Minnesota Journal of Law, Science & Technology

Volume 16 | Issue 2 Article 9

2015

Driving into the Digital Age: How SDVs Will Change the Law and Its Enforcement

Sarah Aue Palodichuk

Driving into the Digital Age: How SDVs Will Change the Law and Its Enforcement

Sarah Aue Palodichuk*

INTRODUCTION

As technological advances enable autonomous vehicles to merge onto public roadways, the effects of this change will be felt throughout daily lives, with great adaptations required in many aspects of society. Creating vehicles capable of driving themselves is only the beginning of a process that includes significant changes to our road infrastructure, psychological acceptance necessary to allow a computer to chauffer humans on their grocery runs, and financial freedom to afford such a vehicle, coupled with marketing strategies to convince drivers to give up ownership of a private vehicle and laws that accommodate the technical and control changes that accompany autonomous vehicles. The impact vehicle automation will have on law enforcement and the

* J.D., pending, University of Minnesota Law School, 2015; Town Chair, Oak Grove, Wis., 2013–present; Research Assistant, University of Minnesota Humphrey School of Public Affairs, 2009–2011; M.M. in Music Performance, Southern Illinois University at Edwardsville, 2005; B.Mus.Ed., Bethel College, Minn., 2001. A working draft of this Article was presented at the conference "Autonomous Vehicles: The Legal and Policy Road Ahead." The author would like to thank Frank Douma for his mentorship and insight.

corresponding privacy rights of the users of automated vehicles is the piece of the puzzle addressed in the following discussion.[1]

A potentially drastic reduction in law enforcement engagement with citizens is an often overlooked outcome of self-driving vehicles, as the focus remains steadily on highway safety and efficiency of traffic flow.[2] Many of the safety benefits reaped as humans are taken out of the second-by-second decision-making equation of driving will also eliminate traffic violations; as vehicles become increasingly automated, the number of traffic violations will continually decrease.[3] At the point where vehicles are driverless, it appears that the necessity of traffic-related stops could become moot altogether.[4] Between now and then, however, there will be questions raised every step of the way, with answers that are likely to change as quickly as the modifications in the technology. Criminal liability issues in particular will arise in two ways—a legislative need for the actual rules of the road to change and a judicial response regarding the enforcement of those laws.

The majority of the answers sought depend on more detailed specifications of the technologies to be used, as well as infrastructure plans for self-contained and interconnected vehicles, but the areas to be impacted are easily identifiable. This Article will focus on the criminal liability aspects of automated vehicles, beginning with impacts on the traffic codes that are expected (and in some cases, have already begun). The heart of the discussion will be in the judicial response category, examining the privacy protections around the digital information created by the car itself. The conclusion will identify possible courses of action for both government entities and manufacturers of these vehicles as they establish the parameters in which the vehicles operate.

---

1. Automated Vehicles have varying levels of automation, while autonomous vehicles are capable of driving themselves independently. Additionally, some self-driving vehicle concepts include vehicle-to-vehicle and vehicle-to-infrastructure communication.

2. *See* Dorothy J. Glancy, *Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J.L. SCI. & TECH. 619, 663 (2015) ("[J]ust over half of all citizen contacts with police occur in connection with traffic stops.").

3. *See* Frank Douma & Sarah Aue Palodichuk, *Criminal Liability Issues Created by Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1157, 1158 (2012).

4. Pursuit of criminals would still require traffic stops, but would not likely be considered a traffic-related stop.

I. LEGISLATIVE RESPONSE: CHANGING THE TRAFFIC CODE

Automated vehicles will eliminate traffic offenses, create traffic offenses, and change the implications of everything from who is driving to how violations are defined.[5] Several states and the District of Columbia have begun authorizing autonomous vehicles legislatively,[6] although experts argue that a lack of permission in other jurisdictions does not necessarily serve as a prohibition of their use.[7] The first priority in establishing regulation of these vehicles is designating who is responsible for their operation. Operation of—or control of, in the legal sense—the vehicle is required by every state that expressly allows for the testing or use of an autonomous vehicle on public roads.[8] In Nevada, this requirement for operation is met by a "human operator . . . [s]eated . . . [m]onitoring . . . [and c]apable of taking over immediate manual control of the autonomous vehicle in the event of a failure of the autonomous technology or other emergency."[9] Nevada also requires a specific "driver's license endorsement for the operation of an autonomous vehicle,"[10] while Florida specifies that anyone "who possesses a valid driver license may operate an autonomous vehicle in autonomous mode."[11]

