NOTES

Herbie Fully Downloaded: Data-Driven Vehicles and the Automobile Exception

LINDSEY BARRETT*

The Fourth Amendment's automobile exception generally allows vehicles to be searched without a warrant. This lessened degree of protection is based partially on the need to afford law enforcement officials discretion when a suspect, evidence, or contraband is found in an automobile. It is also based on the diminished expectation of privacy in vehicles, due to their pervasive regulation and use of the public roadways. Although an autonomous vehicle would seem to undermine the mobility rationale for the automobile exception, it is the information such vehicles collect about their drivers that merits a departure from established Fourth Amendment doctrine to ensure that basic privacy protections remain in full force. This Note argues that although the mobility analysis of the automobile exception does not compel a new approach to Fourth Amendment analysis for autonomous vehicles, the information these vehicles collect represents such a significant privacy interest that law enforcement officials should be required to obtain a warrant before accessing vehicle data. This result is supported by the Supreme Court's analysis in Riley v. California *and* United States v. Jones.

TABLE OF CONTENTS

---

* Policy Fellow, Future of Privacy Forum; Georgetown Law, J.D. 2017; Duke University, B.A. 2014. Thank you to Professor Ed Walters, whose enthusiasm for self-driving vehicles sparked my own; Professors Paul Ohm and David Vladeck, for their unceasing patience and thoughtful advice; and Molly Clarke, without whom the title of this piece would be boring.

INTRODUCTION

Automated vehicles may seem like the purview of the science fiction writer, but the accelerated development of this technology has made them highly relevant to industry leaders, government regulators, and drivers in the here and now.[1] Companies like Tesla, Google, and Uber have made remarkable advances in automation, leading to a scramble among competitors to keep apace with each other.[2] Industry actors are eager to take on the role of marketplace innovator, and regulators are eager to facilitate their progress, particularly given the potential of autonomous vehicle technology to diminish the rate of traffic fatalities; 94% of traffic deaths this year were due to human error, a percentage manufacturers and regulators alike hope can be diminished through the use of autonomous vehicles.[3] Other possible benefits, though uncertain, seem similarly

1. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY 5 (2016), https://one.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf [https://perma.cc/7T6T-GSBE] ("Today, the automobile industry is on the cusp of a technological transformation that holds promise to catalyze an unprecedented advance in safety on U.S. roads and highways.").

2. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 1, at 5; Letter from Steve Kenner, Director of Products Integrity, Apple, Apple's Comments on the Federal Automated Vehicles Policy (Nov. 22, 2016), https://www.regulations.gov/contentStreamer?documentId=NHTSA-2016-0090-1115&attachmentNumber=1&contentType=pdf [https://perma.cc/BS96-DZZT] ("Apple uses machine learning to make its products and services smarter, more intuitive, and more personal. The company is investing heavily in the study of machine learning and automation, and is excited about the potential of automated systems in many areas, including transportation."); *Apple Reveals Autonomous Vehicle Ambitions*, GMA NEWS ONLINE (Dec. 4, 2016, 7:51 AM), http://www.gmanetwork.com/news/scitech/technology/591147/apple-reveals-autonomous-vehicle-ambitions/story/ [https://perma.cc/3JEB-7D8Y] ("Apple looks forward to collaborating with NHTSA and other stakeholders so that the significant societal benefits of automated vehicles can be realized safely, responsibly, and expeditiously . . . ."); *Ford Targets Fully Autonomous Vehicle for Ride Sharing in 2021; Invests in New Tech Companies, Doubles Silicon Valley Team*, FORD MOTOR COMPANY: MEDIA CTR. (Aug. 16, 2016), https://media.ford.com/content/fordmedia/fna/us/en/news/2016/08/16/ford-targets-fully-autonomous-vehicle-for-ridesharing-in-2021.html [https://perma.cc/8SPE-9KGU]; *Pittsburgh, Your Self-Driving Uber Is Arriving Now*, UBER: BLOG (Sept. 14, 2016), https://newsroom.uber.com/pittsburgh-self-driving-uber/ [https://perma.cc/3FK5-B3QE].

3. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 1, at 5.

promising, such as reduced traffic congestion,[4] increased emissions efficiency,[5] and increased autonomy for individuals unable to drive themselves.[6] Federal officials have emphasized a gentle and cautious approach to new regulation, guided by an acknowledgement of the technology's potential and the desire to facilitate its further development.[7] Self-driving cars seem to offer the logical next step of what the car itself has always symbolized: a powerful and innovative form of freedom.

But new technology promises new freedoms only to the extent that our existing freedoms are retained through a thoughtful approach to technology and the law. Academics and policymakers spar over exceptionalist and generalist approaches to new technology,[8] but the greatest danger emerges when new technology is ill understood by courts and legislatures and allowed to be used in a way that erodes fundamental rights. When judges and lawmakers are unable to discern the practical differences between old and new technology, the inapt application of precedent can undermine the principles that those older frameworks were intended to protect.

The car is a driving force of American life, and it occupies an appropriately singular position in Fourth Amendment jurisprudence in the form of the automobile exception. In general, a vehicle is subject to a search by law enforcement on the basis of probable cause only, rather than on the basis of the warrant that is normally needed for a search.[9] But the remarkable possibilities of a self-driving vehicle invite intriguing questions about the continued relevance of the automobile exception and compel reexamination of the continued vitality of prior precedent in this new context. Automated vehicles present particular Fourth Amendment questions not only because the searched vehicle does not

4. *See* Jamie Condliffe, *A Single Autonomous Car Has a Huge Impact on Alleviating Traffic*, MIT TECH. REV. (May 10, 2017), https://www.technologyreview.com/s/607841/a-single-autonomous-car-has-a-huge-impact-on-alleviating-traffic/ [https://perma.cc/A4H8-3FPU].

5. *See* Melanie Zanona, *How Driverless Cars Can Reduce Pollution*, THE HILL (Oct. 24, 2016, 4:02 PM), http://thehill.com/policy/transportation/302550-how-driverless-cars-can-reduce-pollution [https://perma.cc/G63W-PZG4].

6. *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1186 (2012).

7. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 1, at 5–6.

8. *Compare* JOHN VILLASENOR, BROOKINGS INST., PRODUCTS LIABILITY AND DRIVERLESS CARS: ISSUES AND GUIDING PRINCIPLES FOR LEGISLATION 1, 2 (2014), http://www.brookings.edu//media/research/files/papers/2014/04/products-liability-driverless-cars-villasenor/products_liability_and_driverless_cars.pdf [perma.cc/9BFH-HVB8], *and* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208–10 (1996) (arguing that enacting technology-specific laws, rather than applying general laws to arising technology, is redundant and will result in misguided, quickly outmoded frameworks and precedent), *with* RYAN CALO, BROOKINGS INST., THE CASE FOR A FEDERAL ROBOTICS COMMISSION 1, 1–4 (2014), https://www.brookings.edu/wp-content/uploads/2014/09/RoboticsCommissionR2_Calo.pdf [https://perma.cc/MY6N-FFN9], *and* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 534–49 (1999) (responding to Judge Easterbrook and arguing that cyberspace provides categorically different behavioral incentives and constraints that existing law will fail to effectively shape). Both arguments have been made in the context of self-driving cars.

9. *See, e.g.*, California v. Carney, 471 U.S. 386, 394–95 (1985).

contain a driver, but also because the viability of the technology is contingent on the generation and collection of enormous amounts of data about the vehicle and where it travels. The presence or absence of the car's owner, the mobility of the vehicle, and the extent to which it is regulated all contribute to the justification for the Fourth Amendment's vehicle exception, and each of those aspects is impacted by the different attributes of the autonomous vehicle. But it is the quantity of the different kinds of data generated and collected by autonomous vehicles that compels a substantively different approach from current Fourth Amendment jurisprudence, and which would enable the erosion of individual privacy if current precedent were applied without acknowledging that categorical shift. Connected cars—vehicles that are distinguished by their ability to send and receive information, whether or not they are automated—present similar risks. The ability of modern vehicles to collect and transmit information also implicates the Fourth Amendment's third-party doctrine—the idea that entrusting information to a recipient obviates the sender's reasonable expectation of privacy in that information.[10]

Although the theoretical capabilities of modern vehicles invite creative and far-reaching speculation, this Note will discuss the Fourth Amendment implications of autonomous and connected vehicles as they exist now or in the proximate future. It will discuss the underlying technology of autonomous vehicles and relevant Fourth Amendment doctrine. It will then analyze two Supreme Court cases with the most bearing on the application of the Amendment to vehicle data, *United States v. Jones*[11] and *Riley v. California*,[12] and examine ensuing legal developments influenced by those two cases that could impact vehicle privacy. Finally, this Note will argue that although the differences in mobility of autonomous vehicles may not merit a radically different Fourth Amendment approach, the privacy interests implicated by data-driven vehicles should mandate that a warrant is required to search the information the car contains.

I. CONNECTED CARS AND AUTOMATED VEHICLES

Today's cars, much like everything else, are driven by data. Connectivity and automation are distinct capabilities of modern vehicles, but both enable the modern vehicle to implicate a significantly greater privacy interest than the analog car ever could due to the vast amounts of data they collect. Connected cars have some ability to record, send, or receive information. This functionality could be as rudimentary as inscrutable technical information that the driver

10. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

11. 565 U.S. 400 (2012).

