BYU Law Review

Volume 48 | Issue 4 Article 6

Spring 5-12-2023

The Tesla Meets the Fourth Amendment

Adam M. Gershowitz

The Tesla Meets the Fourth Amendment

Adam M. Gershowitz[*]

Can police search a smart car's computer without a warrant? Although the Supreme Court banned warrantless searches of cell phones incident to arrest in Riley v. California*, the Court left the door open for warrantless searches under other exceptions to the warrant requirement. This is the first article to argue that the Fourth Amendment's automobile exception currently permits the police to warrantlessly dig into a vehicle's computer system and extract vast amounts of cell phone data. Just as the police can rip open seats or slash tires to search for drugs under the automobile exception, the police can warrantlessly extract data stored in a vehicle's infotainment system.*

This Article's contribution is important and timely. Police in multiple states have already extracted basic digital data from cars without a warrant. As Tesla and other smart cars become ubiquitous, police departments will be tempted to use more sophisticated data extraction tools to examine private cell phone data without first obtaining a warrant. Because the Supreme Court moves extremely slowly in addressing the legality of high-tech searches, this article argues that Congress and state legislatures should amend outdated privacy statutes to require police to obtain search warrants before extracting private cell phone data from a vehicle's computer system.

CONTENTS

* Vice Dean and Hugh & Nolie Haynes Professor of Law, William & Mary Law School. I am grateful to Jeff Bellin, Paul Belonick, Doug Berman, David Kaye, Tracey Meares, Jerry Norton, Jim Shellenberger, Jenia Iontcheva Turner, and Sandra Guerra Thompson for helpful suggestions, and to Caroline Lewis and Darian Kanouff for excellent research assistance.

INTRODUCTION

Can police use a high-tech device to tap into your car's "infotainment" system and retrieve your text messages, emails, and other private information without a warrant? In *Riley v. California*, the Supreme Court forbid police from conducting a warrantless search of a cell phone incident to arrest.[1] Because cell phones contain an enormous amount of data, the Court concluded that warrantless searches incident to arrest would be too invasive.[2] But the Court left the door open for warrantless cell phone searches under other exceptions to the warrant requirement, noting that

1. Riley v. California, 573 U.S. 373 (2014).

2. *See id.* at 393 ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity.").

"even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone."[3]

One of the case-specific exceptions that likely permits warrantless searches of electronic devices is the automobile exception.[4] The automobile exception authorizes extremely broad searches. For nearly one hundred years, the Supreme Court has permitted police to search all parts of a vehicle without a warrant so long as the police have probable cause.[5] The automobile exception is not limited to a search of visible items in the passenger compartment. It also permits police to dig into the bowels of a vehicle by slashing tires, ripping open seats, looking in the engine compartment or gas tank, and searching under floorboards or behind door panels.[6]

When the Court banned warrantless cell phone searches incident to arrest in *Riley*, the decision never mentioned the automobile exception. This made perfect sense when *Riley* was decided in 2014. At that point, there had only been a handful of cases in which police had found a cell phone in a vehicle and conducted a warrantless search of the phone on the grounds that it was a container that had been left in a vehicle.[7]

3. *Id.* at 401–02. Following this statement, the Court spent a few sentences explaining how the exigent circumstances exception could potentially allow warrantless cell phone searches in emergency situations. *See id.* at 402. Three paragraphs later, the Court ended its landmark opinion without addressing the other exceptions to the warrant requirement that could potentially apply to electronic devices. *See id.*

4. In addition to exigent circumstances (discussed in Riley) and the automobile exception (the subject of this article), courts have also grappled with whether law enforcement officers can conduct warrantless cell phone searches under the border exception, warrantless searches of parolees and probationers, and warrantless searches of children in schools. *See infra* note 121.

5. *See* Carroll v. United States, 267 U.S. 132 (1925); *see also infra* section II.A.

6. *See infra* section II.B.

7. *See* United States v. Monson-Perez, No. 4:09CR623 HEA, 2010 WL 889833, at *6–7 (E.D. Mo. Mar. 8, 2010) (concluding there was probable cause to search a cell phone and allowing a warrantless search under automobile exception); United States v. Rocha, No. 06-40057-01-RDR, 2008 WL 4498950, at *6 (D. Kan. Oct. 2, 2008) (finding probable cause to search a cell phone for drug activity and relying on automobile exception); United States v. James, No. 1:06CR134CDP, 2008 WL 1925032, at *7 (E.D. Mo. Apr. 29, 2008) (upholding a search of cell phone's call log based on the automobile exception); United States v. Fierros-Alvarez, 547 F. Supp. 2d 1206, 1211–14 (D. Kan. 2008) (upholding a search of a cell phone located in a vehicle under the automobile exception because an inventory of the vehicle turned up drugs, and there was probable cause to believe the cell phone had facilitated drug transactions).

Less than a decade later, though, the world looks very different. Police can now stop millions of vehicles across the country that are themselves electronic devices.[8] Tesla is the shiniest example[9] because it has the equivalent of an iPad built directly into the dashboard that runs almost every function of the vehicle. At present, Tesla vehicles record everywhere the car has been, the speed it traveled to get there, how long it was parked, whether seat belts were worn, and whether the vehicle departed from its lanes.[10] More interestingly, Tesla vehicles also contain a "Sentry Mode" that records live video when anyone comes near the parked car,[11] as well as "Dash Cam," which constantly records the road while the vehicle is traveling.[12] And of course, each day millions of people (even those without Teslas) connect their cell phones to their cars' infotainment systems in order to receive phone calls, text messages, and other data through their vehicles' computers.[13] In short, millions of vehicles contain a treasure trove of electronic data that law enforcement can use in investigating criminal activity that ranges from vehicular homicides all the way down to speeding. The amount of data generated and stored in smart cars will only grow in the future.

It is presently very easy for law enforcement to extract information from vehicle computers. There are two types of devices

8. *See* Andrew J. Hawkins, *Tesla Delivered Over 200,000 Cars in the Second Quarter of 2021*, THE VERGE (July 2, 2021, 7:26 AM), https://www.theverge.com/2021/7/2/22560608/tesla-q2-2021-deliveries-elon-musk.

9. Of course, Teslas are not the only smart cars. Many car manufacturers are selling sophisticated smart cars with computers built into the dashboard. *See* Keith Barry, *Screen Stars: Which Infotainment System Deserves a Leading Role in Your Next New Car*, CONSUMER REPS. (Aug. 5, 2020), https://www.consumerreports.org/infotainment-systems/screen-stars-in-car-infotainment-systems/ ("Almost all new vehicles sold in the U.S. this year (98.8 percent) will have a digital display screen . . . ."). And these computers—some of which look and operate just like an iPad—already contain tremendous amounts of data.

10. *See* Melanie Reid, The Impact of Autonomous Driving and Artificial Intelligence on Road Surveillance, Evidence Collection, and Criminal Prosecutions of Traffic Violations (unpublished manuscript) (on file with the author).

11. *See* Geoffrey A. Fowler, *My Car Was in a Hit-and-Run: Then I Learned It Recorded the Whole Thing*, WASH. POST. (Feb. 27, 2020, 7:00 AM), https://www.washingtonpost.com/technology/2020/02/27/tesla-sentry-mode/ ("A year ago, Tesla updated its software to also turn its cameras into a 360-degree video recorder. Even when the car is off.").

12. *See id.* ("With another function called Dash Cam that records the road, Tesla has saved hours and hours of my travels.").

13. This technology dates back for years, and therefore it is ubiquitous on the road. *See* Joe Donovan, *Want to Know If Your Car Pairs With Your Phone?*, DIGITAL TRENDS (Aug. 14, 2014), https://www.digitaltrends.com/cars/automobile-bluetooth-compatibility/.

that police use. The simpler device can extract event data recordings (so-called "EDR" or "black box" data) following a crash.[14] Police officers can plug the device into the same port under the steering wheel that a mechanic uses when repairing your car.[15] This is exactly what the police did to determine that Tiger Woods was traveling at more than 82 mph when his car crashed and rolled over in 2021.[16] The black box data gives the police interesting but limited information about speed, braking, and acceleration.[17] The standard black box extraction device—the Bosch Crash Data Retrieval Tool[18]—is not particularly expensive and police departments large and small all over the country utilize them.[19]

The second type of extraction device—a product manufactured by a company named Berla—enables the police to extract tremendously more information. The Berla device can access the infotainment system of many newer vehicles. The Berla device enables the police to discover navigation data, which tells the police where the driver has been. More concerning, if the driver has connected her cell phone to the vehicle—as all smart cars do[20]—the Berla device will enable police to access the cell phone data transferred to the car from the time the phone was connected to the vehicle.[21] Thus, the police can use the Berla device to access text messages, call histories, contact lists, emails, and perhaps even social media data.[22]

14. *See* Daniel Harper, Note, *Automobile Event Data Recorders and the Future of the Fourth Amendment*, 120 COLUM. L. REV. 1255, 1256 (2020).

15. *See* Steven T. Kean, *Virginia State Police, Event Data Recorder: An Overview*, VA. HIGHWAY SAFETY OFF. 1, 6 (2015), https://cdn.ymaws.com/mcaa-mn.org/resource/resmgr/files/tsrp/Resources/EDR_Overview_2-2015_-_Virgin.pdf.

16. *See* Brent Schrotenboer, *Tiger Woods Driving More Than 82 mph Before Crash, Unclear if He Was Conscious, Sheriff Says*, USA TODAY (Apr. 7, 2021, 1:29 PM), https://www.usatoday.com/story/sports/golf/2021/04/07/tiger-woods-update-crash-82-mph-unclear-consious/7120758002/.

17. *See* Kean, *supra* note 15.

18. *See id.*

19. *See The Bosch CDR Tool*, CRASH DATA GRP., https://crashdatagroup.com/pages/the-bosch-cdr-tool (last visited Mar. 11, 2023) (noting that it is "routinely used by law enforcement agencies").

20. *See* Taylor Martin, *How to Add Bluetooth to an Old Car*, CNET (July 26, 2017, 9:49 PM), https://www.cnet.com/tech/mobile/ways-to-add-bluetooth-to-an-old-car/ ("Bluetooth is now a standard feature in practically every modern car.").

21. *See infra* section I.B.

22. It is unclear whether the Berla device enables police to extract sentry mode videos recorded by the car's cameras. Berla only sells its extraction device and software to law

There is reason to be concerned that police across the country are using data extraction devices to access highly sensitive and private cell phone data from vehicles without a warrant. According to reported decisions from at least six states—California, Florida, Georgia, Missouri, New York, and Tennessee—police have acknowledged downloading black box data from vehicles without a warrant.[23] Given that there are nearly 18,000 law enforcement agencies across the country,[24] it is likely that many police departments permit their officers to warrantlessly extract data from vehicles. Moreover, even if departments presently have an internal policy requiring a warrant, they could always abandon their self-imposed restrictions and begin conducting warrantless searches.

Is it constitutional for police to warrantlessly download and search through text messages and other cell phone data run through a vehicle's infotainment system? The answer is likely "yes." As this article details, there is a strong argument that the automobile exception—which has long permitted police to conduct invasive searches into the bowels of a vehicle—permits the police to warrantlessly dig into a car's computer system to extract private cell phone data. Moreover, the existing federal Driver Privacy Act, which provides some statutory protection for black box data,

enforcement agencies, and it has not made public how the device works, the exact makes and models of vehicles it can access, the price, or how many law enforcement agencies have purchased one. *See* Patrick Howell O'Neill, *Meet Berla, The Little-Known Company That Can Pull Smart-Phone Data From Your Car*, CYBERSCOOP (Sept. 11, 2017), https://cyberscoop.com/berla-car-hacking-dhs/. We do know, however, that the Berla device has the potential to access a tremendous amount of data and that law enforcement organizations are beginning to buy more of them. Berla's website does specify that its product can "[a]ccess event logs associated with activity such as door opens, gear shifts, odometer reads, ignition cycles, speed logs, and more" and that it can "[r]ecover location data and navigation information such as track logs, saved locations, active routes and previous destinations." *Discover Vehicle Forensics*, BERLA, https://berla.co/discover/(last visited Mar. 29, 2023). More interesting, the Berla website notes that it can "[i]dentify devices that have been connected via the USB ports, over Bluetooth or wireless network and all of the data associated with those devices."). *Id.* According to police officers who spoke off the record, most police departments do not have Berla devices yet because they are too expensive and require considerable training to use correctly. However, some large law enforcement organizations—such as state troopers—that possess the requisite resources do possess Berla devices. *See infra* note 66 and accompanying text. Indeed, the Berla device is proving to be a valuable tool for investigating both low-level and serious criminal activity. *See* O'Neill, *supra* (noting that the Berla devices assisted in the San Bernadino terrorist attack case).

23. *See infra* notes 39–45 and accompanying text.

24. *See* BRIAN A. REAVES, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, CENSUS OF STATE AND LOCAL LAW ENFORCEMENT AGENCIES, 2008 2 (2011).

simply does not apply to the far more private cell phone data that runs through a vehicle's infotainment system. Because the Fourth Amendment and existing statutes do not forbid warrantless smart car searches, legislatures should enact statutes that will protect private cell phone data in smart cars. Congress and state legislatures have required a warrant by statute in a host of areas, including wiretapping, third-party electronic data, body cavity searches, and DNA databases.[25] There is no reason legislatures could not also specify by statute that a warrant is necessary to search smart car computers.