That these legislative approaches require a human operator is likely a reflection of the tolerance of the general public's comfort level. It is also the simplest transition available to lawmakers who face the task of navigating a complicated road of strict liability traffic violations, settled

---

5. Gabriel Weiner & Bryant Walker Smith, *Automated Driving: Legislative & Regulatory Action*, CTR. FOR INTERNET & SOC'Y, http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action (last modified Feb. 3, 2015) (providing a current fifty-state survey of statutes that were adopted or changed in order to address increases in autonomous vehicles).

6. *See id.*

7. Bryant Walker Smith, *Automated Vehicles Are Probably Legal in the United States*, 1 TEX. A&M L. REV. 411, 413 (2014).

8. *See* Weiner & Smith, *supra* note 5; *infra* notes 9–11 and accompanying text.

9. NEV. REV. STAT. § 482A.070(1)–(3) (2013); *see also* CAL. VEH. CODE § 38750(b)(2) (West 2015).

10. NEV. REV. STAT. § 482A.200 (2013).

11. FLA. STAT. § 316.85(1) (2014).

court precedents, and looming public safety concerns.[12] If there is an operator responsible for the behavior of the vehicle, then speeding is still speeding, drunk driving will continue to result in a DWI, and negligence can be met as an intent requirement in a fatal accident. Interestingly, some states that demand an operator pay attention to the vehicle on autopilot have exempted those very operators from bans on texting and use of handheld wireless communications devices.[13]

If the autopilot of airplanes is of any use in predicting effects of the automation of vehicles, the biggest problem with holding drivers responsible as operators, even though they are not operating cars in a meaningful way, is complacency. Human error, whether through boredom or simply not paying attention, "remains *the leading cause* of aviation accidents" as automation has increased.[14] Another significant difficulty with holding drivers accountable as operators is the potential benefits lost from a policy standpoint without a "designated driver" option, including the possibility of being used as a late-night ride home for an intoxicated person,[15] a shuttle for an elderly person who no longer can pass a driving test, or a taxi for someone not yet old enough to take the wheel himself.[16] Drivers of the next generation must be considers as well; eventually there will be people whose driving experience is limited to self-driving vehicles. It is likely that handing control over to an inexperienced operator in the case of an emergency would yield a worse result than having the car make decisions for itself.

A challenge to this operator-as-babysitter approach is already on the horizon, as Google has announced that its

---

12. *See* Douma & Palodichuk, *supra* note 3, at 1162 (discussing how new laws regulating autonomous vehicles might "var[y] significantly from traditional laws that consider the operator of a motor vehicle to be actively controlling the vehicle.").

13. *E.g.*, FLA. STAT. § 316.305(3)(b)(7) (2014); NEV. REV. STAT. § 484B.165(7) (2013).

14. Maria Konnikova, *The Hazards of Going on Autopilot*, NEW YORKER (Sept. 4, 2014), http://www.newyorker.com/science/maria-konnikova/hazards-automation (introducing the article with a narrative about a flight crew engaged in a distracting conversation during landing which caused an unnecessary stall and killed everyone on board).

15. Formerly known as the "Take me home, I'm drunk" button. Douma & Palodichuk, *supra* note 3, at 1158.

16. *Id.*

driverless cars will be ready for deployment in two to five years.[17] These cars have no steering wheel and no pedals[18] (although for test purposes manual controls are present because they are required under California law[19]). Whether California will choose to amend its regulations to allow for Google's design is yet to be seen, but Google "hope[s to] see you on the streets of Northern California" in 2015.[20]

Switching gears to actual traffic violations, it does not take much of an imagination to see how some offenses could easily be eliminated over time and how the creation others will be absolutely necessary in order for the technology to progress. Expired registration tags and the proof of insurance requirement could become things of the past if autonomous vehicles require codes confirming the car is up-to-date administratively to function. Further, some prominent new offenses will likely address handovers from autopilot to human operator,[21] situations where autonomous vehicles are prohibited,[22] and the consequences for hacking into a vehicle's driving technology.[23]