12. 134 S. Ct. 2473 (2014).

cannot access or change, such as Event Data Recorder (EDR) information,[13] or as accessible (and readily revealing) as a driver's synced cell phone contacts or messages. Connected cars may have some basic automated features, such as crash collision avoidance, but they are closer in kind to a garden-variety Toyota than they are to Knight Rider. Automated vehicles will have some degree of connected features (such as an EDR) and, depending on the system involved, will require recording and possibly transmitting certain types of information for the system to function.[14] These vehicles are primarily identified, however, by an advanced degree of automation, as opposed to their connectivity.

This Part will discuss the technological capabilities of connected and automated vehicles, the differences between them, and the commercial and regulatory enthusiasm for both that have spurred the rapid growth of the technology.

A. CONNECTED CARS

Event Data Recorders (EDR), devices that record and provide technical vehicle information relating to safety events (such as a vehicle crash),[15] have been mandated in new vehicles since 2014.[16] Newer models generate increasing amounts of information and rely upon using and sharing data for the technology to improve.[17] Cars can sync with mobile devices or home-based assistant devices;[18] store the driver's phone number, contacts, call logs, text messages,[19] and financial information;[20] and keep granular records of the driver's location.[21]

---

13. *See Event Data Recorder*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/research-data/event-data-recorder [https://perma.cc/HA7V-AK2E] (defining an EDR as "a device installed in a motor vehicle to record technical vehicle and occupant information for a brief period of time (seconds, not minutes) before, during and after a crash").

14. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 1, at 5 (introducing and discussing automated vehicles); *id.* at 17–18 (discussing possible data collection requirements).

15. *See Event Data Recorder*, *supra* note 13.

16. Erin Biba, *How Connected Car Tech Is Eroding Personal Privacy*, BBC (Aug. 19, 2016), http://www.bbc.com/autos/story/20160809-your-car-is-not-your-friend [https://perma.cc/C7XA-6H8K].

17. *See* Kate Conger & Darrell Etherington, *Federal Policy for Self-Driving Cars Pushes Data Sharing*, TECHCRUNCH (Sept. 20, 2016), https://techcrunch.com/2016/09/20/federal-policy-for-self-driving-cars-pushes-data-sharing/ [https://perma.cc/MY36-2D3Q] ("Uber, Lyft and GM have all separately pointed to the vast stores of driving data collected by their respective fleets as key competitive advantages in the race to develop truly effective autonomy. And of all the data used to train these systems—information related to how autonomous vehicles handle challenging conditions or actual impact events—might be most valuable in terms of creating a really robust, adaptable self-driving car.").

18. *See, e.g.*, Natt Garun, *Screendrive: 2017 Ford Fusion Energi Is the First Car with Alexa*, VERGE (May 1, 2017, 10:00 AM), https://www.theverge.com/2017/5/1/15438554/2017-ford-fusion-energi-alexa-sync3-review [https://perma.cc/K6RX-5HN5].

19. Lisa Weintraub Schifferle, *What Is Your Phone Telling Your Rental Car?*, FED. TRADE COMMISSION: CONSUMER INFO. BLOG (Aug. 30, 2016), https://www.consumer.ftc.gov/blog/what-your-phone-telling-your-rental-car [https://perma.cc/7FNG-9WPK].

20. *See, e.g.*, Kristen Hall-Geisler, *Volkswagen Purchases PayByPhone for Parking*, TECHCRUNCH (Dec. 28, 2016), https://techcrunch.com/2016/12/28/volkswagen-purchases-paybyphone-for-parking/ [https://perma.cc/85ZW-QGAH]; Lucas Mearian, *By 2020, Your Wi-Fi-Connected Car Will Pay for Parking, Gas*, COMPUTERWORLD (Sept. 30, 2016, 11:59 AM), http://www.computerworld.com/article/3126153/car-tech/by-2020-your-wi-fi-connected-car-will-pay-for-parking-gas.html [https://perma.cc/9KWX-5MAQ] (discussing the Audi Connect

New cars generate and share data through a variety of methods, such as vehicle-to-vehicle (V2V) communications, vehicle-to-infrastructure (V2I) communications, vehicle-to-device (V2D) communication,[22] or vehicle-to-everything (V2X) communications—the catchall term for the vehicle's ability to communicate with anything.[23] Depending on the type of system the vehicle relies on—such as whether it collects and uses data within a closed system, or whether it collects, sends, and receives information throughout a wireless network—the vehicle is likely to produce differing expectations of privacy.[24] The design of the car's data system is likely to have a particularly significant impact on how the third-party doctrine is applied.[25]

Even among nonautonomous vehicles, connectivity is an increasingly prevalent phenomenon. In the first quarter of 2016, connected cars accounted for a third of all new cellular devices—the telecommunications company AT&T, for example, has eight million cars on its network.[26] As cars have become more like smartphones, like the Tesla model that comes with a touchscreen web browser,[27] they begin to implicate more of the same privacy interests because they are able to record and collect increasing amounts of user information. GPS systems map the location of the vehicle, and the ability to sync to the driver's mobile device allows the car to access information contained on the device, such as messages and contacts.[28] Other features go further: Consider the Chevy Corvette, which allows the driver to record high-definition video of the car driving from the driver's point of view and any noise made in the cabin, and to download the

parking payment program); *The Connected Car: Visa Looks Ahead*, VISA, https://usa.visa.com/visa-everywhere/innovation/visa-connected-car.html [https://perma.cc/C84R-REU8].

21. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-649T, CONSUMERS' LOCATION DATA: COMPANIES TAKE STEPS TO PROTECT PRIVACY, BUT PRACTICES ARE INCONSISTENT, AND RISKS MAY NOT BE CLEAR TO CONSUMERS 7 (2014) (statement of Mark L. Goldstein), http://www.gao.gov/assets/670/663787.pdf [https://perma.cc/K56A-YR2P] ("[M]ost of the in-car navigation service companies we examined for the 2013 report provide broadly worded reasons for collecting location data that potentially allow for unlimited data collection and use.").

22. U.S. Dep't of Transp., *Connected Vehicle Core System Baseline Documentation*, INTELLIGENT TRANSP. SYS. JOINT PROGRAM OFFICE, http://www.its.dot.gov/press/2011/connected_vehicle_coresystem_docs.html [https://perma.cc/K2LZ-7WTN].

23. *See* Glancy, *supra* note 6, at 1178.

24. *See id.* at 1177 (discussing the differences between "self[-]contained autonomous vehicle[s]" and "interconnected autonomous vehicles").

25. *See infra* Section IV.C.

26. Kristen Hall-Geisler, *More Cars Than Phones Were Connected to Cell Service in Q1*, TECHCRUNCH (June 20, 2016), https://techcrunch.com/2016/06/20/more-cars-than-phones-were-connected-to-cell-service-in-q1/ [https://perma.cc/7VHP-6BFF].

27. *See* Anthony Ha, *Tesla Drivers Are Using Their In-Dash Browser to Keep Up with the News, Quantcast Says*, TECHCRUNCH (Apr. 2, 2014), https://techcrunch.com/2014/04/02/quantcast-measures-tesla/ [https://perma.cc/U37P-SSD9].

28. *See* Schifferle, *supra* note 19.

footage remotely.[29] Companies are leaping at the chance to monetize the data generated by connected cars, manufacturing new vehicles that are increasingly able to collect vast amounts of information about drivers.[30]

The increased connectivity of today's vehicles and the ensuing implications have not gone unnoticed by legislators. A report on connected vehicles by Senator Ed Markey found that nearly all new vehicles sold today are connected and that manufacturers "collect large amounts of data on driving history and vehicle performance."[31] That information includes location, such as "[p]hysical location recorded at regular intervals; [p]revious destinations entered into navigation system; [and] [l]ast location parked,"[32] as well as less sensitive information related to vehicle performance, such as battery health and tire pressure.[33] The report relied on data compiled from twenty major automobile manufacturers, which included a wide range of collection, retention, and use policies.[34] The overwhelming conclusion of the report was that drivers are frequently unaware of what data is collected and frequently unable to opt out of collection even when they are aware.[35]

B. AUTONOMOUS VEHICLES

A connected car may not necessarily be autonomous, but a highly automated or autonomous vehicle necessarily will contain some capacity to collect, send, and receive different types of data, or will at least depend on some manner of mapped data (such as through GPS) for the vehicle to function autonomously, in

29. *See Corvette Stingray and Z06 Performance Data Recorder Quick Reference Guide*, CHEVROLET (Dec. 2014), https://www.chevrolet.com/content/dam/Chevrolet/northamerica/usa/nscwebsite/en/Home/Ownership/Manuals_and_Videos/02_pdf/PDR_Quick_Reference_Guide.pdf [https://perma.cc/6M4T-JFKL] (allowing users to "record, share and analyze [their] driving experiences on and off the track"); *see also* Jaclyn Trop, *The Next Data Privacy Battle May Be Waged Inside Your Car*, N.Y. TIMES (Jan. 10, 2014), https://www.nytimes.com/2014/01/11/business/the-next-privacy-battle-may-be-waged-inside-your-car.html [https://nyti.ms/1cLG1eC].

30. *See* MCKINSEY & CO., MONETIZING CAR DATA: NEW SERVICE BUSINESS OPPORTUNITIES TO CREATE NEW CUSTOMER BENEFITS 11 (2016), http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/monetizing-car-data [https://perma.cc/GCY8-FDXS] ("With increasing proliferation of new features and services, car data will become a key theme on the automotive industry agenda and—if its potential is fully realized—highly monetizable.").

31. ED MARKEY, TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 1 (2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [https://perma.cc/4Q6X-RU2W].

32. *Id.* at 8.