Part I of this article explains the two types of data extraction devices that law enforcement can use to extract information from vehicles. Part I focuses, in particular, on the Berla device, which enables police to go beyond the basic black box driving data to search through the enormous amount of cell phone data that flows through a smart car's infotainment system. Part II then explains how the automobile exception permits the police to warrantlessly extract cell phone data with the Berla device. Part II explains why the Supreme Court will likely decline to extend its decision in *Riley v. California* banning cell phone searches incident to arrest to searches under the automobile exception. The Court has long provided reduced Fourth Amendment protection to automobiles. And unlike cell phones, which the police recognized could be immobilized while police seek a warrant, there is no faraday bag large enough to hold a two-ton vehicle. Additionally, the *Riley* decision was premised in large part on the absence of probable cause, a situation that is not present in automobile exception cases. Part III then details how the Court is unlikely to address the constitutionality of smart car computer searches for many years or even decades. Part IV then considers how the closest applicable statute—the Driver Privacy Act of 2015—offers only minimal protection for black box data and absolutely *no* protection against warrantless searches of the far more private cell phone data that flows through vehicles' infotainment systems. Part V then explains how Congress and state legislatures have the authority to enact statutes that would forbid warrantless smart car searches.

25. *See infra* notes 194–213.

I. POLICE CAN ACCESS "BLACK BOX" DRIVING DATA AND VERY PRIVATE CELL PHONE DATA STORED ON VEHICLES' COMPUTERS

Police frequently use data extraction devices to acquire information from vehicles.[26] In order to reconstruct accidents, police regularly tap into vehicles' computers to gather information about how the vehicle was operating at the time of the crash. In some cases, police officers acknowledge downloading this data without first having procured a warrant.[27] The "simple" data extraction devices used to download driving data, and courts' inconsistent approach to them, are described in section I.A below. Some police agencies also have a far more advanced data extraction tool that enables them to recover not just basic driving data but also reams of cell phone data that have been transferred to the vehicle's infotainment system. As explained in section I.B below, some police agencies have a Berla device that can extract "a vast array of sensitive personal information quietly stored in the infotainment consoles and various other computers used by modern vehicles, [including] . . . [r]ecent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been."[28]

A. Black Box Data Extraction Devices

Almost every car manufactured in the United States since 2013 is equipped with an event data recorder (an "EDR")[29] which is often referred to as a "black box." Under federal regulations, a vehicle's EDR must record more than a dozen pieces of data, including speed, braking, seat belt, and airbag information.[30] Vehicles are constantly recording and writing over this data, though the information is stored if the vehicle is in an accident.[31]

To retrieve the EDR data, law enforcement must access the EDR, which is typically below the carpet on the driver's side of

26. *See* Harper, *supra* note 14, at 1260.

27. *See infra* notes 39–45.

28. *See* Sam Biddle, *Your Car Is Spying on You, and a CBP Contract Shows the Risks*, THE INTERCEPT (May 3, 2021, 12:21 PM), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/.

29. *See Bosch CDR Tool*, supra note 19.

30. *See* 49 C.F.R. § 563.7.

31. *See* Harper, *supra* note 14, at 1256. In addition to an accident, the EDR may store data when there has been very forceful braking of the vehicle. *See id.* at 1259.

the vehicle.[32] Once the police have located the EDR, they then plug in a Crash Data Retrieval device ("CDR").[33] The most common CDR is made by a company named Bosch.[34] The officers plug the CDR into the vehicle's Diagnostic Link Connector beneath the steering column.[35] In plainer language, the officer will plug the CDR into the same port that a car mechanic uses to check the various systems on a vehicle.[36] As of 2015, the Bosch CDR enabled law enforcement to extract EDR data from Hondas, Toyotas, Fords, Mercedes, and more than two-dozen other car manufacturers.[37]

Police frequently utilize CDR devices to retrieve EDR black box data. One scholar observed that Texas police departments downloaded EDR data "sixty-six percent of the time in fatal or possibly fatal crashes, forty-one percent of the time in serious personal injury cases, eleven percent of the time in accidents involving property damage, and two percent of the time in minor injury accidents."[38]

Multiple police agencies have acknowledged downloading EDR data without first obtaining a warrant. A California highway patrol officer acknowledged that it was "standard practice" to download EDR data without first obtaining a warrant.[39] In one example from California, police restored battery power to a vehicle over a year after a fatal accident to warrantlessly extract data from the car's computer.[40] In New York, a state trooper "used computer equipment in his police car to download information from the Sensing Diagnostic Module (SDM) located in the Defendant's vehicle" without first obtaining a warrant.[41] In Florida, police "downloaded data from the 'event data recorder' or 'black box'" twelve days after the vehicle was involved in a fatal crash without

32. *See id.* at 1255.
33. *See* Kean, *supra* note 15, at 6.
34. *See id.* at 8.
35. *See id.*
36. *See id.*
37. *See id.*
38. Harper, *supra* note 14, at 1260.
39. *Id.*; People v. Diaz, 153 Cal. Rptr. 3d. 90, 96 (Cal. Ct. App. 2013).
40. *See* People v. Xinos, 121 Cal. Rptr. 3d 496, 502, 504 (Cal. Ct. App. 2011).
41. People v. Christmann, 776 N.Y.S.2d 437, 438 (Just. Ct. 2004).

first procuring a warrant.[42] In Georgia, an officer at the scene of a two-car accident "entered the passenger compartments of both vehicles, attached a crash data retrieval (CDR) device to data ports in the cars, and used the CDR to download data" without first obtaining a warrant.[43] And in Tennessee, a state trooper used a crash data recorder to extract air bag sensor data in a vehicular homicide case without procuring a warrant.[44] In Missouri, a highway patrol officer admitted to downloading EDR data without a warrant at the initial stage of a car accident investigation.[45]

Courts have been all over the map in resolving suppression motions in these cases. One court concluded that the driver had no reasonable expectation of privacy in the EDR, and thus the police did not conduct a search.[46] Another court has found that downloading the EDR data is a search but that the search could be permissible under the automobile or exigency exceptions to the warrant requirement.[47] Still other courts have concluded that EDR downloads are a search that requires a warrant.[48] Despite the varying judicial interpretations, two things are quite clear: (1) police regularly download "black box" data from vehicles' EDRs in order to investigate criminal activity; and (2) officers in multiple

42. State v. Worsham, 227 So. 3d 602, 603 (Fla. Dist. Ct. App. 2017). Another Florida case appears to suggest (though does not specifically state) that police extracted EDR data without a warrant. *See* State v. Pierre, 293 So. 3d 640 (Fla. Ct. App. 2020).

43. Mobley v. State, 834 S.E.2d 785, 788 (Ga. 2019).

44. *See* State v. Holladay, No. E2004-2858, 2006 WL 304685 (Tenn. Crim. App. Feb. 8, 2006).

45. *See id.*; State v. West, 548 S.W.3d 406, 410, 412 (Mo. Ct. App. 2018).

46. *See* People v. Diaz, 153 Cal. Rptr. 3d 90, 101–02 (Cal. Ct. App. 2013) (finding no reasonable expectation of privacy in the data collected by the device). This decision is from 2013 and seemingly would have come out differently today. The Supreme Court has indicated that police can conduct a search either by invading a reasonable expectation of privacy or by engaging in a physical trespass. *See* Florida v. Jardines, 569 U.S. 1 (2013). The government can plausibly argue that a driver does not have a subjective expectation of privacy if she does not know an EDR is located in the vehicle. And the prosecution could also argue that even if the driver had a subjective expectation of privacy that it is not objectively reasonable because the data held in the EDR provides the same information (e.g., speed and braking) that the driver had already made available to the public. But it is far harder to see how an officer would not have physically trespassed when she accessed the EDR. To access the EDR, police must either rip up the carpet from inside the vehicle or insert a device into a port under the steering wheel. Either of those actions would seemingly be a trespass.

47. *See West*, 548 S.W.3d at 418–19 (recognizing that the automobile exception could apply, but finding that there was no probable cause in this case).

48. *See, e.g.*, State v. Worsham, 227 So. 3d 602, 602 (Fla. Dist. Ct. App. 2017); *Mobley*, 834 S.E.2d at 792–93.

states have acknowledged in open court that they downloaded the black box data without first seeking a warrant.

B. More Sophisticated Berla Devices

As indicated in section I.A above, many police departments have crash data retrieval devices to recover traditional driving data about speed, braking, seat belts, and airbags. A smaller number of police agencies have more sophisticated devices that are capable of downloading text messages, contact lists, call histories, social media data, email, photos, and other personal and sensitive data that has been transferred by Bluetooth from a cell phone to the vehicle's infotainment system.

A Maryland company named Berla manufactures a device and accompanying software that allows law enforcement agencies to extract data from smart cars.[49] The company keeps a low profile. Little is known about how many models of cars the Berla device interfaces with or about how many law enforcement agencies have purchased the devices. The manufacturer discloses very little information on its website. It appears though that Berla sells its device and software only to law enforcement agencies and the Department of Homeland Security.[50]

So how does it work? A 2017 news article explained that "Berla's flagship product is Project iVe, a forensics tool that breaks into a vehicle's data systems to find, organize and analyze a vast range of information that often includes far more than what the car generates itself."[51] Like other data extraction devices, the Berla device can recover driving routes, vehicle events, and location data.[52] But the Berla device is able to dig out considerably more information than traditional extraction devices.

Many new vehicles on the road enable drivers to connect their cell phones to the car via Bluetooth.[53] Drivers can then receive cell phone communications—calls, text messages, and push notifications—through the vehicle's computer screen.[54] Drivers can

49. *See What We Do*, BERLA, https://berla.co/ (last visited Mar. 29, 2023).
50. *See* Biddle, *supra* note 28.
51. O'Neill, *supra* note 22.
52. *See Discover Vehicle Forensics*, *supra* note 22.
53. *See* Donovan, *supra* note 13.
54. *See Discover Vehicle Forensics*, *supra* note 22.

also use the apps on their phone—such as Spotify, Apple Podcasts, or iTunes—to play content through the vehicle's infotainment system. These functions are very convenient and therefore used by many drivers.

Once a driver has connected her cell phone to the infotainment system however it provides an opportunity for law enforcement to extract data that had originally been on the cell phone. The cell phone transfers "SMS messages, contact lists, emails, social media feeds and more" to the vehicle.[55] Berla's founder put it more colorfully when he explained that "[w]hen you plug [your phone] into th[e] USB port . . . it's going to start sucking all your data down into the car."[56] Berla's founder went on to explain the sheer amount of data that a Berla device was able to extract from a rental car:

> We had a Ford Explorer . . . we pulled the system out, and we recovered 70 phones that had been connected to it. All of their call logs, their contacts and their SMS history, as well as their music preferences, songs that were on their device, and some of their Facebook and Twitter things as well . . . And it's quite comical when you sit back and read some of the text messages.[57]

In addition to infotainment data, smart cars like Tesla have "dashboard cameras and selfie cameras [that] can record while the

55. *See* O'Neill, *supra* note 22. According to Berla's own website, the device empowers police to:

- Provide insight on the sequence of events that took place leading up to an incident;
- Identify patterns of life and unusual events that happened around an incident.
- Determine timelines of activity and establish a chain of significant events.
- Provide historical data to show where a vehicle was at specific times.
- Identify areas frequently visited, new locations traveled, and future plan.
- Determine how long particular locations were visited.
- Provide unique identifiers that tie individuals to a specific vehicle.
- Identify known associates and establish communication patterns between them.
- Determine who may have been present or aware of key information during an incident.

Discover Vehicle Forensics, *supra* note 22.

56. *See* Biddle, *supra* note 28.

57. *Id.*

car is parked, even in your garage, and there is no way for an owner to know when they may be doing so."[58] The Tesla also has a built-in internet browser that drivers can use to surf the internet.[59] Because Berla does not advertise in detail what its product is capable of extracting, it is unclear whether the device can download sentry video recordings and internet browsing data.

The Berla device is not compatible with all vehicles, especially older vehicles that have been on the road for a long time. But the number of compatible vehicles is growing. The Berla device could only access 80 car models when it launched in 2013. By 2017 that number had risen to "over 6,730 globally, including cars from BMW, Ford, General Motors and Volkswagen, among others."[60] By 2021, the Berla device could be used with 19,576 types of vehicles.[61]

In an effort to gather more information about the Berla device, a research assistant and I contacted multiple police departments to ask if they possessed a Berla device. Many departments said that they did not have a Berla device; other departments declined to answer. A North Carolina State Police Trooper from the Collision Reconstruction Unit was willing to provide information though.[62]

Consistent with the description above, the trooper indicated that a Berla device can access the infotainment data on some, but certainly not all, vehicles.[63] For the vehicles that the Berla device can connect with, it can access navigation data including the "bread crumbs" of where a suspect may have physically been.[64] The trooper confirmed that the Berla device can also access cell phone data from the time the phone connected to the car, including text messages, phone calls, and more.[65]

58. *See* Kate Fazzini & Lora Kolodny, *Tesla Cars Keep More Data Than You Think, Including This Video of a Crash That Totaled a Model 3*, CNBC (Mar. 29, 2019), https://www.cnbc.com/2019/03/29/tesla-model-3-keeps-data-like-crash-videos-location-phone-contacts.html.