There is also a category of pre-existing laws that will need modification to accommodate autonomous vehicles, some of which should already be revised considering the number of vehicles on the road already that possess low-level automated capabilities.[24] These low-level automations include driver assistance such as adaptive cruise control and partial automation features like lane assist.[25] Even when working properly, it is possible for adaptive cruise control to

---

17. The Associated Press, *Google Expects Public in Driverless Cars in 2 to 5 Years*, N.Y. TIMES (Jan. 14, 2015, 5:34 PM), http://www.nytimes.com/aponline/2015/01/14/business/ap-us-google-driverless-car.html.

18. *Id.*

19. CAL. VEH. CODE § 38750(c)(1)(D) (West 2015).

20. *Google Self-Driving Car Project*, GOOGLE PLUS (Dec. 22, 2014) https://plus.google.com/+GoogleSelfDrivingCars/posts/9WBWP2E4GDu.

21. *See* Douma & Palodichuk, *supra* note 3, at 1162–64 (discussing new regulations for autonomous vehicles).

22. *See generally id.* (discussing scenarios where the driver would be required to take control of an autonomous vehicle).

23. *Id.* at 1159, 1164–68.

24. JAMES M. ANDERSON ET AL., RAND CORP., AUTONOMOUS VEHICLE TECHNOLOGY: A GUIDE FOR POLICYMAKERS 2 (2014), *available at* http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-1/RAND_RR443-1.pdf.

25. *Id.*

"misbehave" under the written rules of the road.[26] For example, if a car is gauging speed based on the vehicle in front of it in a thirty-five mile per hour zone, what happens as the two vehicles pass into a fifty-five mile per hour zone? The second car will likely be speeding at some point. Following too closely is another citable activity that becomes routine for cars traveling together with adaptive cruise control.[27] Lane assist features present their own problems that range from switching lanes inappropriately to creating unnecessary traffic stops because of weaving.[28] Along with technical issues, it will also be important for the new traffic code to clarify the standards for automated operators if they are different from those expected of human operators. The question has been raised whether standards "merely require an automated vehicle to perform as well as a reasonable human driver—or will governments, courts, and consumers expect something more?"[29]

Other states are looking at the legislative prototypes as they are adopted, with many proposals sitting in committee.[30] Legislators, as well as proponents of the technological advances, are looking to the federal government for nationwide guidelines, but the National Highway Traffic Safety Administration (NHTSA) is hesitant to recommend rules for consumer use.[31] NHTSA's reserved involvement has frustrated

---

26. *See* ORG. FOR ECON. CO-OPERATION & DEV., ROAD SAFETY: IMPACT OF NEW TECHNOLOGIES 77 (2003).

27. *Id.* ("Abuse of new technologies is also a serious threat. As an example if adaptive cruise control results in drivers following each other too closely, then risk might actually increase.").

28. Chad Kirchner, *Lane Keeping Assist Explained*, MOTOR REV. (Feb. 17, 2014), http://motorreview.com/lane-keeping-assist-explained/ (discussing the strengths as well as the weaknesses of new lane keeping assist technologies).

29. Bryant Walker Smith, *Automated Vehicles Are Probably Legal in the United States*, CENTER FOR INTERNET & SOC'Y (Apr. 15, 2013, 11:58 AM), http://cyberlaw.stanford.edu/blog/2013/04/automated-vehicles-are-probably-legal-united-states. Smith also asks, "how and to whom will laws that prescribe 'reasonable,' 'prudent,' 'practicable,' and 'safe' driving apply?" *Id.*

30. *See* Weiner & Smith, *supra* note 5 (presenting a breakdown of the progress various states have made in terms of autonomous vehicle legislation).

31. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., PRELIMINARY STATEMENT OF POLICY CONCERNING AUTOMATED VEHICLES 10 (2013), *available at* http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf ("NHTSA has considerable concerns . . . about detailed state regulation on safety of self-driving vehicles, and does not recommend at this time that states permit operation of self-driving vehicles for purposes other than testing.").

the process for some, as Florida's Autonomous Vehicle Report points out, "[w]hile NHTSA recommends establishing reporting requirements to monitor the performance of self-driving technology during testing, Department staff does not have the expertise to interpret or apply the results. This is a function normally provided by the federal government (NHTSA)."[32] It appears, unsurprisingly, that it is difficult to create legislation around a technology that doesn't yet exist.[33] On the other hand, it is possible that government intervention could stifle progress and limit the development of this technology by addressing only that which is reasonably anticipated at the moment rather than looking to potential uses ten or twenty years down the road.

II. JUDICIAL RESPONSE: IS IT A PHONE, IS IT A CAR . . . IT'S A MINICOMPUTER!

The only place a conversation on the Fourth Amendment and transportation technologies can start is with the creation of data. The bottom line is that once data exists, it is accessible for prosecutorial use.[34] The strength of the restrictions on its use through the courts, specific legislation aimed at protecting the data of users of smart vehicles, and the architects who make the final calls on privacy and security decisions in automated vehicles each play important roles in setting expectations—not just for criminals, but all consumers—in the new era of smartphones, minicomputers, and self-driving vehicles.

If the discussion on legislating autonomous vehicles created uncertainty around the development of applicable traffic codes, the privacy protections surrounding data found within those vehicles are equally difficult to predict considering

---

32. JULIE L. JONES, FLA. HIGHWAY SAFETY & MOTOR VEHICLES, AUTONOMOUS VEHICLE REPORT 5 (2014), *available at* http://www.flhsmv.gov/html/HSMVAutonomousVehicleReport2014.pdf.

33. *See* Alex Davies, *Self-Driving Cars Are Legal, but Real Rules Would Be Nice*, WIRED (May 15, 2015, 7:00 AM), http://www.wired.com/2015/05/self-driving-cars-legal-real-rules-nice/ ("The tech is new, complicated, and being developed in different ways by different companies, so just understanding how it works is difficult, let alone knowing how to make it work safely.").

34. *See* Douma & Palodichuk, *supra* note 3, at 1167–68; Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1196, 1216 (2012).

the absence of examples to study at this point in time.[35] This creates difficulties because there are a wide variety of prototypes utilizing various levels of automation, some sharing similar technology, but all having unique attributes.[36] It is hard to determine the level of privacy protection expected when one cannot even determine exactly what is being protected.[37]

Automated vehicles will potentially contain a wealth of digital information previously unavailable to law enforcement officers, including personally identifiable information, route history and planning, and a log of the car's actions.[38] The protections afforded through the Fourth Amendment will be vital in making the public feel comfortable using these vehicles without having a chilling effect on their actions. The mobile nature of the car lends itself to creating locational privacy problems, but the Supreme Court has not yet tackled the issue. In 2012, warrantless GPS tracking came before the Court in *United States v. Jones*, but was decided in a narrow ruling on trespass.[39] While the *Jones* ruling that did not lay out expectations that can be relied upon for future vehicle-related privacy cases, Justice Sotomayor's concurrence pieced together the Mosaic theory to address the locational privacy issue presented.[40] It is more common to see location-based cases arising out of historical and real time cell site location information cases, in which people are tracked by their cell phone signals. None of these cases have reached the Supreme Court however, and the lower courts are split significantly.[41] The best insight into whether information stored in an automated vehicle will be accessible by a warrantless search also comes in the context of cell phones. *Riley v. California*

35. Glancy, *supra* note 34, at 1216–17 ("Because autonomous vehicles are not yet available for general use, predictions about privacy expectations regarding autonomous vehicles necessarily have to be extrapolated from experience with other types of vehicles, transportation issues, and intelligent systems.").

36. *Id.* at 1172–73.

37. *Id.*

38. *Id.* at 1186.

39. United States v. Jones, 132 S. Ct. 945, 949–53 (2012).

40. *Id.* at 957 (Sotomayor, J., concurring).