33. *See id.* at 11 ("Manufacturers use personal vehicle data in various ways, often vaguely to 'improve the customer experience' and usually involving third parties, and retention policies—how long they store information about drivers—vary considerably among manufacturers. A wide array of responses was received regarding the ways that manufacturers use vehicle history information . . . . This lack of transparency in personal vehicle data usage leaves consumers with little knowledge about how the companies actually use their data.").

34. *See id.* at 11.

35. *See id.* at 1.

addition to any connected features the car may have.[36] Certain automated features are already widely used, such as blind-spot detectors and collision avoidance.[37] Most current features rely on a combination of lidar,[38] radar, cameras, and other sensors.[39] It follows that automation is not a binary state, but more nuanced. The guidance released by the National Highway Traffic Safety Administration (NHTSA) on automated vehicles relies on a six-part scale of automation, a structure originally established by SAE International.[40] These six levels range from zero, where the human driver is entirely responsible for controlling the vehicle, to six, where the car can conduct all tasks a human driver would be expected to perform under all circumstances.[41] Automated vehicles present particularly unpredictable and significant privacy risks as the machine-learning technology that enables them is dependent on data collection to improve.[42] Although different companies have taken different approaches, all autonomous vehicles produce an enormous amount of data,[43] and dependence on that data will only increase as the technology becomes more viable and popular.[44]

C. REVVED BY REGULATORS

Federal regulators have been eager to facilitate the development of autonomous and connected vehicle technology, particularly in light of its potential to increase driver safety.[45] During the Obama Administration, the Executive Office

36. *See generally* 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 (2015) (discussing different types of technology used in self-driving vehicles).

37. Guilbert Gates et al., *The Race for Self-Driving Cars,* N.Y. TIMES (Dec. 14, 2016), http://www.nytimes.com/interactive/2016/12/14/technology/how-self-driving-cars-work.html [https://nyti.ms/2jRrB55].

38. Lidar, short for light detection and ranging, is a particular type of sensor capable of creating three-dimensional maps of its surroundings. It is a key component of most forms of self-driving technology. *See* John R. Quain, *What Self-Driving Cars See*, N.Y. TIMES (May 25, 2017), https://www.nytimes.com/2017/05/25/automobiles/wheels/lidar-self-driving-cars.html [https://nyti.ms/2rYKpTN].

39. Gates et al., *supra* note 37 (describing the different technology employed by models currently under development at a range of car manufacturers and technology companies, such as Tesla, Ford, Apple, and Google); *see also* Quain, *supra* note 38.

40. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 1, at 9.

41. *See id.*

42. *See generally* Jesse Levinson et al., *Towards Fully Autonomous Driving: Systems and Algorithms*, IEEE Intelligent Vehicles Symposium (June 5–9, 2011), http://cs.stanford.edu/people/teichman/papers/iv2011.pdf [https://perma.cc/BCS2-U35V].

43. *See* Nir Erez, *The New World of Mobility,* TECHCRUNCH (Oct. 10, 2016), https://techcrunch.com/2016/10/10/the-new-world-of-mobility [https://perma.cc/EQ9S-WDJ3] ("The average autonomous vehicle, by 2020, will produce 4,000 gigabytes per day . . . . [T]he average person generates about] 6-to-700 megabits a day. By 2020, the estimate is 1.5 gigabytes a day for the average person." (quoting Intel CEO Brian Krzanich)).

44. *See* Levinson et al., *supra* note 42.

45. *U.S. DOT Advances Deployment of Connected Vehicle Technology to Prevent Hundreds of Thousands of Crashes*, U.S. DEP'T OF TRANSP. (Dec. 13, 2016), https://www.transportation.gov/briefing-room/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands [https://perma.cc/QZ3J-T6ZY] ("Advanced vehicle technologies may well prove to be the silver bullet in

of the President released reports on artificial intelligence that heralded the potential of autonomous vehicles[46] and hosted "The White House Frontiers Conference" at Carnegie Mellon University, which was devoted to exploring the "future of innovation" and the potential of technology like autonomous vehicles.[47] The NHTSA released a Federal Automated Vehicles Policy, as well as a notice of proposed rulemaking, announcing the agency's intention to mandate V2V communications in light vehicles,[48] with a future rulemaking focused on V2I communications.[49] As NHTSA defines it, V2V uses dedicated short-range communications (DSRC) to exchange basic safety messages (BSM) on location, speed, and direction with other vehicles, enabling them to "speak the same language."[50] The Notice of Proposed Rulemaking (NPRM) elaborates on the relationship between connected and automated vehicles, with the agency noting that the rulemaking "complements the Department's work to accelerate the development and deployment of automated vehicles" and that V2V and autonomous vehicle technologies are distinct but related.[51] The final rule's requirement that all light vehicles contain V2V technology will include "highly automated passenger vehicles,"[52] and cites industry comments that "it would not be possible to optimize the benefits of automated vehicles without V2V."[53] The agency also requested further comment on the "interplay between V2V and

---

saving lives on our roadways . . . . V2V and automated vehicle technologies each hold great potential to make our roads safer, and when combined, their potential is untold." (quoting NHTSA Administrator Mark Rosekind)).

46. *See* NAT'L SCI. & TECH. COUNCIL, EXEC. OFFICE OF THE PRESIDENT, PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE 18 (2016), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites /ostp/NSTC/preparing_for_the_future_of_ai.pdf [https://perma.cc/W7CN-URFB]; EXEC. NAT'L SCI. & TECH. COUNCIL, OFFICE OF THE PRESIDENT, THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN 9 (2016), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/ NSTC/national_ai_rd_strategic_plan.pdf [https://perman.cc/V7MX-NWR8].

47. Barack Obama, *Barack Obama: Self-Driving, Yes, but Also Safe*, PITTSBURGH POST-GAZETTE (Sept. 19, 2016, 8:00 PM), http://www.post-gazette.com/opinion/Op-Ed/2016/09/19/Barack-Obama-Self-driving-yes-but-also-safe/stories/201609200027 [https://perma.cc/Z3QL-4N2P]. *See generally The White House Frontiers Conference*, (Oct. 13, 2016), http://frontiersconference.org [https://perma.cc/BN3T-VY39].

48. U.S. DEP'T OF TRANSP., NHTSA ISSUES NOTICE OF PROPOSED RULEMAKING AND RESEARCH REPORT ON VEHICLE-TO-VEHICLE COMMUNICATIONS 3 (2016), http://www.safercar.gov/v2v/pdf/V2V_NPRM_Fact_Sheet_121316_v1.pdf [https://perma.cc/KBK8-E8J2]. "Light vehicles" are defined in the NPRM to include "passenger cars, vans, minivans, sport utility vehicles, crossover utility vehicles and light pickup trucks with a gross vehicle weight rating (GVWR) less than or equal to 10,000 pounds." Federal Motor Vehicle Safety Standards; V2V Communications, 82 Fed. Reg. 3854, 3860 n.14 (proposed Jan. 12, 2017) (to be codified at 49 CFR pt. 571), https://www.transportation.gov/briefing-room/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands [https://perma.cc/5ZGF-ZRDY].

49. *See U.S. DOT Advances Deployment of Connected Vehicle Technology*, *supra* note 45.

50. U.S. DEP'T OF TRANSP., *supra* note 48, at 1.

51. *See U.S. DOT Advances Deployment of Connected Vehicle Technology*, *supra* note 45.

52. *Id.* at 3.

53. *Id.*

autonomous technologies."[54] The NPRM acknowledges the privacy risk inherent to data-driven cars and prohibits V2V transmissions from including "data directly identifying a specific private vehicle or individual regularly associated with it, or data reasonably linkable or linkable, as a practical matter, to an individual."[55] Given that "public acceptance" of a technology is a precondition to any regulation NHTSA may set according to the Safety Act,[56] the regulation emphasizes the importance of protecting privacy in any future regulation not only as a normative consideration but as a condition precedent, because consumers will likely not accept tracking practices they feel are too privacy invasive.[57] In another indication of the agency's focus on data-driven vehicles and the privacy risks they create, NHTSA held a workshop with the Federal Trade Commission to examine the privacy ramifications of data-gathering vehicles.[58]

The capacity of modern vehicles to collect information will be driven by market enthusiasm for autonomous vehicle technology, which depends on data collection. But it may also be incentivized by future regulatory requirements. In its Federal Automated Vehicles Policy, NHTSA indicated that its future regulations may ultimately require data collection by manufacturers.[59] Although the Policy emphasizes the importance of manufacturers' adherence to basic consumer privacy principles,[60] it does not make clear precisely what information must be collected, a point noted by commenters like the ride-sharing company, Lyft.[61] Other commenters raised similar concerns about the lack of clarity surrounding what information would be collected and how consumers could control or limit that collection.[62]

---

54. Federal Motor Vehicle Safety Standards; V2V Communications, 82 Fed. Reg. at 3866.

55. *Id.* at 3904.

56. *See id.* at 3920.

57. *See id.*

58. *See* Press Release, Federal Trade Commission, FTC, NHTSA to Conduct Workshop on June 28 on Privacy, Security Issues Related to Connected, Automated Vehicles (Mar. 20, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-nhtsa-conduct-workshop-june-28-privacy-security-issues [perma.cc/6QU4-ES4K].

59. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 1, at 17.

60. *See id.* at 19.

61. *See* Robert Grant, Lyft, Comment Letter on Federal Automated Vehicles Policy (Nov. 22, 2016), https://techcrunch.com/2016/11/17/lyft-wants-more-explicit-protection-of-consumer-data-from-nhtsa-on-self-driving [https://perma.cc/96U7-GYB2].