59. *See* Rosalie Chan, *Elon Musk Hints that the Web Browsers in Tesla Cars Are Going to Get a Lot Better, Thanks to Technology Created by Google*, BUS. INSIDER (Mar. 22, 2019), https://www.businessinsider.in/elon-musk-hints-that-the-web-browsers-in-tesla-cars-are-going-to-get-a-lot-better-thanks-to-technology-created-by-google/articleshow/68529684.cms.

60. *See* O'Neill, *supra* note 22.

61. *See iVE Timeline*, BERLA, https://berla.co/ive-timeline/ (last visited Mar. 29, 2023).

62. *See* Interview by Caroline Lewis with North Carolina State Police Trooper (Apr. 29, 2021) (interview notes on file with the author).

63. *See id.*

64. *See id.*

65. *See id.*

The trooper indicated that Berla devices are expensive, costing tens of thousands of dollars and requiring officers to take a training course that costs additional money.[66] Because of the cost, the highway patrol division of the North Carolina State Troopers had only recently acquired Berla devices in 2020.[67] The trooper further indicated that the Berla devices are not presently used very often.[68] Officers need training to know how to use the devices so there is a limited number of officers who can use them.[69] Moreover, the trooper explained that unlike black box data (which can be extracted from a port under the steering wheel), the Berla device must be plugged into a circuit breaker, which requires a time-consuming process to disassemble the dashboard of the vehicle.[70]

While Berla devices are not presently used very often, the trooper believed that because they can extract a lot of information, police will use the devices more often in the future.[71] A recent report from NBC news quoted a Michigan State Police officer saying that "four offices across the state . . . routinely" extract forensic data from vehicles for "smaller, everyday felonies" "two to three times a week."[72]

The North Carolina trooper we interviewed indicated that officers never utilize the Berla device without a warrant.[73] As explained in Part II, however, existing Supreme Court precedent suggests that a search warrant is not actually required.

66. *See id.*

67. *See id.*

68. *See id.*

69. *See id.*

70. *See id.*

71. *See id. See also* Olivia Solon, *Insecure Wheels: Police Turn to Car Data to Destroy Suspects' Alibis*, NBC (Dec. 28, 2020), https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939 ("More law enforcement agencies nationwide are using the data to solve cases, and they are devoting more and more resources to this new type of crime solving, law enforcement officers and digital forensic examiners say.").

72. Solon, *supra* note 71.

73. *See* Interview of North Carolina State Trooper, *supra* note 62. The Trooper noted that on rare occasions they receive consent from the owner.

II. THE AUTOMOBILE EXCEPTION LIKELY PERMITS THE POLICE TO USE A BERLA DEVICE TO EXTRACT CELL PHONE DATA FROM A VEHICLE WITHOUT A WARRANT

The Fourth Amendment's automobile exception allows the police to search a vehicle without a warrant so long as the officers have probable cause. This Part explains that (1) Police can search a vehicle without a warrant if they have probable cause; (2) The officers can move the vehicle to the station to conduct the search; (3) The officers face very little time pressure in searching and can wait hours or perhaps days without having to get a warrant; and (4) The search can be invasive, with the officers having authority to dig into and dismantle gas tanks, engine blocks, and other parts of the car to search, as long as they have probable cause to believe they will find evidence or contraband. If existing precedent for the automobile doctrine is carried to its logical conclusion, it would permit the police to tow a Tesla or other smart car to the police station, connect it to a Berla device or other data extraction device, and take as long as they need to figure out how to remove the electronic evidence from the vehicle.

One might think that the Supreme Court's decision in *Riley v. California* would lead to a different result that prevents the police from relying on the automobile exception to conduct a lengthy, invasive, and warrantless search of a smart car's computer. This Part explains however why the Supreme Court's decision in *Riley v. California* banning warrantless searches of a cell phone incident to arrest is not likely to be extended to the automobile exception. In particular, (1) smart cars hold less data than cell phones; (2) some vehicle information is already visible and available to the public; (3) vehicles receive less privacy protection because they are heavily regulated; (4) vehicles are too large to be immobilized by faraday bags; and (5) unlike the search incident to arrest doctrine at issue in *Riley*, the automobile exception is premised on probable cause and it is not automatic.

A. The Automobile Exception Allows Warrantless Searches at the Station Days Later

1. The Police Can Move the Vehicle

The Supreme Court first recognized the automobile exception in a 1925 Prohibition-era case called *Carroll v. United States*.[74] Federal agents searched a car to look for bootlegged liquor. The agents had probable cause, but no warrant. The Court upheld the warrantless search of the vehicle by drawing a distinction between a home and a "ship, motor boat, wagon, or automobile" because a "vehicle can be quickly moved."[75] The mobility of the vehicle became the key rationale for allowing a warrantless search.

In subsequent years, the Court expanded law enforcement's ability to utilize the automobile exception by permitting police to move the vehicle and search it at a later time. In *Chambers v. Maroney*,[76] witnesses to a robbery told the police about the getaway vehicle and what the occupants were wearing. Police were then able to track down the vehicle and arrest the occupants. Rather than search the vehicle at the scene, the officers drove it to the police station where "[i]n the course of a thorough search of the car at the station, the police found concealed in a compartment under the dashboard two .38—caliber revolvers" and other incriminating evidence.[77] Because the search occurred "some time after the arrest" it could not be justified as a contemporaneous search incident to arrest.[78] The Court therefore had to address the legality of the search under the automobile exception. After noting that the *Carroll* doctrine allowed a search on the scene because the car was mobile, the *Chambers* Court recognized that the justification to search "still obtained at the station house" because the car was still mobile.[79]

The decision in *Chambers* is subject to criticism.[80] The car was not really mobile. It was in police custody. There was virtually no

74. Carroll v. United States, 267 U.S. 132 (1925).

75. *Id.* at 153.

76. Chambers v. Maroney, 399 U.S. 42 (1970).

77. *Id.* at 44.

78. *Id.* at 47.

79. *Id.* at 52.

80. *See* Arnold H. Loewy, *Cops, Cars, and Citizens: Fixing the Broken Balance*, 76 ST. JOHN'S L. REV. 535, 539 (2002) ("[T]he Court upheld the search without a warrant on a rationale so transparently flimsy, that it is hard to take seriously.").

chance of it disappearing (or any evidence inside of it disappearing) while police applied for a warrant.[81] Yet, the Court disregarded this logical objection and instead gave the police a green light to move a vehicle to the police station and search it without a warrant. A half-century later, the rule remains in effect and police can tow a vehicle to the station and search it without a warrant.

2. Police Can Take Hours or Even Days Before Searching

If police are searching a car under the automobile exception they do not need to search immediately. The Court has upheld warrantless searches hours and even days after a vehicle was moved to the station. In *Florida v. Meyers*, police searched a vehicle on the scene of an arrest and then towed the vehicle to the station.[82] Eight hours later, a police officer went to the impound lot and searched the vehicle again and found incriminating evidence.[83] The Court reiterated that "the justification to conduct such a warrantless search does not vanish once the car has been immobilized" and it upheld a search that occurred eight hours after impoundment.[84]

A year after *Meyers*, the Court went even further in giving police time to conduct a warrantless search under the automobile exception. In *United States v. Johns*, the Court addressed whether police could search packages without a warrant three days after they had been removed from a vehicle.[85] The DEA had seized pickup trucks from a desert airstrip and brought them back to the DEA headquarters.[86] The agents removed packages from the trucks and placed them in the DEA warehouse.[87] The agents then immediately searched some of the packages, but waited three days before searching the other packages.[88] At no point did the agents procure a warrant.[89] The Supreme Court upheld the warrantless

81. *See* JOSHUA DRESSLER, ALAN C. MICHAELS, & RIC SIMMONS, UNDERSTANDING CRIMINAL PROCEDURE 210–11 (2017).

82. Florida v. Meyers, 466 U.S. 380 (1984) (per curiam).

83. *Id.*

84. *Id.* at 382.

85. United States v. Johns, 469 U.S. 478 (1985).

86. *See id.* at 481.

87. *See id.*

88. *See id.*

89. *See id.*

searches under the automobile exception, even though they occurred three days after the vehicle was impounded. The Court explained that there is simply no contemporaneousness requirement for the automobile exception the way that there is for the search incident to arrest exception:

> [O]ur previous decisions indicate that the officers acted permissibly by waiting until they returned to DEA headquarters before they searched the vehicles and removed their contents. There is no requirement that the warrantless search of a vehicle occur contemporaneously with its lawful seizure. '[T]he justification to conduct such a warrantless search does not vanish once the car has been immobilized.' A vehicle lawfully in police custody may be searched on the basis of probable cause to believe that it contains contraband, and there is no requirement of exigent circumstances to justify such a warrantless search.[90]

The *Johns* Court did recognize that at some point a warrantless search would no longer be reasonable under the automobile exception. The Court noted that "[w]e do not suggest that police officers may indefinitely retain possession of a vehicle and its contents before they complete a vehicle search."[91] And the Court further remarked "[n]or do we foreclose the possibility that the owner of a vehicle or its contents might attempt to prove that delay in the completion of a vehicle search was unreasonable because it adversely affected a privacy or possessory interest."[92] Accordingly, it is clear that there are some temporal restrictions on when police can search a vehicle without a warrant. If police had no plausible basis to continue holding onto a vehicle, it seems quite possible that retaining the vehicle and conducting a warrantless search days after the seizure would be unconstitutional. But when police have probable cause to believe a vehicle contains evidence, the *Meyers* and *Johns* cases suggest that police can take their time in conducting a warrantless search of the vehicle.

* * *

Piecing these rules together, we see that the automobile exception provides the police with a lot of leeway. Officers can

90. *Id.* at 484 (citations omitted) (quoting Michigan v. Thomas, 458 U.S. 259, 261 (1982) (per curiam)).

91. *Id.* at 487.

92. *Id.*

search a vehicle without a warrant, even if it would be practicable for them to obtain one. Officers can search the vehicle at the scene, but they are also free to tow the car to the police station where they can search it more comfortably. And officers can take their time and conduct the search hours or even days after the vehicle has been seized.

The next question is how broad the search can be. As section II.B explains, the automobile exception gives the police considerable authority to conduct broad, invasive searches without a warrant.

B. The Automobile Exception Allows Invasive Searches Deep Inside of Vehicles

The automobile exception typically authorizes an expansive and invasive search of the vehicle. This can include not just the passenger compartment and the trunk but also (in some cases) the gas tank, engine block, beneath the floor boards, and other internal parts of the vehicle.[93]

Let us begin with the conventional cases. Ordinarily, police will have probable cause to search the entire vehicle and open any containers inside the vehicle that could hide the contraband they are looking for. For example, imagine that a reliable informant tells police that she saw Alex carrying a small green bag that contains stolen jewelry and that only moments earlier she saw Alex place the green bag in his vehicle. The tip gives the police probable cause to search Alex's vehicle for the green bag and the stolen jewelry. Because the probable cause is for the vehicle generally and the green bag is small, the police can search the entire vehicle. The officers can look in the trunk, under the seats, in the glove

93. Searches under the automobile exception are often far more invasive than searches under the search incident to arrest doctrine. Under the search incident to arrest doctrine, police can search the passenger compartment of a vehicle (but not the trunk) if the arrestee is unsecured or if the officers have reason to believe evidence of the crime of arrest can be found in the vehicle. *See* Arizona v. Gant, 556 U.S. 332 (2009). Some lower courts have upheld searches as incident to arrest in which police had broken into secret compartments in the vehicles, but other courts have found dismantling of seats and the tailgate to exceed what is permitted under the search incident to arrest doctrine. *See* Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Warrantless Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1152–53 (2011) (collecting cases). The inventory exception permits the police to administratively log any items in the vehicle to prevent false claims of theft. The inventory exception does not allow the police to disassemble the vehicle, however. *See* South Dakota v. Opperman, 428 U.S. 364 (1976).

compartment, and in other locations inside the vehicle. The officers can also open larger containers (e.g., a cardboard box) that the green bag could fit in. In this very common scenario, the automobile exception gives the police vast power to search through practically the entire passenger compartment and trunk of the vehicle.[94]

In some cases, the automobile exception will only authorize a narrower search though. Imagine that our reliable informant instead tells the police that Beverly keeps an unlawful shotgun in the trunk of her car and that "Beverly is too smart to keep the gun in the passenger compartment where the police could see it." Now the police are limited in where they can search. The automobile exception still permits the police to search the trunk of the car. But they cannot open a small green bag because there is no probable cause to believe the shotgun could be in there (because it could not fit). Nor can the police search the passenger compartment of the vehicle because the informant provided no probable cause to believe contraband or evidence could be located there. The probable cause provided by the informant is only for the trunk of the vehicle, and only for areas that are large enough to hold a shotgun.[95] Thus, in some situations the automobile exception allows only a limited search of the car.

