Act for Caution: The Stored Communications Act

The Stored Communications Act ("SCA")[191] was enacted in 1986 as part of the Electronic Communications Privacy Act ("EPCA")[192] and regulates government access to certain communications held by the providers of electronic communication services or remote computing services to the public.[193] The relevant provisions of the SCA apply to any temporary intermediate storage of the communication incidental to its electronic transmission to its final recipient or any associated backup of this communication by the server.[194] Significantly, the *Warshak* Court alluded to the fact that, under some yet–undefined set of circumstances, the mere content status of specific communications data may not be protected by the Fourth Amendment.[195]

The fundamental purpose of the Fourth Amendment "[i]s to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[196] However, not all government actions are invasive enough to implicate the Fourth Amendment.[197] The SCA allows law enforcement to compel stored content under the "reasonable suspicion

---

187 *Id.*
188 *Id.*
189 Ferguson, *supra* note 5, at 576.
190 *Id.*
191 18 U.S.C. §§ 2701–2711 (1986).
192 *Id.*
193 *Id.*
194 *Id.*
195 *See* Steven M. Bellovin et. al., *Its Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, HARV. J.L. & TECH., Fall 2016, at 24.
196 *See* Camara v. Mun. Ct. of San Francisco, 387 U.S. 523, 528 (1967); *see also* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 613-14 (1989) ("The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction.")
197 United States v. Warshak, 631 F.3d 266, 284 (2010).

standard,"[198] or even a mere relevance of showing.[199] The compelled disclosure of email content under standards lower than the Fourth Amendment "probable cause" standard has been found unconstitutional.[200] In *Warshak*, the Supreme Court held the government violated the defendant's Fourth Amendment rights by compelling his Internet Service Provider ("ISP") to turn over the contents of his emails.[201] But the government agents' reliance on the SCA was in good faith, so reversal was unwarranted.[202] The *Warshak* Court considered whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber's emails without triggering the machinery of the Fourth Amendment.[203] *Warshak* extends Fourth Amendment protections to communications' content when the service provider functions as a mere "intermediary" akin to the post office or a telephone company.[204]

Although the case law is not entirely settled, the provisions of the SCA that authorize the government to access email contents—absent a warrant—based on probable cause, is likely unconstitutional. But what about queries stored by a search engine made from your autonomous vehicle? Professor Kerr contends that, "although the issue is difficult and not free from doubt," the SCA likely offers no protection in this context because search engines "plainly do not provide [electronic computing services] as they are destinations for communications, not providers of connectivity or messaging."[205]

---

198 *See* 18 U.S.C. § 2703(d) (allowing law enforcement to compel communications content from ECPA-covered third parties via a court order finding that there are 'specific and articulable facts' that the information sought is "relevant and material to an ongoing criminal investigation").

199 *See* §2703(b)(B)(i) (allowing the use of an administrative, grand jury or trial subpoena to compel communications content from ECPA-covered third parties).

200 *Warshak*, 631 F.3d at 274.

201 *Id.*

202 *Id.* at 286 (Specifically, the court reasoned "[i]f we accept that the email is analogous to a letter or phone call, it manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As discussed above, the policy may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call – unless they get a warrant, that is.").

203 *Warshak*, 631 F.3d at 288.

204 *Id.* (emphasis omitted).

205 Orin Kerr, *The Next Generation Communication Privacy Act*, 162 U. PA. L. REV. 373, 396 (2014).

V. CONCLUSION

Autonomous vehicle technology will revolutionize the world as we know it. Equally important is the tension between existing case law, data collection by autonomous vehicles and the extent of protection under the Fourth Amendment. An AV's data trial warrants protection under the Fourth Amendment. Without a new theory to protect these data trials, an AV's data will be outside Fourth Amendment protection. As autonomous vehicle technology continues to develop, state and federal officials, manufacturers, and IT companies should bear in mind the implications beyond the advantages this type of technology will have on society. More important, autonomous vehicle users must be protected from unlawful invasions of privacy. Requiring a warrant to search the data of an AV is the first step at extending Fourth Amendment protections to the individual. The data must also be reconciled with the automobile exception, the third–party doctrine, and the SCA. The hope is Fourth Amendment can adapt to avoid being outpaced by the development of these new technologies.