62. *See, e.g.*, Leonid Reyzin et al., Center for Democracy & Technology, Comment Letter on Proposed Rule Federal Motor Vehicle Safety Standards; V2V Communications 1 (Apr. 12, 2017), https://www.ftc.gov/system/files/documents /public_comments/2017/04/00008–140526.pdf [http://perma.cc/35MJ-KVRQ] ("Our concern is that the privacy protections currently proposed for V2V communications may be easily circumvented by any party determined to perform large-scale real-time tracking of multiple vehicles at once. This poses a serious costs [sic] for both individual privacy and society at large, and we caution that the proposed privacy statement does not adequately disclose these threats to consumers."); Lauren Smith, Future of Privacy Forum, Comment Letter on Proposed Rule Federal Motor Vehicle Safety Standards; V2V Communications 4–6 (Apr. 12, 2017), https://fpf.org/wp-content/uploads/2017/04/FPF-Comments-on-V2V_041217_Final.pdf [https://perma.cc/6WRG-5E4U] (noting concerns about the opacity of privacy policies governing the use of V2V data, and the risk of third-party access to BSM data).

Of course, the kind of information that regulators mandate be collected and the type of consumer information that is the most privacy invasive may not always overlap. Requiring that information on tire pressure be collected likely implicates little (if any) significant privacy interest. But requiring the collection of locational information very much does, and as long as there is some overlap—or worse, the extent of the overlap is undefined—the risk to individual privacy is still significant. In its guidance explaining the use of DSRC, NHTSA notes that "[p]rivate information from electronic sensors in vehicles and devices can also be transmitted over DSRC to provide better traffic and travel condition information to travelers and transportation managers."[63] This capability would seem to obviate the agency's assurance that V2V systems will not "collect, broadcast or share information linked or linkable, as a practical matter, to individuals or their vehicles."[64] Several commenters raised similar concerns that the proposed standards underestimate the privacy risks they create, because, for example, pervasive tracking could still be possible by linking a vehicle's BSMs to identified cryptographic certificates[65] or gleaning metadata from BSMs,[66] and the proposed privacy statement V2V systems would require fails to adequately convey how severely BSM information could be misused.[67]

Although the full impact of NHTSA's final V2V rule remains to be seen, mandated V2V requirements, guidance for the development of highly-automated vehicles, and other federal efforts to spur the development of autonomous and connected vehicle technology will likely accelerate its adoption and use. Even without governmental motivation, automated and connected vehicle technology increasingly dominates the marketplace. As cars are increasingly driven by data, this sea change will produce concomitant results for individual privacy rights. The more information is collected, the more it may reveal about the driver, to a degree that directly implicates the "persons, houses, papers, and effects"[68] the Framers intended to shield from unreasonable government intrusion.

---

63. U.S. DEP'T OF TRANSP., DEDICATED SHORT-RANGE COMMUNICATIONS (DSRC): THE FUTURE OF SAFER DRIVING 6 (2016), http://www.its.dot.gov/factsheets/pdf/JPO-034_DSRC.pdf [https://perma.cc/5G52-WFH8].

64. U.S. DEP'T OF TRANSP., *supra* note 48, at 4.

65. *See, e.g.*, Reyzin et al., *supra* note 62, at 4–5 (noting that BSMs will be linkable to vehicles through the certificate rotation process, as well as through other message content); Lee Tien et al., Electronic Frontier Foundation, Comment Letter on Proposed Rule Federal Motor Vehicle Safety Standards; V2V Communications 3 (Apr. 12, 2017), https://www.eff.org/document/eff-comments-nhtsa-re-v2v-notice-proposed-rulemaking [https://perma.cc/FNK6-ZFDJ] ("NHTSA has failed to adequately account for the need to protect privacy against *systematic attempts* that will undoubtedly be made to monitor and record BSMs for the purpose of tracking vehicles.").

66. *See* Tien et al., *supra* note 65, at 4.

67. *See* Reyzin et al., *supra* note 62, at 12 ("A stalking victim would not know, from reading this statement, the very real risk to her safety that the BSM entails. It does not mention other potential uses that we expect BSM collection to be put: collection for the purposes of vehicle repossession, blackmail, domestic disputes, mass surveillance, commercial espionage, organized crime, burglary, or stalking.").

68. U.S. CONST. amend. IV.

II. THE FOURTH AMENDMENT AND THE AUTOMOBILE EXCEPTION

The Fourth Amendment requires a government actor to secure a warrant based on probable cause before conducting a search or seizure of individuals, their homes, or their belongings.[69] In evaluating whether a search or seizure has taken place, a court will evaluate whether the government action invaded an individual privacy interest, where the defendant has a subjective belief in a privacy interest which society would objectively consider reasonable,[70] including on the basis of a physical trespass.[71] Over time, that standard has incorporated a number of case-specific exceptions to the warrant requirement,[72] though a court may examine the applicability or validity of the exception when the privacy interest is sufficiently significant.[73] A court may still determine that a warrant is required after weighing the individual's interest in privacy against the interest of the government, which includes officer safety or avoiding the destruction of evidence.[74]

Vehicle searches are a well-established exception to the warrant requirement.[75] In general, a vehicle may be searched on the basis of probable cause that contraband may be found in the vehicle or that evidence of a crime will be recovered.[76] An automobile may be stopped on the basis of reasonable, individualized suspicion (a lower degree of justification than probable cause) or on the basis of a traffic violation, and the officer may conduct a search of the vehicle should probable cause become apparent over the course of the stop.[77]

Two related Fourth Amendment principles are also relevant to the automobile exception: the search incident to arrest exception and the doctrine governing the search of a closed container incident to such an arrest. Subsequent to a lawful arrest, an officer may conduct a search of that person and any personal property "immediately associated with the person of the arrestee," including a closed container.[78] When an individual is lawfully arrested from a vehicle, an officer may search the vehicle upon reasonable belief that evidence related to the arrest may be found in the vehicle, or if the person being arrested has not been handcuffed and is close enough to reach the passenger compartment.[79] This includes a warrantless search of a closed container or the passenger compart-

69. *See id.*

70. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

71. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012).

72. *See* Riley v. California, 134 S. Ct 2473, 2482 (2014) (noting that "the label 'exception' is something of a misnomer in this context, as warrantless searches incident to arrest occur with far greater frequency than searches conducted pursuant to a warrant").

73. *See, e.g.*, *id.* at 2485 (holding that the warrant exception for a search incident to a lawful arrest could not be extended to the search of a cell phone).

74. *See id.* at 2488–89.

75. *See, e.g.*, California v. Carney, 471 U.S. 386, 390 (1985).

76. *See id.* at 391–93.

77. *See* United States v. Arvizu, 534 U.S. 266, 273 (2002).

78. *See* United States v. Chadwick, 433 U.S. 1, 15 (1977) .

79. *See* Arizona v. Gant, 556 U.S. 332, 335 (2009).

ment itself.[80]

The automobile exception is premised on the inherent mobility of the vehicle (which could facilitate the suspect's escape, though the exception does not require any further justification of exigency[81]), the diminished expectation of privacy due to the pervasive regulation of automobiles, and the distinction between an automobile and a home, an area traditionally afforded strong protections under the Fourth Amendment.[82] If the officer has probable cause to search the vehicle, he also has probable cause to search closed containers in the car, such as a glove compartment; however, in the reverse scenario, probable cause to search only containers within the car would not give the officer probable cause to search the entire automobile.[83] After *Riley*, discussed *infra* section IV.A., a cell phone is not subject to the closed container designation or to the search incident to arrest exception.[84] The probable cause to search the vehicle incident to arrest can also justify a search once the car has been impounded because the car need not be searched at the exact moment that the arrest takes place.[85]

Although it is less relevant to traditional automobiles, the third-party doctrine is another part of Fourth Amendment canon that is undermined by the privacy risks inherent to data-driven vehicles. The third-party doctrine dictates that a person does not have a reasonable expectation of privacy in information disclosed to another party because that second person could be expected to give the information to law enforcement.[86] While the logic is straightforward, the principle has become increasingly unworkable as information is increasingly relayed from computers or smartphones, through a service provider, to be stored on cloud servers, all of which may be in different locations and are controlled by multiple parties. Under *United States v. Miller* and *Smith v. Maryland*, the seminal cases establishing the doctrine, an individual does not have a reasonable expectation of privacy in the bank records she uses to complete a transaction (because that information is relayed to the bank), or the phone number she dials (because that information is relayed to the phone company).[87]

---

80. *See id.* at 337.

81. *See* United States v. Nixon, 918 F.2d 895, 903 (11th Cir. 1990) ("[T]he mobility of an automobile is exigency enough.").

82. *See, e.g.*, California v. Carney, 471 U.S. 386, 391–93 (1985).

83. *See* United States v. Ross, 456 U.S. 798, 821 & n.28 (1982).

84. *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014).

85. *See* Florida v. Meyers, 466 U.S. 380, 382 (1984) (per curiam).

86. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

87. *See* David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1110 (2014) (describing a relational approach to privacy as "one reason why the Supreme Court has been wrong to declare that an individual can have no 'legitimate expectation of privacy' in anything shared voluntarily with someone else—and one reason the Court has been right to ignore that principle when it protects, for example, the privacy of a telephone call" (citing *Smith*, 442 U.S. 735; *Miller*, 425 U.S. 435)).

III. APPLYING THE FOURTH AMENDMENT TO AUTONOMOUS VEHICLES

The impact of a new technology on a constitutional protection presents two relevant veins of inquiry: how existing protections may be weakened through the mindless application of analogous precedent to technological facts, and how, regardless of normative considerations, a court is most likely to apply existing precedent to new technology.