On the flip side, and of particular relevance to smart car searches, are situations in which police have probable cause to search more invasively than simply looking in the passenger compartment or the trunk. Often these cases involve drugs. For example, imagine that our informant tells the police that she works for a drug-smuggling operation and that Charles will be driving a car loaded with bags of heroin. The informant provides not only a description of the vehicle, but also that the drugs are hidden in a secret compartment behind the glove box. The compartment can only be accessed by using a screwdriver to take apart the glove box.[96] Can the police take apart the vehicle to search for the drugs

94. For a discussion about the power that the automobile has given the police to stop and search people (and how it has shaped American criminal justice), see SARAH A. SEO, POLICING THE OPEN ROAD: HOW CARS TRANSFORMED AMERICAN FREEDOM (2019).

95. *See*, *e.g.*, State v. Williams, 462 So. 2d 69 (Fla. Dist. Ct. App. 1985) (suppressing drugs found in the glove compartment because the police had only observed contraband being placed in the trunk and thus "the probable cause did not extend to the entire vehicle").

96. *See* State v. Arnaud, No. K2/01-0630A, 2002 WL 31992357, at *4 (R.I. Super. Ct. May 2, 2002) (explaining that "[u]nder the automobile exception, law enforcement officials may dismantle the dashboard of an automobile in police custody whenever probable cause exists").

under the automobile exception? So long as the police have probable cause, the answer is "yes."

Searching secret compartments—even if the police have to disassemble part of the car or break into the compartment—is permissible under the automobile exception as long as there is probable cause to believe the evidence can be located there. In *Carroll v. United States* (the 1925 Supreme Court decision initially recognizing the automobile exception), the agents "opened the rumble seat and tore open the upholstery of the lazyback."[97] In *Chambers v. Maroney* (the 1970 Supreme Court decision authorizing the police to tow the vehicle to the station), "the police found [weapons and stolen property] concealed in a compartment under the dashboard," and the Court made no suggestion that the scope of the search was impermissible.[98]

Many lower court cases have relied on the automobile exception established in *Chambers* to uphold warrantless searches of the engine compartment,[99] spare tires,[100] gas cap,[101] gas tank,[102] and secret compartments found elsewhere in the vehicle.[103] In upholding

97. *See* United States v. Ross, 456 U.S. 798, 817 (1982) (referencing Chambers v. Maroney, 399 U.S. 42, 44 (1970)).

98. Chambers, 399 U.S. at 818.

99. *See* United States v. Jones, 93 F. App'x 576 (4th Cir. 2004) (per curiam) (concluding that automobile exception authorized a search of the engine compartment when there was probable cause for that location); United States v. Marchena-Borjas, 209 F.3d 698 (8th Cir. 2000) (same); United States v. Williams, 23 F. Supp. 3d 46 (D. Mass. 2014) (same).

100. *See*, *e.g.*, United States v. Alverez, 235 F.3d 1086 (8th Cir. 2000) (upholding "a full and thorough search of the tire, including dismantling or damaging it" and in this case slashing it because the tire made a thudding sound when shaken, indicating it was being used as a container).

101. *See* United States v. Goncalves, 642 F.3d 245, 249 (1st Cir. 2011) (upholding search of the engine compartment and gas cap because drugs are often hidden there).

102. *See* United States v. Urbina, 431 F.3d 305, 310 (8th Cir. 2005) ("The sound of objects moving in the tank gave the officers probable cause to believe that the gas tank contained contraband, and probable cause is sufficient to justify the warrantless search of an automobile or a container therein, including the destruction, if necessary, of the container.").

103. *See* United States v. Cooper, 125 F.3d 849 (4th Cir. 1997) (relying on the automobile exception to uphold search of a secret compartment in the passenger back side panel of the vehicle with the use of a screwdriver to pry it open); United States v. Bullock, 94 F.3d 896, 898 (4th Cir. 1996) (upholding search under the automobile exception where police discovered a door and false compartment that had been professionally installed behind a seat and the officers drove the car to a nearby police barracks and "cut the compartment open"); United States v. Patterson, 65 F.3d 68 (7th Cir. 1995) (upholding office folding down the tailgate); United States. v. Waldron, No. CR 09-1271, 2010 WL 11545567 (C.D. Cal. Mar. 30, 2010) (upholding search of the secret compartment under backseat); People v. Davis, 147

searches of these locations, courts have specifically recognized that police can dismantle or even destroy parts of the car to conduct the search. Courts have approved dismantling door panels,[104] glove compartments,[105] dashboards,[106] and even slashing open spare tires.[107] As a Georgia court explained, "when an officer has probable cause to believe a sealed compartment in an automobile contains contraband, he may lawfully search it including dismantling [it] or damaging it."[108] A Rhode Island court has similarly explained that "[u]nder the automobile exception, law enforcement officials may dismantle the dashboard of an automobile in police custody whenever probable cause exists."[109] In upholding a search for a secret compartment "behind a tailgate panel" the Seventh Circuit remarked quite simply that "[u]nder the automobile exception . . . *all* parts of a vehicle may be searched without a warrant if there is probable cause to believe the car contains contraband or evidence."[110]

In sum, the automobile exception provides the police with broad authority to search. In the conventional case, the officers can look in the passenger compartment and the trunk, and they can usually open containers during the search. In some cases—particularly drug cases—the officers are permitted to break beneath the surface of the car to look beneath the upholstery or outer layer of the vehicle in order to look for and through secret compartments. In these cases where police search for secret compartments, the automobile exception provides broad authority to conduct invasive searches inside the structure of the vehicle.

N.E.3d 711, 718 (Ill. App. Ct. 2019) (upholding a search under the automobile exception where the officer "pried open" a secret compartment in the back of the seat).

104. *See* United States v. Harwood, 998 F.2d 91, 94 (2d. Cir. 1993).

105. *See* State v. Arnaud, No. K2/01-0630A, 2002 WL 31992357, at *5 (R.I. Super. 2002).

106. *See* United States v. Sample, 136 F.3d 562, 564 (8th Cir. 1998).

107. *See* United States v. Hernandez-Rubio, No. 8:19-CR-389, 2020 WL 3072040 (D. Neb. 2020).

108. Fernandez v. State, 619 S.E.2d 821, 829 (Ga. Ct. App. 2005).

109. *Arnaud*, No. K2/01-0630A, 2002 WL 31992357 at *5.

110. United States v. Patterson, 65 F.3d 68, 71 (7th Cir. 1995) (emphasis added).

C. The Law Governing the Automobile Exception Suggests that Warrantless Searches of Smart Car Computers Are Lawful

The case law described in sections II.A and II.B above stands for four basic propositions: (1) police can search a vehicle without a warrant if they have probable cause; (2) officers can move the vehicle to the station to conduct the search; (3) officers can take their time in searching—waiting hours or perhaps days—without having to get a warrant; and (4) the search can be invasive, with the officers having authority to dig into and dismantle parts of the car to search, as long as they have probable cause to believe they will find evidence or contraband.

What do these four principles tell us about police authority to search a smart car's computer without a warrant under the automobile exception? The various strands of automobile doctrine precedent strongly suggest that police can utilize the Berla device or other data extraction device to search for evidence without a warrant. A Tesla or other smart car is a vehicle and it is mobile. The officers are permitted to tow that vehicle to the station to search it there, where they can then take their time—hours if necessary—to get the right tools to search the vehicle. And just as the officers could use a screwdriver or a crowbar to conduct an invasive search into a secret compartment, they should be able to use a different tool—a data extraction device—to conduct an invasive search of the smart car's computer. The basic logic is identical whether we are talking about a secret compartment to hold drugs or an electronic container to hold data. Because the car is mobile and the police have probable cause, they can search in the (electronic) container to obtain the evidence without needing a warrant.

Under this logic, the search of a smart car (like it does for a physical search) turns on whether the police have probable cause. Put differently, the question is whether an officer can point to probable cause to believe there is evidence of criminal activity in the smart car's computer. In many instances, police will, in fact, have probable cause to believe the car's computer contains evidence.

First and most obviously, smart car computers hold vast amounts of driving data history such as speed, acceleration, lane departures, and braking.[111] This data could be relevant to low-level

111. *See supra* notes 56–61 and accompanying text.

traffic offenses such as speeding and failure to signal. It could also provide valuable evidence of more serious offenses such as reckless driving, drunk driving, and leaving the scene of an accident. And the car's basic driving data could be crucial to investigating extremely serious crimes such as vehicular homicide.

Second, much like cell phones, smart cars contain location data that tells investigators where a vehicle has been and when it was driven there. If police have probable cause that a suspect was involved in a burglary, robbery, rape, or a host of other offenses, the vehicle's location data could demonstrate that the driver was at the scene of the crime. The data could tell the police the exact time when the car (and ostensibly the suspect) arrived and departed from the scene of the crime.

Third, smart cars now have exterior cameras that record from numerous angles. Tesla vehicles, for instance, have eight cameras.[112] Tesla vehicles also have a "Sentry Mode," in which the vehicle is "continuously monitoring the environment around a car when it's left unattended."[113] The Tesla's Sentry Mode automatically takes video recordings when there is an event such as a person walking near the car. Additionally, when the driver hits the horn, the Tesla makes a recording from the exterior cameras so that an accident or other dangerous driving can be captured on video and saved.[114] Video footage is, of course, relevant if it captures criminal activity in progress. But video recordings can also be a valuable source of contextual evidence, such as what other vehicles were nearby or what was happening at a location prior to or after a crime.

Fourth, as explained in Part I, the Berla device is capable of downloading information from the driver's cell phone if the phone is connected to the vehicle via Bluetooth. The Berla device can give police access to call history, text messages, emails, and a wealth of other data. The police would be interested in this information in drug cases because distributors will use text messages to arrange

112. *See Advanced Sensor Coverage*, TESLA, https://www.tesla.com/autopilot (last visited Mar. 29, 2023).

113. *See Sentry Mode: Guarding Your Tesla*, TESLA, https://www.tesla.com/blog/sentry-mode-guarding-your-tesla (last visited Mar. 29, 2023).

114. *See* Kelly Lin, *Tesla Model 3's Honk to Record Dashcam Catches Hammer Flying Into Window*, MOTOR TREND (Jan. 3, 2020), https://www.motortrend.com/news/tesla-model-3-dashcam-records-hammer-flying-windshield/.

drug buys. As for low-level crimes (such as prostitution or possession of stolen property) and more serious crimes (such as kidnapping, robbery, and murder), text messages and other data from the phone could be relevant.[115]

In short, if courts follow longstanding automobile exception precedent, police would be able to download data from smart cars without a warrant so long as they have probable cause to believe the computer contains evidence of a criminal offense. And there are many offenses in every state's penal code for which police would have probable cause to search the vehicle. The key question, therefore, is whether police should follow longstanding automobile exception precedent or whether the Supreme Court's 2014 decision in *Riley v. California* suggests that courts should refuse to apply the automobile exception to smart car computers.

D. The Court Likely Will Not Extend Riley v. California*'s Search Warrant Requirement to Automobile Searches*

In *Riley v. California*, the Supreme Court unanimously held that police cannot search a cell phone incident to arrest without a warrant.[116] Up to that point, the Court had followed a bright-line rule allowing police to conduct a warrantless search incident to arrest of all containers found on an arrestee or in his immediate grabbing space.[117] In *Riley*, the Court concluded that cell phones contain so much private information that it would be unreasonable for police to be able to search the phones simply because the phone was found on a person who was being arrested.[118] The Court, therefore, carved out an exception to the search incident arrest doctrine requiring police to procure a warrant to search a cell phone.

Notably, the Court was careful not to hold that cell phones can never be searched without a warrant under any circumstances. The Court explained that "even though the search incident to arrest

115. Indeed, some of the incriminating information in *Riley v. California*, 573 U.S. 373, 379 (2014) was discovered in text messages.

116. *See Riley*, 573 U.S. at 401 ("Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.").

117. *See* United States v. Robinson, 414 U.S. 218 (1973); New York v. Belton, 453 U.S. 454 (1981).

118. *See Riley*, 573 U.S. at 403 ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'").

exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone."[119] And the Court then went on to spend two paragraphs explaining why the exigent circumstances exception (which itself is closely related to the automobile exception)[120] might justify a warrantless cell phone search. The *Riley* decision is silent on whether police can rely on the automobile exception to conduct a warrantless search of a cell phone. And the Court certainly did not address whether the automobile exception could apply to a smart car's computer because smart car technology was in its infancy in 2014.[121] Without any concrete guidance, we must attempt to predict whether the Supreme Court is likely to extend *Riley* to ban warrantless searches of electronic devices under the automobile exception, or whether the Court is likely to see such searches as exigencies not requiring a warrant.

The case for extending *Riley* to smart car searches under the automobile exception is not difficult to imagine. Smart cars are very much like cell phones because they hold an enormous amount of data.[122] Indeed, the screen in a Tesla looks like a large iPad built into the vehicle. Moreover, as explained in Part I, a small

119. *Id.* at 401–02.

120. From the beginning of its automobile exception jurisprudence, the Supreme Court relied on an exigency rationale, noting that procuring a warrant in the vehicle context "is not practicable . . . because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought." Carroll v. United States, 267 U.S. 132, 153 (1925).