41. *E.g.*, United States v. Davis, 754 F.3d 1205 (11th Cir. 2014) (holding no warrant was needed to access location data from a cell service provider), *aff'd in relevant part*, 785 F.3d 498 (11th Cir. 2015); Tracey v. State, 152 So. 3d 504 (Fla. 2014) (holding that accessing real time cell site location information required a warrant).

addresses digital data head on for the first time and does so in way that is meaningful beyond the facts in either of the cases at hand.[42]

III. RILEY FACTS

Riley was pulled over for driving with expired registration tags, and the traffic stop resulted in his car being impounded because his license had been suspended.[43] An inventory search of his car revealed two handguns under the hood, resulting in Riley's arrest for possession of concealed and loaded firearms.[44] When searching Riley, an officer seized his smartphone and noticed what he presumed to be the gang abbreviation "CK" next to names in the phone.[45] Later, another detective went through Riley's phone looking for more gang-related evidence, during which photos of Riley in front of a car allegedly used in a shooting were discovered.[46] Riley was charged with (and eventually convicted of) firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder.[47] His sentence of fifteen years to life in prison carried an enhancement due to committing those crimes for the benefit of a criminal street gang.[48]

Wurie was arrested after being observed making a drug sale.[49] Two of his cell phones were seized, including a flip phone.[50] A police officer pressed one button to access the call log and another to determine the phone number associated with the "my house" label shown on the external screen.[51] The number was traced to an apartment building where they saw Wurie's name on the mailbox and a woman resembling the

---

42. Riley v. California, 134 S. Ct. 2473 (2014). The *Riley* decision deals with two sets of facts. The first set of facts concerned Riley, who was arrested as a result of a traffic stop for driving with expired registration tags. *Id.* at 2480. The second set of facts dealt with Wurie, who was arrested after his involvement in an apparent drug deal. *Id.* at 2481.

43. *Id.* at 2480.

44. *Id.*

45. *Id.*

46. *Id.* at 2480–81.

47. *Id.* at 2481.

48. *Id.*

49. *Id.*

50. *Id.*

51. *Id.*

photo on his phone through a window.[52] The building was secured while they got a warrant, after which 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash were found in Wurie's apartment.[53] Convictions stemming from this search led to a prison sentence of 262 months.[54]

IV. RILEY FINDINGS: THE DIGITAL FRONTIER

The decision in *Riley* heralds the Supreme Court's arrival in the "digital age," a time in which the majority of people "carry a cache of sensitive personal information" as they go about their days.[55] The Court held that a warrant is generally required when searching digital information on a cell phone seized during a lawful arrest.[56] In *Riley*, the information was contained in a cell phone, but the Court made clear that the protection is around digital data, describing both flip phones and smartphones as "minicomputers that also happen to have the capacity to be used as a telephone."[57]

The Fourth Amendment protects against unreasonable searches and seizures of one's "persons, houses, papers, and effects," generally requiring a warrant showing probable cause to justify such a search.[58] Exceptions to the warrant requirement are described in *Wyoming v. Houghton* as a balancing act between the furthering of government interests and the extent of an intrusion on an individual's privacy.[59] The Court refers to three cases—*Chimel*, *Robinson*, and *Gant*—for the context of the search incident to arrest (SITA) exception to the warrant requirement.[60] *Chimel* provides the groundwork for the SITA doctrine in the form of two prongs that examine

52. *Id.*
53. *Id.*
54. *Id.* at 2482.
55. *Id.* at 2490.
56. *Id.* at 2493.
57. *Id.* at 2489.
58. U.S. CONST. amend. IV.
59. Wyoming v. Houghton, 526 U.S. 295, 299 (1999) ("[W]e must evaluate the search or seizure under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.").
60. *See* Arizona v. Gant, 556 U.S. 332, 343 (2009); United States v. Robinson, 414 U.S. 218, 235 (1973); Chimel v. California, 395 U.S. 752 (1969).

the government interests of officer safety and preservation of evidence.[61] In *Robinson*, the Court broadly found the *Chimel* prongs to be satisfied in all searches incident to lawful arrest, rejecting a case-by-case determination of whether a weapon or evidence was likely to be found.[62] The pocket searching in *Robinson* was not seen as a greater intrusion of privacy beyond the arrest itself.[63] A third case applies specifically to the search of an arrestee's vehicle.[64] *Gant* extended the SITA exception when it is "reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."[65]

In *Riley*, the Court held that neither prong of government interest in *Chimel* was furthered when applied to the digital contents of cell phones.[66] As far as officer safety is concerned, while the physical phone could be examined for potential use as a weapon, the data inside cannot cause harm to the officer.[67] Warning an officer of impending backup called for by the arrestee was also raised as a potential safety issue and concerns about the destruction of evidence through remote wiping of data or data encryption were considered,[68] but the Court noted those situations can be better addressed through a case-specific exception like the one for exigent circumstances.[69]

Although there was very little to be found in terms of legitimate government interests at stake, the digital distinction lies on the other side of the *Wyoming v. Houghton* balancing

---

61. *Chimel*, 395 U.S. at 762–63 ("When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape . . . . In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.").

62. *Robinson*, 414 U.S. at 235.

63. *Id.*

64. *Gant*, 556 U.S. at 332.

65. *Gant*, 556 U.S. at 343.

66. Riley v. California, 134 S. Ct. 2473, 2478 (2014) ("But a search of digital information on a cell phone does not further the government interests identified in *Chimel*, and implicates substantially greater individual privacy interests than a brief physical search.").

67. *Id.* at 2485.

68. *Id.* at 2485–86 (suggesting two solutions for the prevention of remote wiping or encryption: (1) remove the phone's battery, or (2) use Faraday bags to isolate the phone from radio waves).

69. *Id.* at 2494 (providing reassurance that "extreme hypotheticals" can be addressed through the exigent circumstance exception).

test. The Court did not extend *Robinson* to permit searches of data stored on cell phones because of the vast difference between a search of physical objects and digital content; searching pockets is not that much more intrusive than the actual arrest itself, but it is considerably different than searching digital data.[70] Instead, *Riley* classifies a cell phone search as a substantial intrusion because of both the quantitative and qualitative differences between digital data and physical objects.[71] Not only can a phone store many distinct types of information, it can hold an immense quantity of just one type information[72]—a phone fits in a pocket, but can hold more than a house.[73] The information held in cell phones often touches on every aspect of people's lives: Internet browsing history, location data to reconstruct movements, and apps for everything from tracking pregnancy symptoms to political party affiliations.[74] Therefore, a search of a cell phone and all of the sensitive information it contains outweighs the minimal government interest present.[75]

Finally, the government's argument to extend the application of *Gant* from the context of vehicle-related circumstances was rejected by the Court, finding it would have "no practical limit at all when it comes to cell phone searches."[76] Without discussion, the Court pointed to previous cases that laid a foundation of a diminished expectation of privacy only in the vehicle context, as well as the more heavily weighted government interest in vehicle searches.[77] Other

---

70. *Id.* at 2484 ("But while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones.").

71. *See id.* at 2489.

72. *Id.* Without mentioning *United States v. Jones*, Justice Roberts points out that this decision does not address whether "the collection or inspection of aggregated digital information amounts to a search under other circumstances." *Id.* at 2489 n.1.

73. *Id.* at 2491 ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house . . . .").

74. *Id.* at 2490.

75. *Id.* at 2478.

76. *Id.* at 2492.

77. *Id.* (citing Thornton v. United States, 541 U.S. 615 (2004); Wyoming v. Houghton, 526 U.S. 295, 303–04 (1999)).

fallback options were dismissed as well, based on their inability to provide clear categorical rules.[78]

The facts of *Riley* indicate the case is about the information contained on a cell phone, but the decision was made on data—the 200-year-old institution has entered the digital frontier. Embracing this new terrain does not include looking back and seeing that the old way was wrong; instead it means acknowledging that some things will need to be handled differently moving forward.