An autonomous vehicle's mobility no longer necessarily depends on the choices of the individual occupying it. This seems to demand a radically different application of the Fourth Amendment's automobile exception, which is partially predicated on the likelihood that a vehicle could exit the scene or pose a risk to officer safety. But the exception's mobility rationale is a binary threshold, not a qualitative assessment: if the entity being searched is theoretically capable of movement, it may be searched without a warrant.[88] Autonomous vehicles will qualify for the automobile exception, and it is unlikely that any qualitative consideration—even that the car can drive itself—will obviate that justification. Despite the radically different considerations presented by autonomous vehicles, these considerations will be insufficient to convince a court to overturn such thoroughly entrenched precedent.

Although the mobility basis represents a weak justification for a new Fourth Amendment approach to autonomous vehicles, the privacy implications of the data gathered by these vehicles is far stronger and contradicts the validity of categorically extending the automobile exception to autonomous vehicles. The privacy interests inherent to the vast amounts of data collected by these vehicles are more significant than what the justices who devised the automobile exception could have contemplated. When weighed against government interest, the result should be that a warrant is required to search vehicle data.

The following Part will discuss the mobility component of the automobile exception, why the significant privacy interest created by the data generated and collected by autonomous cars should merit a warrant before search, and illustrate why *Jones*, *Riley*, and ensuing developments could support such a result.

A. AUTONOMOUS VEHICLES AND THE MOBILITY RATIONALE

The impact of a car's mobility on the automobile exception seems fairly straightforward—if, subsequent to a lawful stop or arrest, there is probable cause that evidence of an ongoing crime is located within something, it seems logical to afford an officer additional leeway when that thing is mobile and could either facilitate the escape of the evidence, contraband, and suspects, or pose a safety risk to the officer.[89] However, the applicability of the exception

88. *See* California v. Carney, 471 U.S. 386, 391 (1985) ("Even in cases where an automobile was not immediately mobile, the lesser expectation of privacy resulting from its use as a readily mobile vehicle justified application of the vehicular exception.").

89. *See* Arizona v. Gant, 556 U.S. 332, 346–47 (2009) (discussing the safety rationale in warrantless vehicle search cases).

does not depend on strict exigency or the objective likelihood that the vehicle may move at a given moment—merely a vehicle's inherent mobility is sufficient.[90] Because mobility is a threshold consideration rather than a qualitative assessment, the impact of the autonomous vehicle on the automobile exception may seem functionally moot. Plausible arguments could be made that autonomous vehicles are more or less "mobile" than their counterparts that are manually controlled, and there is a range of functionality that qualifies as "autonomous."[91] An automated vehicle could be required to contain software making it remotely controllable by law enforcement; this seems like an extreme possibility, but it could undermine the need for an automobile exception because it would largely negate the exigency rationale. Conversely, automated vehicles could provide support for the mobility rationale—a car that can be controlled remotely would seem to present more of a mobility risk than a mobile home[92] or an unhitched trailer which, without a car to pull it, cannot inherently move.[93]

Automated vehicles are thus unlikely to compel a categorical reconsideration of the automobile exception based on a qualitative difference in mobility, even though the most seemingly radical characteristic of these vehicles is their mobility. The simple fact that a vehicle could be mobile in some way, and not the likelihood that it will become mobile, is what matters here, and highly automated and autonomous vehicles will meet that threshold. The technology here is fundamentally different, but the aspect of the technology that seems the most revolutionary—that cars can be independently mobile—is unlikely to have a practical impact on the automobile exception or a corresponding impact on individual privacy.

B. AUTOMATED VEHICLES AND INFORMATION GENERATED

The vast amounts of data that automated vehicles collect may seem like one of the least radical aspects of the technology. Most cars have had Event Data Recorders (EDRs) since the mid-1990s, for example,[94] and GPS tracking in the cell phones drivers carry is also not radically new. But it is the vast amount of information that autonomous vehicles create and collect, information that would be searchable without a warrant, that creates the strongest argument for reconsideration of the automobile exception as applied to connected and automated vehicles.

---

90. *See* Pennsylvania v. Labron, 518 U.S. 938, 940 (1996) (per curiam) ("If a car is readily mobile and probable cause exists to believe it contains contraband, the Fourth Amendment thus permits police to search the vehicle without more.").

91. *See supra* notes 36–39 and accompanying text.

92. *See Carney*, 471 U.S. at 394 (holding a motor home qualifies for the automobile exception).

93. *See* United States v. Navas, 597 F.3d 492, 499 (2d Cir. 2010).

94. *See* FUTURE OF PRIVACY FORUM, THE CONNECTED CAR AND PRIVACY: NAVIGATING NEW DATA ISSUE 3 (2014), https://fpf.org/wp-content/uploads/FPF_Data-Collection-and-the-Connected-Car_November 2014.pdf [https://perma.cc/H3XF-HS6P].

The locational data recorded by connected cars can be used to trace an intimate portrait of an individual's habits, beliefs, and patterns through locational tracking, including whether the individual is having an affair, attending church, buying a gun, undergoing an abortion, frequenting Alcoholics Anonymous meetings, or belonging to a political organization.[95] The information can be more directly personal rather than inferentially personal.[96] Locations are often the most revealing in the aggregate, but data such as contacts, call logs, and other files could be more directly revealing and would be accessible when a driver syncs her mobile device to the car. A vehicle that syncs to a device located in the driver's home, such as Amazon's Alexa,[97] could also implicate one of the most heavily protected privacy interests in Fourth Amendment law: the privacy of the home.

The information generated by connected and automated vehicles is also where the third-party doctrine comes into play. Applying the status quo to vehicle data would preclude the driver's reasonable expectation of privacy once the data is transmitted to a third party, such as a service provider. But the criticism of the third-party doctrine raised in other contexts—that it is ill-suited to the digital age, in which nearly all communications are unavoidably relayed through a third party by default—is strengthened by the accelerated development of data-driven vehicles. The third-party doctrine does not obviate the rationale for requiring a warrant for vehicular data. In fact, it is the privacy invasions that warrantless access to that data would permit that create an additional example of the doctrine's weaknesses in the modern age, and an even stronger argument for its obsolescence.

Finally, in the context of a radically new technology, it is important to consider not only the kind of information gathering that is possible now, but what may also be reasonably possible in the future. Features like the Corvette Stingray's in-cabin recording[98] engender the creation of incriminating evidence, and that kind of capability can only be expected to continue developing in unexpected ways. Although a wholesale reimagining of the automobile exception may not be necessary (or plausible), law enforcement should be required to

---

95. *See* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009))); U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 21, at 5–6 ("Location data may be used to form a comprehensive record of an individual's movements and activities. If disclosed or posted, location data may be used by criminals to identify an individual's present or probable future location, particularly if the data also contain other personally identifiable information . . . . In addition to information related to a crime, the location data collected by law enforcement may reveal potentially sensitive destinations, such as medical clinics, religious institutions, courts, political rallies, or union meetings.").

96. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1170 (2015).

97. *See, e.g.*, Garun, *supra* note 18.

98. *See supra* note 29 and accompanying text.

get a warrant to search the data stored by vehicles, just as they would be required to obtain one for a cell phone.[99] The privacy interest in a person's GPS location, the contents of his or her phone, footage from inside his or her vehicle, and whatever else tomorrow's cars may make possible is too significant for any lesser degree of Fourth Amendment protection to suffice.

IV. *RILEY*, *JONES*, AND THE PRIVACY IMPLICATIONS OF A COMPUTER ON WHEELS

The Fourth Amendment is no stranger to new technology,[100] and over the years the Supreme Court has rendered a number of decisions that signal awareness of technology's impact on privacy and the protections that the Fourth Amendment provides for it.[101] And although the Court has not decided a case involving an autonomous or connected vehicle, two of its recent cases, *Riley v. California* and *United States v. Jones*, included highly relevant Fourth Amendment analysis, namely the privacy interest in the modern smartphone, a discussion of the smartphone and the automobile exception, and the reasonable expectation of privacy at issue in the collection of GPS data.[102] The application of those two cases to vehicle data and the Court having granted certiorari in a case that could result in its overruling the third-party doctrine further demonstrate both the feasibility of a new standard for vehicular data, as well as judicial cognizance of the privacy risk that blithe application of existing standards could create.

A. *RILEY V. CALIFORNIA*

In *Riley,* the Supreme Court held that the privacy interests implicated by the modern cell phone are too significant for the phone to be treated as a closed container subject to a warrantless search incident to arrest.[103] When a law enforcement official conducts a search incident to a lawful arrest and locates a cell phone, he will typically need a warrant to conduct a search of the phone.[104] The majority opinion distinguished *Chimel v. California*,[105] which authorized

99. *See infra* Section IV.A.

100. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (arguing that the Supreme Court maintains a status quo degree of Fourth Amendment protection in response to disruptive new technologies and positing judicial delay as a stabilizing factor).

101. *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (holding that the privacy interests implicated by the modern cell phone make the container exception of the search incident to arrest doctrine inapplicable under the Fourth Amendment); United States v. Jones, 565 U.S. 400, 404 (2012) (holding that attaching a GPS to defendant's car constituted a Fourth Amendment search and discussing the impact of GPS monitoring on a reasonable expectation of privacy in the modern era); Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the use of sense-enhancing technology to obtain evidence that would be unobtainable without physical intrusion constitutes a Fourth Amendment search when the technology is not in the public use).