121. One theory might be that because the Court only discussed the exigency exception as a way to warrantlessly search a cell phone, the Court was signaling that other exceptions could not be applicable. However, this is almost certainly wrong. At the time of the *Riley* decision, multiple courts had already upheld warrantless cell phone searches at the border. *See, e.g.*, United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc); United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008). At present, courts are split on whether agents need reasonable suspicion or no suspicion to search an electronic device at the border. *See, e.g.*, Gina R. Bohannon, *Cell Phones and the Border Search Exception: Circuit Splits Over the Line Between Sovereignty and Privacy*, 78 MD. L. REV. 635 (2019). Additionally, lower courts have approved warrantless cell phone searches of probationers and parolees. *See*, *e.g.*, United States v. Luna, 602 F. App'x 363 (9th Cir. 2015). Lower courts have also signaled (though in a less than unified approach) that some warrantless cell phone searches of students are permissible. *See* Ross Hoogstraten, Note, *Implications of the Constitutionality of Student Cell Phone Searches for* Riley v. California, 24 WM. & MARY BILL RTS. J. 879 (2016) (discussing lower court cases but arguing against permitting warrantless searches).

122. *See* George Dery, *Is A Friend Truly A Friend If You Can Just Leave It in the Garage? Toyota's and Honda's Concept Cars Could Have Significant Fourth Amendment Implications*, 55 AM. CRIM. L. REV. 585, 603 (2018) ("[R]ather than reinventing the wheel, the Court has often analyzed one technology by reference to another upon which it has already ruled.").

number of police agencies have Berla devices that enable law enforcement to extract not just the driving data stored in the car's computer but also some cell phone data that was communicated to the vehicle's infotainment system via Bluetooth.[123] In short, if police should not be able to engage in warrantless rummaging of a cell phone incident to arrest, it makes sense that they would not be permitted to engage in far-reaching searches of a smart car's computer under the automobile exception.

While the comparison between cell phones in *Riley* and smart cars under the automobile exception initially seems correct, there are at least five reasons why the Court might conclude that *Riley* is inapplicable and that police should, therefore, be permitted to conduct warrantless searches of smart car computers under the automobile exception.

1. Smart Cars Hold Less Information than Cell Phones

First, a smart car contains far less information than a cell phone. Cell phones contain thousands of photos, videos, emails, texts, and various other extremely private information. Moreover, phones contain hundreds of Apps that can paint a detailed (potentially intimate or embarrassing) picture of a person's life. A cell phone can reveal medical information, dating profiles, Tinder contacts, work communications, and tens of thousands of photos and videos.

Police will be able to extract far less private information from a smart car with a traditional data extraction device. As explained in Section I.B, if the driver connected her phone to the infotainment system and the police use a Berla device, the officers can dig out very personal information. Yet, there is no indication that the Berla device can extract *all* data on a cell phone. At least as publicly reported, the Berla device can only extract data that was transferred to the car during the time that the cell phone was connected to the vehicle. This means that officers will not be able to see all text messages and phone data, just what has been transferred through the vehicle. In short, while smart car data will offer a valuable window into the driver's private information, it is not likely to reveal nearly the quantity of cell phone data that was at issue in *Riley*.

123. *See supra* Section I.B.

2. A Lot of Vehicle Information Is Already Visible and Available to the Public

Second, a lot of information that smart cars contain is made available to the public. The locations where a car is driven, the speed traveled, and whether it has been driven erratically all occur out in the open and is readily visible to the public. As the Court explained nearly fifty years ago, "[a] car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view."[124] The result of that visibility is that a driver should not reasonably expect privacy in their movements.

For instance, in *United States v. Knotts*, a case in which police pre-installed a beeper in a barrel and used it to follow a vehicle, the Court explained that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[125] This principle is, of course, consistent with basic Fourth Amendment doctrine outside the automobile context that a person cannot expect privacy protection in that which she has made available to the public.[126] Accordingly, under longstanding precedent, a lot of the information disclosed by a smart car search—especially the black box data in the EDR—would not receive Fourth Amendment protection in the first place.

This second argument is admittedly subject to criticism. It would be cost-prohibitive for police to devote enough time and personnel to gather driving data from the naked-eye observation

124. Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion).

125. United States v. Knotts, 460 U.S. 276, 281 (1983).

126. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 41 (1988) (concluding that a person has no reasonable expectation of privacy in trash left at the curb because "the police cannot reasonably be expected to avert their eyes from evidence that could have been observed by any member of the public"); California v. Ciraolo, 476 U.S. 207, 213 (1986) (determining there is no search when police observe a backyard from navigable airspace because "the mere fact that an individual has taken measures to restrict some views of his activities [does not] preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible"); Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

that they can glean from searching a smart car.[127] As Professor Orin Kerr has observed, the Supreme Court deals with this problem by engaging in "equilibrium adjustment" to respond "to changing technology and social practice. When new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."[128] Arguably, the Court did just that in *United States v. Jones*,[129] when it held that police installing a GPS monitor on a car and using it to track the driver for twenty-eight days constituted a search.[130] Yet, past is not necessarily prologue and Professor Kerr's theory is just that—a theory. As Professor Christopher Slobogin has pointed out, the Court has failed to engage in effective equilibrium adjustment in prior technology cases, including automobile exception cases.[131] Thus, while it is, of course, possible that the Court will engage in equilibrium adjustment to disregard prior decisions about the scope of the automobile exception, that is speculative and far from certain. At present, the doctrine is quite clear that little to no Fourth Amendment protection is afforded to information that is made available to the public. Quite unlike cell phones, which are kept in a person's pocket, vehicles and their movements are typically in public view.

3. Cars Are Heavily Regulated and Receive Less Privacy Protection

A third difference between the cell phone search in *Riley* and smart car searches also relates to well-established Supreme Court doctrine about the automobile exception. The Supreme Court's

127. *See* William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1275 (1999) (explaining that warrants and probable cause requirements make searches more costly and thus less desirable for police to engage in).

128. *See* Orin S. Kerr, *An Equilibrium Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

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

130. Shortly after *Jones* was decided, Professor Kerr staked out the position that the Court's decision amounted to an equilibrium adjustment. *See* Orin S. Kerr, *Defending Equilibrium Adjustment*, 125 HARV. L. REV. F. 84, 87–89 (2011).

131. *See* Christopher Slobogin, *An Original Take on Originalism*, 125 HARV. L. REV. F. 14 (2011) (noting that *United States v. Knotts* upheld the automobile surveillance made possible by new technology—a beeper that had been pre-installed in a barrel before it was loaded into the vehicle). Professor Slobogin also argues that the Court failed to engage in equilibrium adjustment in other high-profile technology cases such as *Kyllo v. United States*, 533 U.S. 27 (2001), and *Smith v. Maryland*, 442 U.S. 735 (1979).

original rationale for the automobile exception was that vehicles were mobile. However, in later cases, the Court added a second rationale: vehicles are heavily regulated. In *California v. Carney*, the Court explained that warrantless searches of vehicles are justifiable because "there is a reduced expectation of privacy stemming from its use as a licensed motor vehicle subject to a range of police regulation inapplicable to a fixed dwelling."[132] The Court then reiterated that "the vehicle was licensed to "operate on public streets; [was] serviced in public places; . . . and [was] subject to extensive regulation and inspection."[133]

Cell phones, of course, are not heavily regulated. People do not need a license to use a phone. Your cell phone is not subject to annual inspection. No state requires the equivalent of an emissions test to make sure the phone is working properly. And while each cell phone has a serial number (like each vehicle has a VIN number), cell phones do not have the equivalent of license plates

132. California v. Carney, 471 U.S. 386, 393 (1985). Ironically, *Carney* introduced the rationale of reduced expectation of privacy for vehicles in a case involving a motor home, rather than an ordinary vehicle. *See id.* at 399 (Stevens, J., dissenting) ("In this case, the Court can barely glimpse the diverse lifestyles associated with recreational vehicles and mobile living quarters.").

133. *See id.* (quoting Rakas v. Illinois, 439 U.S. 128, 154 n.2, (1978)). The idea that vehicles can be subjected to warrantless searches because they are heavily regulated has never been particularly persuasive. It is true that drivers can be stopped for myriad reasons in the traffic code. But that is an imposition on the driver, not a reduced expectation of privacy in the vehicle. (Police can also stop people *walking* down the street.) The traffic code may justify the police in stopping the driver and the vehicle, but it does not (and could not) justify a search of the vehicle. And when police search a vehicle, it is ordinarily not because of a car's emissions or its roadworthiness. The State's regulation of vehicles does not, practically speaking, actually reduce a driver's expectation of privacy. The average person only takes a driver's license test once in their life. And they only have their car inspected for about an hour once a year. The rest of the time, the "extensive regulation" of vehicles has no effect on drivers. For further discussion of the problems with the extensive regulation rationale, *see* Carol A. Chase, *Privacy Takes a Back Seat: Putting the Automobile Exception Back on Track After Several Wrong Turns*, 41 B.C. L. REV. 71, 89-92 (1999). *See also* Tracey Maclin, *Cops and Cars: How the Automobile Drove Fourth Amendment Law*, 99 B.U. L. REV. 2317, 2353 (2019) ("Nobody—including the Justices—sincerely believes that motorists have diminished privacy interests in purses, wallets, and suitcases placed in cars . . . . [W]hat propelled the results in these cases were fictional claims regarding motorists' privacy in their effects, intellectually dishonest reasoning, and an effort to make car searches easier."). While the Court's "extensive regulation" rationale is not particularly persuasive, it is nevertheless governing law. In addition to *Carney*, see *New York v. Class*, 475 U.S. 106, 113 (1986) ("[A]utomobiles are justifiably the subject of pervasive regulation by the State. Every operator of a motor vehicle must expect that the State, in enforcing its regulations, will intrude to some extent upon that operator's privacy.").

that enable police to easily identify their owners. Anyone who has ever put a cell phone in a basket at trivia night knows that it is very difficult for the public (and the police) to know whose phone belongs to who. Put simply, one of the main rationales that the Court relies on for the automobile exception—"extensive regulation" of vehicles—is not present for cell phones. Thus, cell phones are arguably entitled to greater Fourth Amendment protection than the computers found in heavily regulated vehicles.

4. Police Cannot Use Faraday Bags for Automobiles

A fourth reason why *Riley*'s search warrant requirement for arrests may not be extended to the automobile exception is that it is much harder to immobilize data on a smart car than on a cell phone. In *Riley*, the Supreme Court recognized that police can preserve cell phone data by placing it in a Faraday bag, wrapping it in aluminum foil, or otherwise preventing it from accessing a network.[134] Any of these steps will protect the data from being remotely deleted while the police apply for a search warrant.[135] The ability to prevent remote wiping or automatic destruction of evidence was key to the Court's decision to eliminate the search incident to arrest doctrine for cell phones.[136]

However, the Court cannot be as confident about police ability to prevent destruction of evidence in smart cars. Cell phones are small and therefore can easily be placed inside of cheap Faraday bags or aluminum foil.[137] By contrast, police departments almost certainly do not have Faraday cages large enough to hold multi-ton vehicles. And it is obviously quite difficult to wrap a two-ton vehicle in aluminum foil! Moreover, Tesla allows owners to use an app to remotely operate the horn, air conditioning, and cameras.[138] A Tesla owner can also already share access to the vehicle and

134. *See* Riley v. California, 573 U.S. 373, 390-91 (2014); *see also* Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 WM. & MARY BILL RTS. J. 601 (2013).

135. *See Riley*, 573 U.S. at 390–91.

136. The Court's discussion of preserving data and preventing remote wiping covered multiple pages of the opinion. *See Riley*, 573 U.S. at 389–91.

137. Anyone can purchase a Faraday bag from Amazon.com for less than $20. A roll of aluminum foil costs only a few dollars.

138. *See* Stu Robarts, *Everything Tesla Drivers Can Do with the Tesla Mobile App*, SCREENRANT (Mar. 13, 2021), https://screenrant.com/tesla-vehicles-mobile-app-features/.

almost all functions on the app with five other people.[139] As technology improves, it may become possible for car owners to remotely erase data from their vehicles. If that comes to pass, it would be a stark contrast from the certainty that cell phone data can be preserved with a Faraday bag or aluminum foil.

5. The Automobile Exception Is Based on Probable Cause and Is Not Automatic

Finally, and perhaps most importantly, there is a fundamental difference between the search incident to arrest doctrine at issue in *Riley*, which is an automatic search based on zero suspicion, and the automobile exception, which requires police to have probable cause. Under the search incident to arrest doctrine, the right to search is automatic.[140] Police can arrest a person for a minor offense—for instance jaywalking or public urination—and then automatically conduct a search incident to arrest. While the search incident to arrest doctrine is premised on the idea that an arrestee could destroy evidence or pose a danger to the officer, the police do not have to show in any particular case that the arrestee is dangerous or that he has evidence on him that he would be in a position to destroy. The police can search automatically, regardless of the facts of the particular case. When it came to cell phones, it was not hard to see how the Court felt the need to rebalance the equities given how much blanket authority the doctrine afforded police to search devices that carry tremendous amounts of private information.