V. WILL SDVS REAP RILEY'S BENEFITS?

In declining to apply the *Robinson* rationale to cell phones, the Court established that a search of digital content constitutes substantial intrusion upon an individual's privacy, creating a different rule for handling digital searches than is used for physical searches.[79] The ruling suggests a natural extension of this protection to other containers of digital data by labeling cell phones as "minicomputers." While the potential for its application to automated vehicle technology remains uncertain,[80] *Riley* indicates that the interest in protecting the personal information disclosed through use of such a vehicle would be weighed heavily as well.[81]

Like cell phones, autonomous vehicles could contain types of digital data that are qualitatively different from physical objects and could have the capacity to record that data in significant amounts. As mentioned above, the three most sensitive types of data would be personally identifiable information, route history and planning, and a log of the car's actions. The combination of this information could readily confirm the identity of a driver while revealing where she has been and is going, as well as provide evidence that a traffic violation has occurred. Even just one aspect, though, in a large

78. *Id.* at 2491 (dismissing the government's suggestions of applying an analogue test, saying it would create questions of which digital files are comparable to physical records; it would also allow a more invasive search because it could include items not typically carried in physical form).

79. *Supra* note 70 and accompanying text.

80. It should be acknowledged that it isn't clear what that technology will even look like. *See supra* notes 35–37 and accompanying text.

81. *Riley*, 134 S. Ct. at 2492 ("[I]n the vehicle context *Gant* restricts broad searches resulting from minor crimes such as traffic violations."). The decision goes on to discuss cell phone searches to look for evidence of speeding or texting while driving. *Id.*

quantity is likely considered an intrusion.[82] For example, the location information element could be structured in a way to show where a person has been in the last twenty-four hours, if routes were time stamped and biometrics authentication of users were required to operate the vehicle.

Although it may seem apparent that sensitive digital data such as this assuredly deserves protection after reading *Riley*, *Gant*'s automobile exception to the warrant requirement will have some effect on the balance of the equation because of the diminished expectation of privacy in vehicles. Even though the Court did not extend *Gant*'s holding that the SITA exception includes searches for evidence related to the crime of arrest because there would be no practical limit to the search of a cell phone, when that same rule is applied solely in the vehicle context and to a search of the vehicle itself, it could yield a different result. Another decision leaning in the government's favor is *Knotts*,[83] which established that there is no reasonable expectation of privacy in a person's movements "in an automobile on public thoroughfares."[84] Even though this rule has never been overturned, two concurrences in *Jones* found some types of surveillance to violate a reasonable expectation of privacy.[85] The concurrences were signed by a total of five justices,[86] indicating *Knotts* is susceptible to challenge.

The Court's desire to provide law enforcement with clear, categorical rules would run into the same difficulties with automated vehicle technology that were present in Riley's smartphone if *Gant* were applied. There would be no practical limit to the amount of information accessed and the substantial intrusion of privacy would remain the same. However, vehicles

---

82. *See id.* at 2489–91 & n.1 (discussing the privacy consequences arising from the quantitative capacity of a cell phone).

83. United States v. Knotts, 460 U.S. 276 (1983).

84. *Id.* at 281. *But see* Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 299 ("But that does not mean that expectations of privacy on public roads are worthy of no legal protection at all.").

85. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); *id.* at 957 (Alito, Ginsburg, Breyer, Kagan, JJ., concurring) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

86. Justice Ginsburg, Justice Breyer, and Justice Kagan joined Justice Alito's concurrence. *Id.*

are highly regulated and there is precedent acknowledging the diminished expectation of privacy on the open road.[87] Whether the government's interest in gaining incriminating evidence of moving violations is significant enough to justify the intrusion of privacy is yet to be seen.

CONCLUSION

While the road ahead is not perfectly clear, it is encouraging that some states are taking the lead on creating a regulatory structure for the testing of autonomous vehicles in the absence of federal guidelines and that the courts have identified digital data as worthy of substantial protection. The legislative process must be proactive in addressing the needs identified here as manufacturers progress through the levels of automation available in consumer vehicles, with states producing more thorough codes and Congress establishing the *Riley* digital privacy protections in a way that specifically applies to automated vehicle technology. In the meantime, the next Supreme Court cases likely to have direct impact on autonomous vehicles will be centered on locational privacy issues that come from cell site tracking.

As levels of automation increase to the point where self-driving vehicles do not necessarily rely on a human operator present and where infrastructure development allows these vehicles to become interconnected rather than self-contained, more questions will be raised. If infrastructure enters the equation, expect the availability of real time location information to become an even hotter topic and to hear some experts discuss the possibility of central control options like rerouting vehicles in emergencies or police executing traffic stops electronically.

---

87. *See supra* note 84 and accompanying text.

***