102. *See Riley*, 134 S. Ct. at 2489; *Jones*, 565 U.S. at 428–29 (Alito, J., concurring in the judgment).

103. *See Riley*, 134 S. Ct. at 2485.

104. *See id.*

105. 395 U.S. 752 (1969).

warrantless searches of vehicles incident to arrest when the arrestee is unsecured and within reach of the passenger compartment, and *Arizona v. Gant*,[106] which permitted the warrantless search of a vehicle's passenger compartment when it is reasonable to believe it could contain evidence of the crime that led to the arrest.[107] Writing for the majority, Chief Justice Roberts explicitly rejected extending *Gant* to cell phones found in a vehicle, noting that the *Gant* holding relied on Fourth Amendment considerations unique to the vehicle context—namely, the reduced expectation of privacy due to the pervasive regulation of vehicles, and heightened law enforcement needs.[108] The majority also found that the smartphone may contain all manner of incriminating evidence that is entirely irrelevant to the basis for the vehicular stop, a disproportionately severe invasion of privacy when weighed against the government's interests.[109] Although the physical search of a vehicle and its closed containers necessarily will produce a more limited range of evidence, the modern cell phone will not, particularly considering the added complication of files uploaded from a cell phone to the cloud.[110] A smartphone search provides access to the information the phone stores locally, such as the owner's texts, but it can also provide access to information stored elsewhere through a mobile application for a cloud service like Google Drive or Dropbox. A smartphone search thus poses no logical limiting principle and—depending on its capabilities—the modern-day vehicle could be similarly unlimited in the kind of information it provides.[111]

B. *UNITED STATES V. JONES*

Chief Justice Roberts's opinion in *Riley* also cites *Jones*, noting that the GPS capabilities of the modern cell phone enable the same kind of panoptical surveillance of the driver enabled by the attachment of a tracker to a vehicle.[112] In *Jones*, the Supreme Court held that the attachment of a GPS tracker to the defendant's vehicle constituted a physical trespass and thus an unreasonable and unconstitutional search.[113] The majority opinion, written by Justice Scalia, explicitly declines to decide the case on the basis of the privacy interest in the GPS data, opting instead to base the ruling on the privacy interest implicated by the physical integrity of the vehicle and the trespass that took place when the officer placed the GPS tracker on the undercarriage of the vehicle.[114]

The two concurrences, authored by Justices Sotomayor and Alito, addressed the futility of focusing on physical trespass as surveillance methods become

106. 556 U.S. 332 (2009).
107. *See Riley*, 134 S. Ct. at 2485–86, 2492.
108. *Id.* at 2492.
109. *See id.* These interests include the risk of evidence spoliation and officer safety.
110. *See id.* at 2491.
111. *See supra* Part I.
112. *See Riley*, 134 S. Ct. at 2490) (Sotomayor, J., concurring) (citing United States v. Jones, 565 U.S. 400, 415 (2012)).
113. *See* 565 U.S. at 404.
114. *See id* at 404–06.

ever more intangible.[115] The concurrences also seemed to endorse mosaic theory, the idea that a number of individual steps, which separately cannot be considered a search under the Fourth Amendment, can collectively be considered a search due to the depth of the privacy interest involved.[116] Justice Sotomayor's concurrence focused on the sensitivity of the information that could be gleaned from GPS surveillance,[117] while Justice Alito's concurrence focused on the reasonableness of the length of the surveillance.[118] Acknowledging how revealing GPS data can be in the aggregate is crucial here—although autonomous vehicles, as a class, may not always have the capability to store the kind of sensitive data that Chief Justice Roberts found so persuasive in *Riley*, they will require enormous amounts of mapped information to function.[119] Whether an autonomous vehicle's system is closed or interconnected,[120] or allows for the kind of internet use and file storage that some connected cars do,[121] at a minimum, some manner of locational data will be involved.

C. APPLYING *JONES* AND *RILEY* TO VEHICLE DATA

These two holdings sidle tantalizingly close to the most intriguing Fourth Amendment question elicited by modern vehicles without providing a reliable answer: how does the Fourth Amendment protect the privacy interest implicated by automated and connected vehicles, which are essentially vehicular cell phones? The *Jones* concurrences' discussion of geolocational tracking enabled by cellphones[122] and the *Riley* discussion of the automobile exception[123] suggest a complex analytical overlap.[124] The *Jones* Court was perturbed by the

115. *See id.* at 415 (Sotomayor, J., concurring); *id.* at 426–27 (Alito, J., concurring in the judgment).

116. *See id.* at 415 (Sotomayor, J., concurring) ("In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."); *id.* at 430 (Alito, J., concurring in the judgment). *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (defining, discussing, and rejecting the viability of the approach).

117. *See* 565 U.S. at 415 (Sotomayor, J., concurring).

118. *See id.* at 430 (Alito, J., concurring in the judgment).

119. *See* Glancy, *supra* note 36, at 636–37.

120. *See supra* Section I.A.

121. *See* Ha, *supra* note 27 (discussing a Tesla model with a built-in web browser).

122. *See* 565 U.S at 428–29 (Alito, J., concurring in the judgment) ("Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users . . . . For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining ('crowdsourcing') the speed of all such phones on any particular road. Similarly, phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements." (internal footnotes omitted)).

123. *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014).

124. *See* Glancy, *supra* note 36, at 665 (discussing the application of *Riley* and *Jones* to autonomous vehicles, and noting that "[l]aw enforcement interaction with first generation autonomous cars may also

extent to which pervasive tracking, even when intangible, could invade individual privacy and how a rigid application of search and seizure doctrine seemed to produce a perverse result unintended by the drafters of the Fourth Amendment or even the drafters of that opinion.[125]

The type of information the vehicle may record directly implicates the strength of the privacy interest in it, and it is unclear whether the Court would only be persuaded by the type of content Chief Justice Roberts found particularly persuasive in *Riley*, such as information from a synced mobile device or whether locational information would suffice. In articulating why a smartphone invokes a heightened degree of privacy protection, the *Riley* opinion "qualitatively" distinguishes the kinds of records that a smartphone is capable of retaining, such as internet browsing history, from physical records.[126] Yet in making that distinction, Chief Justice Roberts includes GPS tracking information in the category of information worthy of protection, rather than distinguishing it as a less-protected form of information, and cites Justice Sotomayor's *Jones* concurrence for the proposition.[127] Between physical records, the contents of a smartphone, and GPS data, the *Riley* opinion highlights the latter two as both inherently implicating Fourth Amendment privacy interests. This is a logical result, but not an insignificant one; had the *Riley* opinion cabined the significance of either smartphone content or GPS data, it could have implied that a warrant was required for certain kinds of vehicle information, but not others.

The underlying assumption of Chief Justice Roberts' distinction between the privacy interests inherent to a smartphone and the government interests inherent to the automobile exception is the idea that those two contexts are separable, a distinction that is obviated by the informational capacities of the modern vehicle.[128] He contrasts the limits of the evidence that can be located in the

---

generate some novel Fourth Amendment search and seizure issues" such as "whether an autonomous vehicle's systems are at least as worthy of protection against warrantless law enforcement searches as those of a smart phone").

125. *See* Jones, 565 U.S. at 420 (Alito, J., concurring in the judgment) ("The Court argues—and I agree—that 'we must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."' But it is almost impossible to think of late–18th-century situations that are analogous to what took place in this case. (Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?)." (internal citations omitted)).

126. *See Riley*, 134 S. Ct. at 2489–91.

127. *See id.* at 2490 ("An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns . . . . Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

128. *See id.* at 2492 ("*Gant* relied on 'circumstances unique to the vehicle context' to endorse a search solely for the purpose of gathering evidence. Justice Scalia's *Thornton* opinion, on which *Gant* was based, explained that those unique circumstances are 'a reduced expectation of privacy' and 'heightened law enforcement needs' when it comes to motor vehicles. For reasons that we have explained, cell phone searches bear neither of those characteristics.") (internal citations omitted)).

containers of a car, with the limitless possibilities of what a cell phone might contain:

> An individual pulled over for reckless driving might have evidence on the phone that shows whether he was texting while driving. The sources of potential pertinent information are virtually unlimited, so applying the *Gant* standard to cell phones would in effect give "police officers unbridled discretion to rummage at will among a person's private effects."[129]

Permitting the warrantless search of an automated vehicle with the capabilities of a smart phone would enable exactly that. In addition, similar technological developments have made it far easier for an officer to remotely acquire a warrant from the scene of the arrest, undercutting the exigency rationale for a warrantless search.[130]

As noted above, both autonomous vehicles and connected cars depend upon data collection to operate, and companies have considerable incentive to continue manufacturing cars that can collect and subsequently monetize data—not to mention retain that data for government inspection.[131] The *Jones* Court noted how quickly geolocational tracking could create a detailed portrait of an individual's life, and the *Riley* Court noted the modern cell phone's resemblance to a "minicomputer."[132] Modern cars increasingly implicate the aspects of Fourth Amendment doctrine questioned by both cases: the privacy interests inherent to the smart phone, a context that does not allow for Fourth Amendment exceptions, and the Fourth Amendment privacy concerns of intangible surveillance, particularly GPS tracking in a vehicle.

That analysis is further complicated (and perhaps further highlighted as obsolete) by the generational shift from individually-owned vehicles to the widespread use of ride-sharing services. Companies like Uber and Lyft have made considerable efforts to incorporate autonomous capabilities into their fleets, and ride sharing has become an increasingly large part of how Americans get around.[133] An expectation of privacy in a temporarily occupied autonomous vehicle is unlikely to be deemed objectively reasonable, even if the defendant subjectively believed that it was. Although that would not be an unfair outcome,

---

129. *Id.* at 2492 (quoting Arizona v. Gant, 556 U.S 332, 345 (2009)).