The automobile exception is quite different. It does not authorize an automatic search. There can be no general rummaging that is completely disconnected from the crime the police are on the scene to investigate. Instead, the police can only invoke the automobile exception if they have probable cause.[141]

Given that probable cause is required for searches under the automobile exception, the Court may see a warrantless search of a smart car computer as not nearly as outrageous as the automatic,

139. *See* Rob Maurer, *Tesla Adds "Car Access" Sharing Feature*, THE STREET (June 7, 2020), https://www.thestreet.com/tesla/articles/tesla-adds-car-access-sharing-feature.

140. *See* United States v. Robinson, 414 U.S. 218, 235 (1973); Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 34 (2008).

141. *See supra* notes 96–110 and accompanying text.

suspicionless search incident to arrest at issue in *Riley*. Searching a smart car computer under the automobile exception will still require the police to have individualized suspicion for a particular offense that could plausibly be held in the car's computer. That is a far cry from police rummaging through a cell phone with no suspicion after arresting the person for a minor offense.

* * *

In short, there are multiple plausible arguments why *Riley*'s warrant requirement for searches incident to arrest might not be extended to automobile searches: (1) Smart cars contain a smaller amount of private information than cell phones. (2) Unlike cell phones, a considerable amount of smart car information is already made available to the public because the location and movement of a vehicle are publicly visible. (3) Smart cars are heavily regulated and entitled to less Fourth Amendment privacy protection. (4) It is harder to immobilize smart car data than a cell phone because police departments likely do not have a Faraday cage large enough to hold an automobile. (5) And the automobile exception (unlike the search incident to arrest doctrine) requires probable cause before the police can rely on it to engage in a search.

Of course, the *Riley* decision staked out a strong position on the privacy of cell phone data and the importance of a search warrant. These lofty principles may lead the Supreme Court to ultimately conclude that police cannot conduct warrantless searches of smart car computers under the automobile exception. But that outcome is far from ordained. And, as Part III details, even if the Court were to forbid smart car computer searches under the automobile exception, it will likely take the Supreme Court many years (and likely even decades) to do so.

III: SUPREME COURT GUIDANCE IS LIKELY TO TAKE A LONG TIME

Legislators, lawyers, and scholars often presume that it is exclusively the Supreme Court's job to resolve complicated search and seizure questions. Legislatures often choose to "sit out" search and seizure debates because there is no need to intervene if the courts will handle the issues.[142] This Part argues that waiting for

142. For instance, in the leadup to *Riley*, state legislatures could have banned warrantless cell phone searches incident to arrest but failed to do so. *See* Gershowitz,

the Supreme Court is ill-advised, however, because it could be years or even decades before the Court addresses smart car computer searches. During that time, tens of millions of cars will log billions of miles on the roads and potentially be subject to many warrantless searches.

To understand how long it takes the Supreme Court to act, consider the time it took the Court to forbid warrantless cell phone searches incident to arrest. At first glance, it seems like the Court moved relatively quickly. The most prominent case rejecting the search incident to arrest of a cell phone was the Ohio Supreme Court's decision in *State v. Smith*, which came in December 2009.[143] Less than five years later, the Court decided *Riley*. In the world of Supreme Court decision-making, five years seems quite quick.

But the backstory is much longer. Federal courts had been dealing with searches incident to arrest of cell phones since at least 2003.[144] And the controversy over warrantless searches of electronic devices actually dates back to the 1990s. Before cell phones, it was common for drug dealers to use pagers to distribute their narcotics. Law enforcement officers quickly figured this out. And because pagers could only hold a few numbers and the next call would therefore destroy evidence of a prior call, police began to search pagers incident to arrest without a warrant. The earliest reported case upholding the search of a pager incident to arrest occurred in 1993.[145] While pagers of course held less data than (even early

Password Protected, *supra* note 93, at 1146–47 ("Despite the dozens of cases involving warrantless searches of cell phones over the last decade, the author is unaware of a single proposed bill to restrict such searches, or even a solitary legislative hearing to investigate the increasingly common practice."). Eventually, California passed legislation, though it was vetoed by the governor on the ground that "[t]he courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections." Bob Egelko, *Brown Vetoes Bill to Limit Cell Phone Searches*, S.F. CHRON. (Oct. 10, 2011), https://www.sfgate.com/bayarea/article/Brown-vetoes-bill-to-limit-cell-phone-searches-2328058.php.

143. State v. Smith, 920 N.E.2d 949 (Ohio 2009). Another prominent decision reaching the opposite conclusion was issued by the Fifth Circuit in 2007. *See* United States v. Finley, 477 F.3d 250 (5th Cir. 2007).

144. *See* United States v. Parada, 289 F. Supp. 2d 1291, 1303–04 (D. Kan. 2003) (upholding search of stored numbers on a cell phone to prevent destruction of evidence). For a list of other early cases, see Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 140, at 39 nn.82–83.

145. *See* United States v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993). For additional cases from the early 1990s, see Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 140, at 37 n.67.

model) cell phones, the concept of searching an electronic device was identical. Accordingly, it is more accurate to say that it actually took the Supreme Court over twenty years—from at least 1993 to 2014—to decide the question of whether it was constitutional to search an electronic device incident to arrest without a warrant.

The Court has been similarly slow in resolving the question of how much suspicion customs agents need to search a cell phone at the international border. In 2009, the Department of Homeland Security "issued directives that authorize their agents to inspect any electronic devices that travelers seek to carry across an international border into the United States."[146] The regulations provided that ICE and Customs agents did not need suspicion before searching the phones.[147] The Ninth Circuit addressed the constitutionality of suspicionless searches of electronic devices at the border nearly a decade ago in 2013.[148] Federal courts have since split on the scope of the border search exception for forensic searches of electronic devices[149] and that split has existed for nearly four years.[150] More than a dozen years after the DHS regulations, and more than four years since the circuit split was created, the Supreme Court has yet to clarify the level of suspicion and the scope of border searches of cell phones.

The Court's lack of guidance on the border search of cell phones is particularly striking given how many cell phone searches have likely been conducted over the last dozen years. In 2018, there were an estimated 33,000 border searches of cell phones and laptops,

146. Abidor v. Napolitano, 990 F. Supp. 2d 260, 264 (E.D.N.Y. 2013).

147. *See id.*

148. *See* United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc) (upholding manual searches of cell phones with no suspicion).

149. *Compare* Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021) (allowing search for all types of evidence); United States v. Touset, 890 F.3d 1227 (11th Cir. 2018), *with* United States v. Cano, 934 F.3d 1002 (9th Cir. 2019) (concluding that "officials must reasonably suspect that the cell phone contains digital contraband" and that "searches at the border, whether manual or forensic, must be limited in scope to a search for digital contraband"); United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018).

150. *See Touset*, 890 F.3d 1227 (11th Cir. 2018) (not requiring reasonable suspicion and noting that "[t]o be sure, the Fourth and the Ninth Circuits have concluded—in divided decisions—that the Fourth Amendment requires at least reasonable suspicion for forensic searches of electronic devices at the border").

which represented a 400% increase from three years earlier.[151] By 2019, the number of searches had climbed to 41,000.[152] Moreover, consider that the Supreme Court has been taking a record low number of argued cases each term—just 56 merits cases in the 2020 term.[153] Indeed, for all the attention that cases like *Riley* and *Jones* receive, the Court has actually only decided a handful of criminal procedure cases focused on technology issues.[154] And that is in spite of the fact that electronic devices are ubiquitous.

Or consider the limited guidance on third-party data. In 2018, the Supreme Court issued its landmark decision in *Carpenter v. United States*, holding that police needed a warrant to obtain more than seven days of historical cell site location data.[155] The *Carpenter* decision left many open questions and understandably the Court remarked that we "do not begin to claim all the answers today . . . and therefore decide no more than the case before us."[156] Those questions are both interesting and significant. For instance, if the police collect enough data for there to have been a search, when did that search occur?[157] Should the decision be extended to wearable devices such as Fitbits[158] or to genetic materials held by third parties such as 23andMe?[159] Or what should happen to the

151. *See* Matthew S. Schwartz, *ACLU: Border Agents Violate Constitution When They Search Electronic Devices*, NPR (May 2, 2019), https://www.npr.org/2019/05/02/719337356/aclu-border-agents-violate-constitution-when-they-search-electronic-devices.

152. *See* Kristina Davis, *Returning from Travel Abroad? A Court Put Limits on Border Officers Rummaging Through Your Phone*, SAN DIEGO UNION-TRIB. (July 24, 2021), https://www.sandiegouniontribune.com/news/courts/story/2021-07-24/court-ruling-phone-search.

153. *See Stat Pack for the Supreme Court's 2020–21 Term*, SCOTUSBLOG (July 2, 2021), https://www.scotusblog.com/wp-content/uploads/2021/07/Final-Stat-Pack-7.2.2021.pdf. The Court has, however, increased the size of its "shadow docket" of non-argued emergency orders. For one of many critical takes on the shadow docket, see Stephen I. Vladeck, *The Solicitor General and the Shadow Docket*, 133 HARV. L. REV. 123 (2019).

154. Consider that the search and seizure chapter of the leading computer crime textbook is filled with numerous lower court cases, but few Supreme Court decisions. *See* ORIN S. KERR, COMPUTER CRIME LAW, ch. 5 (4th ed. 2018).

155. Carpenter v. United States, 138 S. Ct. 2206 (2018).

156. *Id.* at 2220–21 n.4.

157. *See* Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47, 90 (2020) ("Did the search occur when the third-party cell phone company collected the information, when the police asked for it, when they received it, when they examined the digital information or at some other time?").

158. *See* Ashleigh Elizabeth Draft, *Pacemakers, Fitbits and the Fourth Amendment: Privacy Implications for Medical Implants and Wearable Technology*, 2019 MICH. ST. L. REV. 511 (2019).

159. *See* Natalie Ram, *Genetic Privacy After Carpenter*, 105 VA. L. REV. 1357 (2019).

location data, driving data, or perhaps even Sentry Mode camera recordings that may be sent from a single Tesla car to Tesla the company?[160] Nearly four years after *Carpenter*, the Court has never taken a follow-up case to answer any of the complicated issues left open in *Carpenter*, and it shows no signs of doing so anytime soon.

The Court's plodding pace in answering search and seizure questions posed by new technology is problematic given how quickly smart cars are proliferating. Tesla released its first mass-produced vehicle—the Model S—in 2012.[161] In 2013, Tesla sold between 18,000 and 22,000 Model S vehicles.[162] Sales have increased dramatically since then. Only six years after the Model S release, Tesla's annual sales had jumped to 367,000 cars, which was more than the previous two years combined.[163] By 2021, Tesla was selling more than 200,000 cars per quarter—over 800,000 per year.[164] When we add other smart cars, there are tens of millions of vehicles that enable drivers to connect their cell phones to the infotainment systems to share data with the vehicle.[165] Now fast forward two decades—the same period from the first pager case to the *Riley* decision—and think about how many smart cars will be on the road in the United States in the year 2042.

Consider also how much more sophisticated smart cars will become in the next few decades and how much private data they

160. A Sept. 1, 2021, over-the-air update to Tesla vehicles provided a new opt-in tool: "Dashcam can now automatically save clips whenever your vehicle detects the occurrence of a safety event (such as an accident or airbag deployment). Recordings captured are stored locally and never transmitted to Tesla." *2021.24.5 Release Notes*, NOT A TESLA APP, https://www.notateslaapp.com/software-updates/version/2021.24.5/release-notes (last visited Mar. 29, 2023). While this data is not transmitted to Tesla the company, it of course begs the question of what other data from the car is being, or has been, transmitted from the vehicle to the company's database and computers.

161. *See* Brittany Chang, *Every Major Change Tesla Has Made to the Model S Throughout the Years*, BUS. INSIDER (Aug. 24, 2019), https://www.businessinsider.com/tesla-model-s-every-major-change-2019-8.

162. *See* John Voelcker, *How Many Tesla Model S Electric Cars Have Been Built So Far?*, GREEN CAR RPTS. (Jan. 15, 2014), https://www.greencarreports.com/news/1089703_how-many-tesla-model-s-electric-cars-have-been-built-so-far.

163. *See* Sean O'Kane, *Tesla Sold More Cars in 2019 Than In the Previous Two Years Combined*, THE VERGE (Jan. 3, 2020), https://www.theverge.com/2020/1/3/21047233/tesla-2019-deliveries-q4-record-model-3-sales.

164. *See* Andrew J. Hawkins, *Tesla Delivered Over 200,000 Cars in the Second Quarter of 2021*, THE VERGE (July 2, 2021), https://www.theverge.com/2021/7/2/22560608/tesla-q2-2021-deliveries-elon-musk.

165. *See* Donovan, *supra* note 13 and accompanying text.

will hold. Moreover, consider how much better and cheaper the data extraction technology is likely to be in the years to come. It seems reasonable to conclude that in the next few decades companies will create data extraction devices that extract even more information than they presently do. And it seems reasonable to believe that the cost of the technology (especially the more rudimentary devices) will come down, thus enabling many more police departments to acquire sophisticated data extraction devices.[166]

With more smart cars on the road and law enforcement in possession of more data extraction devices that operate more effectively, it is likely that police will be more tempted to search smart car computers for the valuable information they contain. Indeed, it is quite possible that a few law enforcement agencies are already using data extraction devices to conduct warrantless searches of smart cars[167] and only then applying for warrants if the initial warrantless search yielded valuable evidence.[168]

Assuming that we have a problem with warrantless smart car computer searches (or that we will have a growing problem in the future), the natural reaction is to say that we can rely on lower courts to effectively handle those cases. But that argument is problematic. The lower courts are likely to follow the existing doctrinal precedent described in Part II that would authorize such searches under the automobile exception. Lower courts typically do not reach out and predict that the Supreme Court might overrule its current precedent.[169] They are supposed to be guided

166. By way of comparison, consider the thermal imaging devices at issue in Kyllo v. United States, 533 U.S. 27, 34 (2001), which the Court noted were not in "general public use." Within a decade, thermal imagers were "available for sale online, relatively cheaply" and a company was even preparing to make them available as a cell phone app. Katie Barlow, *Thermal Imaging Gets More Common But the Courts Haven't Caught Up*, NPR (Feb. 27, 2014), https://www.npr.org/sections/alltechconsidered/2014/02/25/282523377/thermal-imaging-gets-more-common-but-the-courts-havent-caught-up.

167. *See supra* notes 39–45 and accompanying text (discussing cases where police acknowledged warrantless searches of EDR data from vehicles).

168. The best analogy here is to the infamous independent source exception case of Murray v. United States, 487 U.S. 533 (1988) in which the police entered a warehouse based on their suspicion of drug activity and only took the time to apply for a warrant after confirming that there were in fact drugs in the warehouse. For trenchant criticism of the incentives such an approach creates, see Craig M. Bradley, Murray v. United States: *The Bell Tolls for the Search Warrant Requirement*, 64 IND. L.J. 907 (1989).

169. *See* Aaron-Andrew P. Bruhl, *Deciding When to Decide: How Appellate Procedure Distributes the Costs of Legal Change*, 96 CORNELL L. REV. 203, 229 (2011) (explaining that "a

by existing precedent.[170] For that reason, most lower courts that were confronted with warrantless searches of cell phones incident to arrest prior to *Riley* grudgingly upheld such searches.[171]

In short, the Supreme Court is unlikely to quickly resolve the conflict between historical automobile exception precedent and the argument extrapolated from *Riley* that the doctrine should be changed. In the meantime, lower courts will be guided by existing precedent that would authorize warrantless searches of smart car computers under the automobile exception.

IV. FEDERAL AND STATE STATUTES PROVIDES MINIMAL AND INCOMPLETE PRIVACY PROTECTION FOR CELL PHONE DATA TRANSFERRED TO VEHICLES

As explained in Part II above, there is a strong argument that the automobile exception permits warrantless searches of smart car computers without running afoul of the Fourth Amendment. Congress and state legislatures can, of course, provide more privacy protection than required by the Fourth Amendment. And the legislatures have taken some protective actions with respect to driving data. Nevertheless, the statutory restrictions imposed on law enforcement are minimal, outdated, and ineffective.

A. Federal Attempts to Protect Driver Data

In 2015, Congress passed, and President Obama signed, the Driver Privacy Act, which made clear that the owner of a vehicle also owned the vehicle's EDR black box data. The Driver Privacy Act specified that no one other than the vehicle owner could access the EDR data unless "a court or other judicial or administrative

substantial majority" of federal circuit courts upheld the Federal Sentencing Guidelines after *Blakely v. Washington* even though it appeared fairly clear that the Supreme Court would soon rely on that decision to find the guidelines to be unconstitutional); *see also* Richard M. Re, *Narrowing Supreme Court Precedent from Below*, 104 GEO. L.J. 921, 940 (2016) (noting that "in an unusual subset of cases a lower court might predict that the higher court will overrule or otherwise set aside its own case law").

170. *See* Re, *supra* note 169, at 923; Hutto v. Davis, 454 U.S. 370, 375 (1982) ("But unless we wish anarchy to prevail within the federal judicial system, a precedent of this Court must be followed by the lower federal courts no matter how misguided the judges of those courts may think it to be.").

171. *See* Gershowitz, *Password Protected*, *supra* note 93, at 1143 (explaining before the *Riley* decision that "most courts to address the constitutionality of searching cell phones incident to arrest have upheld the practice").

authority having jurisdiction (A) authorizes the retrieval of the data; and (B) to the extent that there is retrieved data, the data is subject to the standards for admission into evidence required by the court or other administrative authority."[172]

While the Driver Privacy Act places some restrictions on retrieval of car data it is important to see how limited it is. First, nowhere does the statute specify that a warrant is required. The language states that "the data is subject to the standards for admission into evidence required by that court or other administrative authority."[173] It is unclear what this language means, but it appears to be geared toward ensuring the reliability of the data and the chain of custody, not a requirement that it be obtained with a search warrant. Indeed, a warrant requirement is impossible given that the text of the statute says the data retrieval can be authorized by an "administrative authority," which of course is not a neutral and detached magistrate capable of issuing a search warrant.

Unsurprisingly, a search of Westlaw's caselaw database for "Driver Privacy Act" returns only a handful of cases where the law is referenced in passing. No case has ever held, or even suggested, that the statute requires a warrant before police can retrieve the black box EDR data.

Second, even if the Driver Privacy Act did impose a warrant requirement (which it does not) the statute only applies to EDR black box data. The relevant portion of the statute is captioned "Limitations on Data Retrieval from Vehicle Event Data Recorders."[174] The statute does not apply to other computer systems in the vehicle. The limited scope of the statute was not lost on Berla, the company that makes the data extraction tool for infotainment data. Immediately after the Driver Privacy Act was enacted, Berla issued a guidance document specifically telling law enforcement that the statute does not apply to infotainment data:

> One very important thing to note is that The Driver Privacy Act of 2015 only covers Event Data Recorders (EDRs) as defined by 49

172. *See* Driver Privacy Act of 2015, Pub. L. No. 114-94, § 23402(b)(1), 129 Stat. 1712–13 (2015). The statute also provides for data to be retrieved in other ways not relevant to this article, such as if the owner consents or if it is necessary for an emergency medical response or traffic research. *See id.* § 23402(b)2–5, 129 Stat. 1712–13.

173. *See id.* § 23402, 129 Stat. 1712–13.

174. *See id.*

> CFR 563.5, which is limited to special purpose devices that record very specific types of information "just prior to a crash event or during a crash event." The act only mandates provisions related to data stored within an Event Data Recorder and, therefore, it does not impact the Infotainment and Telematics systems targeted by iVe.[175]

Berla's reading of the statute and regulations is correct. The Driver Privacy Act only covers the black box data. Because the statute does not require a warrant and applies only to black box data, rather than the more private infotainment data, the statute is essentially meaningless in a smart car world.

In 2021, Senator Ron Wyden drafted a bill called "Closing the Warrantless Digital Car Search Loophole Act of 2021"[176] that would require law enforcement to obtain a warrant to take almost any electronic data from a vehicle.[177] The bill would only provide exceptions for consent or emergency situation in which the data is necessary to prevent immediate death or serious physical injury.[178] After being introduced, the bill was referred to the Judiciary Committee, where it has languished.

The only previous effort to amend the Driver Privacy Act was far more modest, and it also failed. That proposed amendment would only require manufacturers to disclose the existence of the black box recorders and that "the information recorded by the event data recorder also may be used in a law enforcement proceeding."[179] However, even that amendment failed to make it out of committee.[180] In short, the Driver Privacy Act is toothless.

---

175. *The Driver Privacy Act of 2015*, BERLA (Dec. 21, 2015), https://berla.co/the-driver-privacy-act-of-2015/.

176. *See* Closing the Warrantless Digital Car Search Loophole Act of 2021, S. 3231, 117th Cong. (2021).

177. The bill broadly defines "covered vehicle data" to include:

> all onboard and telematics data generated by, processed by, or stored on a noncommercial vehicle using computing, storage and communication systems installed, attached to, or carried in the vehicle, including diagnostic data, entertainment system data, navigation data, images or data captured by onboard sensors, or cameras, including images or data used to support automated features or autonomous driving, internet access, and communication to and from vehicle occupants.

Id.

178. *See id.*

179. *See* Black Box Privacy Protection Act, H.R. 3568, 115 Cong. § 3(a)(i)(3) (2017).

180. *See id.*

B. State Attempts to Protect Driver Data

Some states have enacted similar laws designed to protect drivers' data.[181] While well-intentioned, these laws are not helpful for protecting the privacy of data in smart car computers. For instance, California's statute authorizes the release of EDR data "[i]n response to an order of a court having jurisdiction to issue the order."[182] New York's statute is similar and allows the police to extract EDR data "[i]n response to an order of a court or other judicial or administrative authority having jurisdiction to issue the order."[183] It is important to recognize that, like the federal Driver Privacy Act, both the California and New York statutes are limited to EDR "black box" data and offer no protection to the far more private cell phone data that runs through the car's infotainment system. Additionally, neither the California nor New York laws impose a warrant requirement and instead require only a court order, which can be granted under a lower standard of proof.[184] Another dozen statutes are quite similar and thus quite ineffective.[185]

Virginia's statute—which was adopted in 2006 and has not been updated to account for smart cars—is slightly more protective but is similarly problematic. Like the federal statute and the California and New York laws, the Virginia statute appears to be limited to EDR "black box" data.[186] Moreover, the Virginia statute provides that

181. *See* Harper, *supra* note 14, at 1269.

182. CAL. VEH. CODE § 9951(c)(2) (2021).

183. N.Y. VEH. & TRAF. L. § 416-b(3)(b).

184. By way of example, court orders under the Stored Communications Act require specific and articulable facts that the information is relevant to an ongoing criminal investigation. A warrant requires probable cause, which is a higher standard. *See* 18 U.S.C. § 2703; *see also* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 361 (2015) (reviewing different mechanisms in the Stored Communications Act); *In re* Application of U.S. for an Ord. Directing a Provider of Elec. Commc'n Serv. to Disclose Recs. to Gov't, 620 F.3d 304, 319 (3d Cir. 2010) ("A warrant requires probable cause, but there is no such explicit requirement for securing a § 2703(d) order.").

185. The National Conference of State Legislatures tracks statutes dealing with EDR devices. *See* NAT'L CONF. OF STATE LEGISLATURES, PRIVACY OF DATA FROM EVENT DATA RECORDERS: STATE STATUTES (Aug. 8, 2021) (removed from the organization's website) (archived version available https://web.archive.org/web/20220901012834/http:/www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx) (last visited Apr. 3, 2023).

186. Recorded data is defined to mean "the data stored or preserved electronically in a recording device identifying performance or operation information about the motor vehicle." VA. CODE § 46.2-1088.6.

> [t]he recorded data [can be] accessed by law enforcement in the course of an investigation where constitutionally permissible and in accordance with any applicable law regarding searches and seizures upon probable cause to believe that the recording device contains evidence relating to a violation of the laws of the Commonwealth or the United States.[187]

This language is seemingly more protective than the federal, California, and New York laws. But so long as the police can point to probable cause and a valid warrant exception—such as the automobile exception—they seemingly can extract the data because doing so would not violate federal or Virginia law.

Two states—Montana[188] and New Jersey[189]—have statutes that mention warrants, but both of those states also indicate that police can acquire black box data from court orders. The New Jersey statute comes closest to providing protection to cell phone data captured by the car's infotainment system because the statute applies not only to black box data but also to "sensing and diagnostic modules, electronic control modules, automatic crash notification systems, geographic information systems, and *any other device that records and preserves data that can be accessed through that vehicle*."[190] This more expansive language would seemingly cover Berla devices used to extract text messages, call history, contacts, emails, photos and other data from the car's infotainment system. Of course, as noted above, the New Jersey statute does not require a warrant and can be obtained with a lesser standard of proof under a court order.

To summarize, the federal Driver Privacy Act, while adopted in the relatively recent past, is outdated and inadequate. Most states have no comparable law in place to protect against police searching

187. *Id.*

188. *See* MONT. CODE ANN. § 61-12-1004(1)(a) & (c) (2015). Montana's statute specifies that car data can be retrieved pursuant to a warrant, but it also indicates that such data can be retrieved with a court order. And Montana's statute is specifically limited to EDR data. Accordingly, the Montana statute appears to be as unhelpful as the federal, California, New York, and Virginia laws.

189. *See* N.J. STAT. ANN. § 39:10B-8(a)(2) (2015) ("The recorded data is retrieved or obtained by a law enforcement officer pursuant to a search warrant issued by a judge of the Superior Court or upon order by a court of competent jurisdiction or, except for recorded data concerning vehicle location, a grand jury subpoena."). While not a model of clarity, New Jersey's law indicates that a warrant is not required.

190. *See* N.J. STAT. ANN. § 39:10B-7 (2015) (emphasis added).

vehicle data. Roughly one-third of states do have a statute in place, but almost all of those statutes are limited to EDR black box data. Only New Jersey appears to have a statute that potentially extends to the private infotainment data that can be extracted by a Berla device. And none of the statutes—not even New Jersey's broader law—require a warrant. In sum, there is basically no statutory protection preventing police from warrantlessly downloading private data from a smart car anywhere in the United States. As noted in section I.B, the Berla device is capable of extracting an enormous amount of private information such as text messages, call histories, and social media data. Better statutory protection is therefore necessary.