130. *See id.* at 2492 (noting that in one Kansas county "police officers can e-mail warrant requests to judges' iPads [and] judges have signed such warrants and e-mailed them back to officers in less than 15 minutes" (citing Missouri v. McNeely, 133 S. Ct. 1552, 1573 (2013) (Roberts, C.J., concurring in part and dissenting in part))).

131. *See supra* Part I.

132. *See Riley*, 134 S. Ct. at 2489 ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

133. *See* MCKINSEY & CO., *supra* note 30, at 10 (noting that "[b]y 2030, one out of ten cars sold could be a shared vehicle").

it may bear revisiting if a significant portion of the population starts to rely on corporate-owned shared vehicles as opposed to individually owned vehicles, a development that may not be far off.[134] The shared-vehicle passenger would also most likely not have a protected interest in privacy under the property theory that captured a majority in *Jones*.[135] Ride sharing is increasing, and ride-sharing companies are at the forefront of developments in autonomous vehicles, making the privacy interest in an autonomous vehicle used by such a company an increasingly relevant vein of inquiry.[136]

Jones and *Riley* also contained reservations about the third-party doctrine, illustrating how the privacy implications of vehicle data could serve as further ammunition for the doctrine's demise. Although the third-party doctrine is often used to undercut an asserted privacy interest, *Riley* uses the factual basis for the third-party problem—that a smartphone can access files located remotely, rather than on the device—to argue against the government's interest in conducting a warrantless search, and for a stronger privacy interest. A smartphone connected to a cloud service presents two arguments relevant to an individual's privacy in her device: one strengthening the argument for a strong privacy interest in a cloud-enabled device and one weakening it. On the one hand, a smartphone's ability to connect to a cloud service that could provide access to all of an individual's files, located anywhere, creates a strong privacy interest. On the other hand, a cloud service's requirement that the individual entrust her information to a third party, the provider storing her information on a remote server, undermines that interest under the current approach.

Chief Justice Roberts chose the former. In distinguishing *Chimel*, Chief Justice Roberts proffered cloud computing as a further basis for why the closed container exception is inapplicable to smartphones—not because the suspect has a diminished expectation of privacy, but because it would be illogical to extend the search incident to arrest exception to files located on a server at an unknown location.[137] He highlighted the strength of the privacy interest and the risks of abuse due to the lack of a limiting principle concerning what could be searched, rather than focusing on the third-party issue.[138] This is a notable approach because cloud computing is far more often defined by the third-party problem

134. Glancy, *supra* note 36, at 625–26 ("When consumers are asked about the application of autonomous cars most people want to be available first, consumers often choose on-demand personal mobility services . . . . Such a transportation-as-service approach is potentially transformative in changing expectations about personal mobility away from the purchase of a machine that one owns, maintains, and drives.").

135. *See, e.g.*, United States v. Jones, 565 U.S. 400, 426 (2012) (Alito J., concurring) (noting the artificial distinctions that would result from state variations in property laws under the majority's trespass-based approach).

136. *See* Grant, *supra* note 61; Mike Isaac, *Uber Bets on Artificial Intelligence with Acquisition and New Lab*, N.Y. TIMES. (Dec. 5, 2016) http://www.nytimes.com/2016/12/05/technology/uber-bets-on-artificial-intelligence-with-acquisition-and-new-lab.html [https://nyti.ms/2h5GX4p].

137. *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014).

138. *See id.*

than as evidence of a stronger privacy interest. Of course, cloud computing does not necessarily require entrusting files to a third party because a defendant could maintain a private server in her home. But in the overwhelming majority of cases, cloud computing does involve the individual entrusting his or her information to a third party, thus invoking the third-party doctrine and making Chief Justice Robert's distinctive approach to the issue in *Riley* even more significant. Further, Justice Sotomayor's *Jones* concurrence questions the continued utility of the third-party doctrine outright.[139]

Data-driven vehicles also raise unique third-party doctrine problems, in addition to those that are equally applicable to other forms of technology. Different vehicles will rely on communications with outside providers to different degrees. Judicial sanction of a reasonable expectation of privacy might then depend on whether the car operates on a closed system,[140] or if it relies on an external carrier.[141] That the validity of a driver's privacy interest may depend on whether Justice Scalia's "tiny constable" is riding in a Jeep, a Waymo car, or a Lyft demonstrates the need to reconsider the continued utility of those doctrines.[142]

D. FURTHER DEVELOPMENTS

Several recent cases shed light on how a court might approach the Fourth Amendment implications of data-driven vehicles.

In *State v. Worsham*, a Florida district court held that the EDR data from the defendant's vehicle implicated a reasonable expectation of privacy such that a warrant was required before law enforcement could access it.[143] The court's basis for the privacy interest was that the EDR data is not exposed to the public and is "difficult to extract and interpret."[144] Although EDR data is not as personal as the type of data stored by cell phones, the majority found *Riley*'s approach to privacy in electronic data to be relevant to its analysis because "[j]ust as cell phones evolved to contain more and more personal information [and] . . . electronic systems in cars have gotten more complex, the data recorders are able to record more information."[145] The court also distinguished a contradictory holding, *People v. Diaz*,[146] on the basis that the decision relied on the third-party doctrine.[147]

---

139. *See* United States v. Jones, 565 U.S. 400, 415 (2012).

140. Glancy, *supra* note 36, at 641 (noting that automated vehicles may or may not be connected vehicles, such as the initial designs for the Google Car, which "avoided use of wirelessly communicated information, aside from GPS").

141. *See supra* note 17.

142. *Jones*, 565 U.S. at 420.

143. *See* No. 4D15-2733, 2017 WL 1175880, at *5 (Fla. Dist. Ct. App. Mar. 29, 2017).

144. *Id.* at *4.

145. *Id.*

146. 153 Cal. Rptr. 3d 90 (Cal. Ct. App. 2013).

147. *See Worsham*, 2017 WL 1175880 at *5 (noting that the Court has "moved away from the *Smith* rationale," and that the *Diaz* court's reliance on the third-party doctrine was "misplaced" because it

Worsham has several implications. The notion that difficulty of extraction and interpretation ought to increase a reasonable expectation of privacy could apply to the more complex and inscrutable data recorded by vehicles, such as V2V basic safety messages or forms of mapping data that are not easily accessed or understood. In addition, information that could be easily accessed and interpreted, such as synced text messages, locational tracking information, or contacts, are described by the *Worsham* court as meriting greater privacy protection under *Riley* and *Jones*.[148] Though the justifications may be competing, the opinion nevertheless offers multiple rationales for future courts to require a warrant for various kinds of vehicle information, whether the data is more inscrutable and difficult to access (for example, lidar data or V2V basic safety messages) or more accessible, yet more immediately sensitive and revealing (such as GPS data or information synced from a smartphone).

Finally, the Supreme Court recently granted certiorari in *Carpenter v. United States*, a case that could result in the Court's overruling of the third-party doctrine.[149] The issue in *Carpenter* involves the level of protection the Fourth Amendment affords for historical cell-site information acquired from a service provider—whether a Stored Communications Act (SCA) subpoena is sufficient, or if a warrant based on probable cause is required. Although the Fourth Amendment provides no protection for electronic communications and records held by a third-party provider, the SCA requires a subpoena before law enforcement can access certain kinds of information.[150] However, the evidentiary standard for that subpoena is akin to reasonable suspicion—a less demanding standard than probable cause.[151] If the Supreme Court were to find that there was a reasonable expectation of privacy in historical cell site information, for example, warrantless access to that information would violate the Fourth Amendment.

Although *Carpenter* concerns law enforcement access to historical cell site information, rather than vehicle data, the scope of the review sought is directly relevant to the vehicle data context, and a ruling for the defendants would support the argument that a warrant should be required to access vehicular information. The case would not change the automobile exception, but a more privacy-protective rule governing information passed through third parties could

---

ignored both the *Jones* majority's trespass test, and the sensitivity of the information recorded as noted by Justice Sotomayor).

148. *See id.* at *4.

149. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 2017 WL 2407484 (June 5, 2017) (No. 16-402); *see also* Orin Kerr, *Supreme Court Agrees to Hear* 'Carpenter v. United States,' *The Fourth Amendment Historical Cell-Site Case*, WASH. POST (June 5, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/05/supreme-court-agrees-to-hear-carpenter-v-united-states-the-fourth-amendment-historical-cell-site-case/ [https://perma.cc/AFL3-2HL9].

150. Stored Communications Act, 18 U.S.C. § 2703(d) (2012).

151. The standard is "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.*

still be applied to vehicular data. This would remove one of the obstacles (the third-party doctrine) preventing a court from finding that drivers have a reasonable expectation of privacy in vehicle data. Even a narrower ruling limited to the application of the SCA to certain kinds of records could have a significant impact on vehicle privacy because it would limit law enforcement access to the vehicle data held by service providers, car companies, and others. The ever-growing role of ride-sharing companies, and the vast stores of data they hold about their users,[152] means that even a circumspect, SCA-grounded holding could have a considerable impact on driver privacy.[153]

These are complex considerations, and attempting to augur future holdings from dicta can be a fruitless exercise. Ultimately *Jones* was decided on the basis of trespass, and a future case involving the search of vehicle data will have to reconcile with that standard, in addition to the barriers posed by the longstanding precedent of the automobile exception and the third-party doctrine. However, both *Jones* and *Riley* suggest that a warrant requirement for a search of vehicle data is not only normatively desirable, but also analytically consistent with current law, a suggestion supported by the subsequent application of those cases to EDR data in *Worsham* and the Court's grant of certiorari in *Carpenter*. The privacy interests implicated by vehicle data are categorically distinct from the privacy interests justifying the automobile exception, and requiring a warrant to search vehicle data is a sensible and necessary update of the Fourth Amendment for the digital age.