V. LEGISLATURES HAVE THE POWER TO IMPOSE A STATUTORY WARRANT REQUIREMENT

Not surprisingly, most Fourth Amendment scholars and criminal lawyers approach search and seizure questions by first asking whether the Fourth Amendment requires a warrant. When the U.S. Supreme Court or lower federal courts reject the argument that a warrant is required, most observers tend to look next to state supreme courts to protect individual liberties.[191] These scholars and defense attorneys typically argue that state constitutions should provide more search and seizure protection than the Fourth Amendment.[192] The gravitational pull from the federal courts is strong though. And scholars have increasingly recognized that state supreme courts are typically unwilling to interpret their state constitutions more broadly.[193] Accordingly, a court-centered solution to smart car searches may well be futile. This Part therefore proposes a legislative rather than judicial solution. Legislatures should use their authority to impose a statutory requirement that police obtain a search warrant in order to search a smart car's

191. Most famously, see William J. Brennan, *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489 (1977).

192. *See, e.g.*, J. Thomas Sullivan, *Developing a State Constitutional Law Strategy in New Mexico Criminal Prosecutions*, 39 N.M. L. REV. 407 (2009).

193. *See* Neal Devins, *State Constitutionalism in the Age of Party Polarization*, 71 RUTGERS U.L. REV. 1129, 1132–33 (2019) ("I am skeptical that there will be a renaissance of state constitutionalism in the age of party polarization . . . . [S]tate supreme courts are unlikely to fill the void by interpreting their constitutions more broadly than the U.S. Supreme Court interprets the Federal Constitution.").

computer—particularly private cell phone data that runs through the infotainment system.

While scholars often ignore legislative solutions to protect criminal suspects from intrusive searches and seizures, there are multiple examples of legislatures affording greater protection than the Fourth Amendment requires. The most well-known example of legislative rules that limit police investigatory power are the restrictions on wiretaps. Both Congress and state legislatures have imposed limitations on wiretaps that go beyond what the Fourth Amendment requires. Federal and state statutes limit police to seeking wiretaps only for a select set of serious crimes.[194] And the federal wiretap statute requires that the intercept "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter."[195] Some state even have "all party" wiretap and eavesdropping statutes that require police to obtain judicial authorization, even if one of the parties has consented to the recording.[196]

State legislatures have also enacted statutes to protect electronic data. Consider cell site location information for example. Prior to the *Carpenter* decision, states imposed restrictions on police authority to obtain electronic communications (including cell phone) data from third-party carriers.[197] Some of those statutes are even more protective than *Carpenter*, which only requires a warrant for more than seven days of cell site data.[198] For instance, Maine's statute provides that law enforcement may never obtain location

194. *See, e.g.*, 18 U.S.C. § 2516; Md. Code Ann., Cts. & Jud. Proc. § 10-406.

195. 18 U.S.C.A. § 2518(5).

196. *See, e.g.*, 720 ILCS § 5/14-2(b)(1) (forbidding police from using an eavesdropping device unless "acting pursuant to an order of interception"); Rauvin Johl, *Reassessing Wiretap and Eavesdropping Statutes: Making One-Party Consent the Default*, 12 HARV. L. & POL'Y REV. 177, 180 (2018) ("Eleven states have all-party consent schemes. Unlike one-party systems, an all-party consent regime requires individuals who are recording a communication to have the consent of every party involved.").

197. *See* Tracy Lien, *Everything You Need To Know About California's New Electronic Communications Privacy Act*, L.A. TIMES (Oct. 9, 2015), https://www.latimes.com/business/technology/la-fi-tn-california-electronic-privacy-20151009-story.html (explaining that California's new law "bars any state law enforcement agency from getting its hands on any user data without first obtaining a warrant from a judge" and that "Maine and Utah have similarly comprehensive protections").

198. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

information without a valid warrant.[199] Prior to *Carpenter*, Texas amended its Code of Criminal Procedure to require a search warrant for "electronic customer data held in electronic storage, including the contents of and records and other information related to a wire communication or electronic communication held in electronic storage."[200]

A few states have gone further by creating statutory guarantees that are broadly protective of digital data. In 2016, California passed the Electronic Communications Privacy Act,[201] which "requires law enforcement to obtain a warrant to access almost all electronic communication information."[202] In 2019, Utah enacted a statute providing that "state law enforcement can only access someone's transmitted or stored digital data (including writing, images, and audio) if a court issues a search warrant."[203] These state statutes impose search warrant requirements on far more police activity than is required by the Fourth Amendment.

Outside of electronic data and wiretaps, legislatures have imposed warrant requirements for more traditional searches. For example, the Texas legislature expressed concern in 2015 about "[r]ecent incidents in Texas in which law enforcement officers, pursuant to [warrant] exceptions, conducted body cavity searches of individuals during traffic stops without a warrant."[204] The Texas Legislature noted that there were a lack of "policies among law enforcement agencies prohibiting such warrantless searches."[205] In short, the Legislature thought police should always have to get a warrant before conducting a body cavity search even though the courts had not imposed such a blanket requirement.

199. *See* ME. REV. STAT. tit. 16, § 648 ("Except as provided in this subchapter, a government entity may not obtain location information without a valid warrant issued by a duly authorized justice, judge or justice of the peace using procedures established pursuant to Title 15, section 55 or 56.").

200. TEX. CODE CRIM. PROC. § 18.02(13).

201. *See* CAL. PENAL CODE §§ 1546 et seq.

202. Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, 33 BERKELEY TECH. L.J. 131, 134 (2018).

203. Nick Sibilla, *Utah Bans Police From Searching Digital Data Without a Warrant, Closes Fourth Amendment Loophole*, FORBES (Apr. 16, 2019, 11:35 AM), https://www.forbes.com/sites/nicksibilla/2019/04/16/utah-bans-police-from-searching-digital-data-without-a-warrant-closes-fourth-amendment-loophole/?sh=1d6c83687630 (discussing H.B. 57, the Utah Electronic Information and Data Privacy Act).

204. H.B. 324, Texas 84th Legislature, (Tex. 2015).

205. *Id.*

Accordingly, the Texas Legislature passed (and the governor signed) a statute providing that "[n]otwithstanding any other law, a peace officer may not conduct a body cavity search of a person during a traffic stop unless the officer first obtains a search warrant pursuant to this chapter authorizing the body cavity search."[206] Other states have likewise enacted laws requiring a search warrant before police can conduct a body cavity search, even though there is no such bright-line rule required by the Fourth Amendment.[207]

Or consider racial profiling—another problem that comes up in traditional investigative stops. Longstanding Supreme Court precedent permits police to stop drivers as long as the officers can point to a violation of the traffic code.[208] If the police decide to let the detained individual go on their way, the officers are not obligated to document who was stopped or their demographic background information.[209] The Fourth Amendment simply does not require police to create a record that documents who was stopped and why. Yet, in an effort to reduce racial profiling, some state legislatures have enacted statutes that require police to record the race, gender, and age of drivers who are stopped, even though the Fourth Amendment imposes no such requirement.[210]

Most recently, two states have enacted laws that require police to obtain judicial authorization before using a consumer DNA

206. TEX. CODE CRIM. PROC. § 18.24(b).

207. *See, e.g.*, OHIO REV. CODE § 2933.32(4) ("Unless there is a legitimate medical reason or medical emergency justifying a warrantless search, a body cavity search shall be conducted only after a search warrant is issued that authorizes the search."); Rev. Wash. Code § 10.79.080(1) ("No person may be subjected to a body cavity search by or at the direction of a law enforcement agency unless a search warrant is issued pursuant to superior court criminal rules.").

208. *See* Whren v. United States, 517 U.S. 806, 819 (1996).

209. *See* Wayne A. Logan, *Reasonableness As A Rule: A Paean to Justice O'Connor's Dissent in Atwater v. City of Lago Vista*, 79 MISS. L.J. 115, 128–29 (2009) (noting that arrest data "fail to reflect instances when police 'unarrest' individuals—that is, police conduct a search ostensibly based on an arrest for a minor offense, find no evidence or contraband resulting in a more serious prosecution, and release an individual with a mere citation or warning"). *Accord* Florida v. Harris, 508 U.S. 247 (2013) (rejecting argument that a drug dog's field performance needs to be documented to determine whether the dog's alert can create probable cause to search).

210. *See* Floyd Weatherspoon, *Ending Racial Profiling of African-Americans in the Selective Enforcement of Laws: In Search of Viable Remedies*, 65 U. PITT. L. REV. 721, 740 (2004) ("A majority of states have passed legislation either prohibiting racial profiling and/or requiring law enforcement agencies to collect racial data on traffic stops.").

database to access genetic genealogy data.[211] In 2021, Montana enacted a law providing that "[a] government entity may not obtain DNA search results from a consumer database… without a search warrant issued by a court on a finding of probable cause."[212] Maryland's law, also enacted in 2021, does not specify that police need a warrant, though it does require that police be investigating a very serious crime such as murder, rape or an ongoing threat to public safety or national security and that a judge authorize access to the DNA database.[213]

In sum, while state statutes requiring search warrants are not widespread, the last few decades have seen some notable state legislative activity designed to impose greater constraints on the police than the Fourth Amendment requires. In areas as diverse as body cavity searches, racial profiling, wiretaps, DNA databases, and electronic data, states have stepped in to impose search warrant requirements by statute.

CONCLUSION

The automobile exception has long authorized the police to conduct invasive searches of a vehicle without a warrant. Supreme Court precedent clearly permits the police to move a vehicle to the station, to take hours or days to conduct a search, and to break beneath the surface to dig deep into the car. Because the automobile exception gives the police broad authority to search, there is a very strong argument that the doctrine permits the police to use data extraction devices to warrantlessly remove basic driving data from a vehicle's black box and far more private cell phone data from its infotainment system.

While *Riley v. California* forbids warrantless searches of cell phones incident to arrest, there are compelling reasons to believe that the Supreme Court will not extend that doctrine to forbid searches of smart car computers under the automobile exception. Vehicles contain a far smaller quantity of private information than cell phones. A considerable amount of information in a smart car's computer is also made available to the public because the vehicle is

211. *See* Virginia Hughes, *Two New Laws Restrict Police Use of DNA Search Method*, N.Y. TIMES (May 31, 2021), https://www.nytimes.com/2021/05/31/science/dna-police-laws.html.

212. MONT. CODE ANN. § 44-6-104(1) (2021).

213. *See* MD. CODE CRIM. PRO. § 17-102.

publicly visible. Unlike cell phones, vehicles are heavily regulated and therefore entitled to less Fourth Amendment protection. Moreover, a key underpinning of the *Riley* decision—the ability to prevent destruction of evidence while the police procure a warrant—is absent in the automobile context. It is far harder to immobilize the data in a two-ton vehicle than a small cell phone because police departments do not have a Faraday cage large enough to hold an automobile. Finally, the automobile exception (unlike the search incident to arrest doctrine) requires probable cause, thus eliminating the concern present in *Riley* about police rummaging without suspicion. In short, there are clear differences between the warrantless cell phone searches incident to arrest in *Riley* and the use of the automobile exception to search a vehicle's computer. It is therefore very possible that the Supreme Court will uphold police authority to conduct warrantless searches of a vehicle's black box and its infotainment system under the automobile exception.

And even if the Court were to eventually forbid warrantless smart car searches under the automobile exception, that may not happen for decades. More than twenty years passed between the first reported case of a search incident to arrest of a pager and the Supreme Court's landmark decision in *Riley*. At that pace, we may not see a Supreme Court decision on the constitutionality of the warrantless search of a smart car until the year 2040 or later.

The prospect of the Court upholding warrantless searches of smart car computers under the automobile exception (or not outlawing them for another twenty years) is deeply problematic. Tesla is on pace to sell one million cars in 2022. Many other car manufacturers are also selling smart cars with extremely sophisticated computer technology. At present, there are tens of millions of vehicles on the road that hold extremely private location and cell phone data. In the near future, the number will rise to hundreds of millions of vehicles.

Police already have the tools to extract private data from vehicles. Many police departments have basic data extraction devices that enable them to download "black box" data about driving speeds, braking, and airbag data. This information is extremely valuable in a host of criminal cases ranging from simple drunk driving all the way up to vehicular homicide. More concerning is that a small number of police departments have Berla

devices that enable the police to extract sensitive cell phone data that the driver has passed through the vehicle's infotainment system. If a cell phone has been connected to the vehicle, the Berla device can extract call histories, contact lists, text messages, emails, photos, and perhaps other highly private data that the driver never realized she might be exposing to law enforcement. In the years to come, smart cars are likely to hold even more data than they do today. And the data extraction devices will almost certainly become more sophisticated and offer law enforcement an opportunity to download even more private data from vehicles than they can extract today. The result will be police ability to pry deep into someone's personal life by going through their automobile's computer.

There are already reported cases from six states in which police openly admitted to extracting data from a vehicle's computer without a warrant. Given that the Supreme Court is unlikely to stop police from searching smart cars without a warrant (or unlikely to stop it anytime soon), Congress and the state legislatures should step in. Legislatures have the power to enact statutes that would require police to procure a search warrant before extracting data from a smart car's computer. A statutory warrant requirement would eliminate police ability to rely on the automobile exception to the warrant requirement. Legislatures should therefore be proactive and forbid warrantless smart car searches before they become a significant invasion of privacy.