V. OTHER CONSIDERATIONS

The scope of this Note is narrow—it addresses how the Fourth Amendment's automobile exception should be applied to data-driven vehicles as they exist now or in the proximate future. It concludes that while the mobility rationale is unlikely to compel a wholesale reimagining of the doctrine, the information recorded by such vehicles merits a doctrinal shift to require that law enforcement officials obtain a warrant before searching the vehicle's data. But there are

152. *See generally* Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. (forthcoming 2017) (manuscript at 21–22) (on file with authors), https://dx.doi.org/10.2139/ssrn.2929643 [https://perma.cc/KY4N-DFJ6] (noting "tremendous volume and variety of information about the behaviors of consumers" held by sharing economy firms, and the abuses that can engender, such as Uber's recording a user's location after the ride is completed); *see also* Kate Conger & Darrell Etherington, *Federal Policy for Self-Driving Cars Pushes Data Sharing*, TECHCRUNCH (Sept. 20, 2016), https://techcrunch.com/2016/09/20 /federal-policy-for-self-driving-cars-pushes-data-sharing/ [https://perma.cc/33SF-AMWE] (discussing the amounts of different kinds of data held by car companies).

153. *See* Orin Kerr, *How Self-Driving Cars Could Determine the Future of Policing*, WASH. POST (June 16, 2017), https://www.washingtonpost.com/amphtml/news/volokh-conspiracy/wp/2017/06/16/how-self-driving-cars-could-determine-the-future-of-policing/ [https://perma.cc/XBY3-XRA2] (discussing how the growth of self-driving cars and ride sharing will impact policing strategies, and how *Carpenter* could impact law enforcement access to the detailed records held by companies like Lyft and Uber).

other benefits and drawbacks to the technology that merit consideration. In addition to the possibility that increased use of autonomous technology will decrease traffic fatalities,[154] Dorothy Glancy raises an additional point about the privacy implications of the informational capacities of autonomous vehicles: although they could increase the ability of otherwise immobile individuals, such as the elderly or disabled, to get around, that possibility of increased personal autonomy may come at the expense of diminished privacy for vulnerable groups.[155] In a subsequent article, Glancy also raises the question of whether a warrant would be required before a law enforcement official could remotely control an autonomous vehicle, if such a capability is developed.[156] Joseph Schafer, a scholar specializing in the impact of new technology on policing techniques, argues that autonomous vehicles could mean the end of the pretextual traffic stop, an area of Fourth Amendment jurisprudence that frequently draws criticism for legally enabling warrantless searches that would otherwise be unconstitutional.[157] The information autonomous vehicles collect is just one part of the risks they pose, and the benefits they may also be poised to create.

Applying the automobile exception to autonomous vehicles also highlights a broader dilemma about privacy, technology, and the Fourth Amendment—the uneasy combination of the circular *Katz* test and a digital era that cycles through new privacy norms far too quickly for the law to keep up.[158] As Justice Alito notes in his *Jones* concurrence, the tests depend on the idea that individual privacy expectations are both comprehensive and stable, an assumption that the protean development of new technology consistently belies.[159] Moreover, equating an informed resignation to the inevitability of privacy invasions with apathy toward those invasions would have the perverse result of defining a legitimate privacy interest as whatever a company, or the government, can most effectively

154. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 1, at 5.

155. Glancy, *supra* note 6, at 1186 ("[For disabled persons and the elderly], an autonomous vehicle would provide enhanced personal autonomy and self-determination about when, how, and with whom to travel . . . . Nevertheless, for such users there may be a trade-off with privacy. Being linked with an autonomous vehicle is likely to generate a great deal of personal information about where the user is and what he or she is doing, as well as a comprehensive log of places the user visited. For some potential autonomous vehicle users, relying on an autonomous vehicle could pose a Hobson's choice—either to take this autonomous vehicle mode of personal transport that tracks your every movement, or to have no individual vehicle mobility at all.").

156. Glancy, *supra* note 36, at 665.

157. Robin Washington, *Driverless Cars Are Coming. What Does that Mean for Policing?*, MARSHALL PROJECT (Sept. 29, 2016), https://www.themarshallproject.org/2016/09/29/driverless-cars-are-coming-what-does-that-mean-for-policing#.W1sxqUVls [https://perma.cc/YZX4-7TB5]; *see also* Wayne R. LaFave, *The "Routine Traffic Stop" from Start to Finish: Too Much "Routine," Not Enough Fourth Amendment*, 102 MICH. L. REV. 1843, 1853 (2004).

158. *See generally*, Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015) (calling the *Katz* test a 'phantom doctrine'); *see also* Sklansky, *supra* note 87, at 1071 (articulating the "persistent and growing confusion about the meaning and continuing validity of the 'reasonable expectations of privacy' test" as a "major source of disarray in current Fourth Amendment law").

159. *See* United States v. Jones, 565 U.S. 400, 427 (2012).

disclaim.

Finally, in examining how individual privacy is protected from the autonomous vehicle, the Fourth Amendment is just one aspect of a larger constellation of sector-specific privacy laws. A great deal of focus has been devoted to privacy and safety concerns tied to autonomous vehicles from the consumer protection perspective or from the perspective of anxious companies.[160] And some protections exist for driver information that may extend to the drivers of autonomous vehicles—the Federal Trade Commission's enforcement authority can extend to data security practices and information collection, the Department of Transportation has an overarching mandate over vehicle standards and safety, and individual legislators have raised concerns over protections for drivers in the twenty-first century car.[161]

As noted above, the SCA would also pose a barrier for agents seeking information directly from the provider of information services to a connected vehicle.[162] However, in addition to the many problems the statute poses in other contexts,[163] the SCA would only provide a safeguard for one aspect of the privacy risk posed by vehicular data because it only applies when agents seek vehicular data directly from the provider, as opposed to accessing data from the vehicle itself during a search incident to a vehicle stop, a search incident to arrest, or a search after impoundment. Moreover, the subpoenas enabled by that statute require a lower evidentiary showing than the probable cause a warrant would require. The focus on information collected by private actors, and the front-end standards companies are held to, often dominate the conversation because they are likely the source of both the biggest part of the problem and the most effective solutions.

---

160. *See* Grant, *supra* note 61; MARKEY, *supra* note 31, at 1.

161. *See* Future of Privacy Forum, Comments on Federal Automated Vehicles Policy (Docket No. NHTSA-2016-0090) 4–5 (Nov. 22, 2016), https://fpf.org/wp-content/uploads/2016/11/FPF-Comments-on-DOT-Guidance_112216_Final.pdf [https://perma.cc/QX6W-5SJC] (noting the FTC's authority to regulate unfair and deceptive trade practices, including those related to data privacy and security, and the agency's shared jurisdiction with NHTSA over this aspect of connected and automated vehicles).

162. *See* Stored Communications Act, 18 U.S.C. § 2701 (2012); *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214 (2004) (explaining the definitions of "remote computing service" and "electronic communication service" under the Act); *id.* at 1212–23 (explaining compelled and voluntary disclosure rules under the Act).

163. The SCA is frequently criticized as a poorly written and structured statute that forces calcified definitions onto forms of technology that could not have been predicted by its drafters. *See* Email Privacy Act, H.R. 387, 115th Cong. (2017); Email Privacy Act, H.R. 699, 114th Cong. (2016); *Electronic Communications Privacy Act (ECPA)*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/ecpa/#reform [https://perma.cc/GF8D-WFKV]. *But see* Kerr, *supra* note 162, at 1208 ("Courts, legislators, and even legal scholars have had a very hard time making sense of the SCA. The statute is dense and confusing, and few cases exist explaining how the statute works . . . . The SCA is a bit outdated and has several gaps in need of legislative attention, but by and large it reflects a sound approach to the protection of stored Internet communications." (citations omitted)).

Ultimately, the Fourth Amendment is just one aspect of this larger privacy framework. Nevertheless, it is a significant bulwark against governmental intrusion upon individual liberty in an area where the interests at stake are perhaps the most easily forgotten, and the least likely to be staunchly advocated for.[164]

CONCLUSION

Automated vehicles are the kind of technology that makes engineers curious, companies hopeful, and lawyers nervous. The possibilities offered by a car that can drive itself seem endless, and not all of them positive. What is most surprising, perhaps, is that their greatest threat to the Fourth Amendment lies with their ability to collect information, rather than with the autonomy that makes them such a radical innovation. As our vehicles increasingly carry data as much as they carry passengers, the privacy interests implicated by that data must be reconciled with the complexities of the existing automobile exception, the third-party doctrine, and other contours of Fourth Amendment jurisprudence. A warrant requirement to access vehicle data is a crucial component of extending the Fourth Amendment's protections for individual privacy, free from unreasonable governmental intrusion, into the twenty-first century. Automated vehicles may facilitate all kinds of new freedoms; but as they do, courts must ensure that the freedoms we already enjoy remain intact.

164. Recall Justice Frankfurter's words: "It is a fair summary of history to say that the safeguards of liberty have frequently been forged in controversies involving not very nice people." United States v. Rabinowitz, 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting).