IF WHEELS COULD TALK: FOURTH AMENDMENT PROTECTIONS AGAINST POLICE ACCESS TO AUTOMOBILE DATA

NICOLE MO*

The relationship between policing and automobiles is long and complicated. Law enforcement's ability to stop and search a vehicle comprises a distinct line of Fourth Amendment jurisprudence. But searching a vehicle no longer means what it did even twenty years ago. Today, automobiles collect data on us from when we open the car door to the moment we turn off the engine. Much of this information is retained in an automobile's hardware and funneled to third party companies, who can share at their discretion. Law enforcement agencies have made use of auto data, obtaining it without a warrant both by extracting auto data from the vehicle itself and by contacting the companies collecting the data firsthand to ask that they share the information. The constitutionality of such a practice may seem up for debate, given the disagreements among lower courts over how auto data fits into a larger web of Fourth Amendment jurisprudence. This Note brings together two strands of Fourth Amendment case law—the automobile exception and the third-party doctrine—and argues that an animating principle motivating the Supreme Court's recent digital search cases provides a clear answer to the auto data confusion: Police need a warrant before they can access auto data, because auto data, much like cellphones and cell site location information, reveals automatically collected diaristic information.

 J.D., 2023, New York University School of Law. I am grateful to Professors Barry Friedman and Emma Kaufman for invaluable mentorship and feedback on this Note, as well as to the other members of the Furman Academic Scholars Program. I also owe deep thanks to Sajid Ahsan for his thoughtful edits as the Primary Editor on this Note; Ben Healy, Kevin Kuate Fodouop, Devin McCowan, Tanya Raja, and Nika Sabasteanski for screening my Note; and other members of the *New York University Law Review* who worked on this piece. And to my friends and family, your love and support are everything.

Introduction

A man bought a used Chevrolet Tahoe at the end of 2006.[1] The car came equipped with OnStar, a General Motors vehicle service that provides emergency assistance and navigation, among other things. The man declined to pay for OnStar, but the service didn't immediately terminate, and in January 2007, OnStar received an inadvertent emergency request from the Tahoe. An OnStar employee began monitoring the vehicle and overheard the car's occupants discussing a drug transaction.[2] The employee, who had already contacted the sheriff's office to request assistance at the vehicle's location, allowed the sheriff's dispatcher to listen in, at which point the police were notified. An officer subsequently pulled over the Tahoe and conducted a search that uncovered marijuana.[3] The Tahoe owner's conversation, undertaken in what he likely thought was the privacy of his vehicle, was all that justified the police in pulling him over, searching his car, and seizing the evidence that led to an indictment.

On average, Americans spend nearly an hour a day in their vehicles.[4] In that hour, a driver could get through a podcast episode, reply to texts using voice commands, turn on the headlights as the sun goes down, or invite another passenger into the vehicle. All of this constitutes data, and the average American car generates twenty-five gigabytes of it per hour.[5] Today's automobiles gather information on our location, speed, transmission shifts, voice commands, messages and calls from synced phones, and plenty more. Vehicles have become exemplary

---

1 State v. Wilson, 5th Dist. Fairfield No. 07CA56, 2008-Ohio-2863.

2 *Id.* ¶¶ 1–2.

3 *Id.* ¶¶ 2–3.

4 Andrew Gross, *Think You're in Your Car More? You're Right. Americans Spend 70 Billion Hours Behind the Wheel*, AAA Newsroom (Feb. 27, 2019), https://newsroom.aaa.com/2019/02/think-youre-in-your-car-more-youre-right-americans-spend-70-billion-hours-behind-the-wheel [https://perma.cc/C8WK-DE3Y].

5 DHS Science and Technology (S&T) Directorate, *Project iVe—Vehicle Navigation/Infotainment System Forensics for Law Enforcement* (Apr. 6, 2017) [hereinafter *Project iVe*], https://www.dhs.gov/sites/default/files/publications/508_FactSheet_CSD_Cybersecurity%20Forensics_Berla%20iVe_Final_April%202016.pdf [https://perma.cc/F697-WQ6G].

eyewitnesses with perceptive capacities and photographic memories exceeding what a human could observe, let alone remember.[6]

Police can avail themselves of these vehicular eyewitnesses and access a wealth of information through two forms of "cartapping." Like in the example above, police can go to companies that collect automobile data themselves. But an emerging industry also provides law enforcement with forensic tools that extract auto data directly from the vehicle.[7] These two approaches—indirect access and direct access—enable police in states across the country to access data from almost any vehicle, just by calling up an auto data company or plugging a tool into a car's hardware.

At a glance, a tangled web of Fourth Amendment doctrine appears to permit warrantless access to auto data, whether the access is indirect or direct, despite a presumption that the Fourth Amendment requires law enforcement to obtain a warrant before conducting a search. This is due to two complicated areas of Fourth Amendment jurisprudence. First, the third-party doctrine provides that the Fourth Amendment doesn't apply when the government obtains information that people have knowingly and voluntarily shared with a third party: Individuals effectively cede any legitimate expectation of privacy in their information by divulging it.[8] In the context of auto data, the third-party doctrine may mean indirect access does not trigger constitutional protections, since individuals have voluntarily shared that data with auto data companies. Second, although police certainly trigger the Fourth Amendment by entering someone's property (their vehicle) to extract information, the automobile exception drastically limits the protections that ensue. The Supreme Court has long permitted vehicle searches on probable cause alone, without requiring the external review and sign-off from a neutral magistrate that a warrant entails.[9] As applied to direct access to auto data, the automobile exception would allow law enforcement to extract a broad range of personal information at a routine traffic stop, merely based on an officer's suspicion that the vehicle may contain evidence of a crime.

---

[6] *See* Anthony D. Cornetto, III, Ben LeMere & Carly McGee, *Vehicle System Forensics: Introducing Your New Star Witness*, U.S.L., Fall-Winter 2015, at 32, 33 (explaining how vehicle software creates a forensic image which can be saved for months); Olivia Solon, *Insecure Wheels: Police Turn to Car Data to Destroy Suspects' Alibis*, NBC News (Dec. 28, 2020), https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939 [https://perma.cc/6ZYT-HT99].

[7] *See, e.g.*, Cornetto et al., *supra* note 6, at 33.

[8] *See infra* Section II.A.1.

[9] *See* Carroll v. United States, 267 U.S. 132 (1925) (holding for the first time that police can search an entire vehicle without a warrant if they have probable cause).

It would be troubling if the doctrines in fact compel such conclusions. The Fourth Amendment protection against state-conducted searches is effectively defanged if law enforcement can warrantlessly peruse auto data companies' archives to find out where people go, how they get there, and what they do in transport. And the automobile exception becomes a gaping carve-out to the presumed warrant requirement if law enforcement can access extensive personal information during warrantless traffic stops, which happen to be the dominant way police interact with civilians.[10] The stakes of warrantless police access to auto data are, unsurprisingly, higher for people of color, who are disproportionately pulled over while driving and also disproportionately searched pursuant to a traffic stop.[11] In 2022, for example, nearly sixty percent of the people pulled over and ninety percent of the people arrested by the NYPD were Black and Latinx.[12]

The datafication of the car is indicative of how so many interactions once considered private or fleeting are now catalogued and stored in our devices. Cellphones are a prime example of this phenomenon. The law is slowly starting to catch up to our new reality. In recent cases concerning digital searches, the Supreme Court has expressed a deep anxiety with applying old doctrines to new technology. By holding that searches of cellphones and cell site location data require a warrant, the Court has made clear that at least one digital device—the cellphone—enjoys meaningful Fourth Amendment protections.[13]

But the cellphone is not the only digital device. What about the automobile? This Note brings together two Fourth Amendment doctrines rarely put in conversation and argues that recent Supreme Court precedent requires police to obtain a warrant before accessing auto data, despite the conventional third-party doctrine and automobile exception. Auto data enjoys similar protections to cellphone data, not because they are identical, but because they share the same characteristics that

---

[10] *See* Bob Harrison, *Stop, Start, or Continue? A National Survey of the Police About Traffic Stops*, RAND (June 30, 2021), https://www.rand.org/blog/2021/06/stop-start-or-continue-a-national-survey-of-the-police.html [https://perma.cc/6KQ2-A88M] ("Traffic stops are the most prevalent way the police have contact with the public.").

[11] *See, e.g.*, Magnus Lofstrom, Joseph Hayes, Brandon Martin & Deepak Premkumar, *Racial Disparities in Traffic Stops*, Pub. Pol'y Inst. of Cal. (Oct. 2022), https://www.ppic.org/publication/racial-disparities-in-traffic-stops [https://perma.cc/3UA4-Q8FS] (finding that police departments were disproportionately likely to stop Black drivers and disproportionately likely to search Black and Latino drivers).

[12] Jesse Barber, *Black, Latinx People Were 90 Percent of Those Arrested in NYPD Traffic Stops*, NYCLU (Mar. 24, 2023), https://www.nyclu.org/en/news/black-latinx-people-were-90-percent-those-arrested-nypd-traffic-stops [https://perma.cc/9GTR-ENYJ].

[13] *See* Riley v. California, 573 U.S. 373 (2014) (concerning cellphones); Carpenter v. United States, 138 S. Ct. 2206 (2018) (concerning cell site location data); *infra* Section II.A.

have motivated the Court's recent decisions: Automobiles and cellphones both collect diaristic information and do so automatically, with little to no human direction or control. By introducing the automatic diary principle as a way to understand the Court's recent cases and as a way to analogize automobiles to cellphones, this Note provides clarity on how to apply an uneasy digital search jurisprudence to police access of auto data.

This Note proceeds as follows. Part I explains the breadth and depth of auto data and discusses how law enforcement has made use of such information. Part II begins by surfacing two Fourth Amendment doctrines that have long complicated a presumptive warrant requirement—the third-party doctrine and the automobile exception—as well as the Court's recent turn to more robust protections for digital devices before demonstrating the confusion among lower courts that have tried to apply Fourth Amendment law to auto data searches. Part III charts a path out of the confusion, introducing a clarifying principle that explains when exactly the Court envisions Fourth Amendment protections: when digital devices collect diaristic information automatically, without affirmative human direction or control. Part III then argues that, despite disagreement among lower courts, Supreme Court precedent as elucidated by the automatic diary principle dictates that police must obtain a warrant before accessing comprehensive auto data.

I
The Auto Data Problem

It may feel these days like every device offers every service—watches read emails, refrigerators field text messages, air conditioners connect to the cloud.[14] Cars are no different. In fact, in terms of the many services offered (and subsequently, the amount of data collected), automobiles are surprisingly similar to smartphones. And as smartphones become emblematic of a digital age incompatible with conventional privacy frameworks, automobiles merit their own scrutiny. This Part surveys the information collected by automobiles and retained by auto data companies before illustrating how law enforcement has appropriated that data for its own use. It then discusses the methods that law

[14] *See, e.g.*, *Access and Manage Emails on Your Samsung Smart Watch*, Samsung, https://www.samsung.com/us/support/answer/ANS00061441 [https://perma.cc/Z5RF-VFKH]; George Avalos, *Your Refrigerator Is Getting a Digital Makeover*, Mercury News (Mar. 17, 2017), https://www.mercurynews.com/2017/03/17/your-refrigerator-is-getting-a-digital-makeover [https://perma.cc/YJ72-XZAR]; Mike Prospero, *Best Smart Air Conditioners in 2023*, Tom's Guide, https://www.tomsguide.com/us/smart-air-conditioner-buying-guide,review-5615.html [https://perma.cc/8JXV-KQ9B].

enforcement uses to access auto data, demonstrating just how easy it is for the government to access some of our most personal information.

A. A Truly Mobile Device

Automobiles in the United States now contain about seventy computers.[15] It wasn't always this way. Mercedes-Benz claims to have invented the first automobile in 1886. Consisting of little more than three spoke wheels, a gas engine, and an open air carriage, that first car bears little resemblance to the vehicles we drive today.[16] By the 1940s, companies were building automobiles that could store, generate, and respond to data—for example, by incorporating preset buttons that saved certain radio channels.[17] By the 1980s, automobile companies had already created a rudimentary version of in-system navigation that calculated a vehicle's position using a film map, a computer, and motion sensors.[18]

The automobile-as-computer properly arrived in the new millennium. Bluetooth technology and USB ports allowed drivers to use their phones through their cars, turning vehicles into literal mobile devices.[19] Most post-2000s models contain an infotainment system, a "central hub" commonly positioned between the two front seats that allows users to access in-system navigation, satellite radio, their cellphones, and more.[20] Accompanying the infotainment system is a telematics system, "the integration of telecommunication and information" that facilitates communications between a modern-day driver and their car.[21] Think of the mechanisms working behind the scenes when you turn on your seat heater or when a vehicle senses an object in the driver's blind spot and sends an alert—that communication between the vehicle and its user is facilitated by telematics. Infotainment and telematics systems provide many of the services we now expect out of automobiles.[22] And they

---

15 *Project iVe*, *supra* note 5.

16 *1885-1886. The First Automobile*, Mercedes-Benz Grp., https://group.mercedes-benz.com/company/tradition/company-history/1885-1886.html [https://perma.cc/M3DT-LGKB].

17 Tiff Rossi, *A Brief History of In-Vehicle Infotainment and Car Data Storage*, Tuxera (July 19, 2021), https://www.tuxera.com/blog/a-brief-history-of-in-vehicle-infotainment-how-tuxera-fits-in [https://perma.cc/6HPG-246U].

18 *Id.*

19 *Id.*

20 *See* Cornetto et al., *supra* note 6, at 32; Keith Barry, *Get the Most from Your Car's Infotainment System*, Consumer Reps. (July 6, 2023), https://www.consumerreports.org/cars/automotive-technology/get-the-most-from-your-cars-infotainment-system-a1056374937 [https://perma.cc/DL66-CJER] ("Almost every new vehicle on sale today has a center control—or infotainment—screen for phone calls, navigation, music, and climate control.").

21 Cornetto et al., *supra* note 6, at 32; *see Vehicle Telematics*, Heavy.AI, https://www.omnisci.com/technical-glossary/vehicle-telematics [https://perma.cc/KL5U-3L4N].

22 *See* Chris Bouchard, *Infotainment vs. Telematics System: What Is the Difference?*, Data One Software (Apr. 21, 2016), https://vin.dataonesoftware.com/vin_basics_blog/

collect massive amounts of data in the process. Two recent class action lawsuits have alleged that Toyota's and Ford's respective infotainment systems download and store all texts from any phone that gets connected to the car.[23] Some of Toyota's vehicles even come with face identification technology now—when the technology is set up, the vehicle will scan faces of people opening car doors and store "facial geometric features."[24]

Alongside the infotainment and telematics systems, another important source of auto data is the event data recorder (EDR), a black box device that records information from the seconds before, during, and after a crash.[25] As of 2018, nearly all American vehicles come with an EDR.[26] EDRs don't collect as much information as infotainment and telematics modules, but they still reveal a lot from those few seconds, including speed of the vehicle pre-crash, acceleration statistics, steering wheel angle, front seat positions, and other parameters.[27] Although EDRs have been around since the 1970s, a 2012 rule by the National Highway Traffic Safety Administration (NHTSA) requiring standardization of data collection and retrieval has increased the data's accessibility.[28]

---

vehicle-infotainment-vs-telematics-systems-what-is-the-difference [https://perma.cc/279H-SRY3] (explaining telematics systems as primarily providing safety features and infotainment as primarily providing entertainment features). The difference between infotainment and telematics systems is not critical to this Note, and even industry experts cannot agree on what actually separates the two. While some define telematics systems as dedicated to facilitating communication of certain information (like changes to the automobile) between driver and vehicle and infotainment systems as dedicated to providing amenities to drivers and occupants, the two work together closely. *See* Randy Frank, *The Line Between Telematics and Infotainment Blurs Even Further*, Elec. Design (Aug. 26, 2009), https://www.electronicdesign.com/technologies/communications/wireless/4g-5g-6g/article/21752638/the-line-between-telematics-and-infotainment-blurs-even-further [https://perma.cc/HDA4-PAU2].

[23] *See* Goussev v. Toyota Motor Sales, USA Inc., No. 3:21-cv-05708-DGE, 2022 WL 1423642, at *1 (W.D. Wash. May 5, 2022); Jones v. Ford Motor Co., No. 3:21-cv-05666-DGE, 2022 WL 1423646, at *1 (W.D. Wash. May 5, 2022).

[24] *Privacy Notice: Connected Services*, Toyota, https://www.toyota.com/privacyvts [https://perma.cc/SV3Z-CX4D].

[25] *Event Data Recorder*, NHTSA, https://www.nhtsa.gov/research-data/event-data-recorder [https://perma.cc/JZB7-YK2Z].

[26] Marina Medvin, *Your Vehicle Black Box: A 'Witness' Against You in Court*, Forbes (Jan. 8, 2019), https://www.forbes.com/sites/marinamedvin/2019/01/08/your-vehicle-black-box-a-witness-against-you-in-court-2/?sh=442d967531c5 [https://perma.cc/8WV5-6HKM].

[27] *See Black Box 101: Understanding Event Data Recorders*, Consumer Reps. (Jan. 2014), https://www.consumerreports.org/cro/2012/10/black-box-101-understanding-event-data-recorders/index.htm [https://perma.cc/7NQZ-S6B3] (explaining what data EDRs are required to collect as of 2012); *Event Data Recorder*, AAA Exch., https://exchange.aaa.com/automotive/automotive-trends/event-data-recorder [https://perma.cc/FGH5-EQJV] (comparing EDRs to black boxes in aircraft).

[28] *See Black Box 101: Understanding Event Data Recorders*, *supra* note 27 (explaining the 2012 Rule).

Between an infotainment module, a telematics system, and a black box, the modern automobile now scrapes together a wealth of information—both about the vehicle itself, and also about the behavior of occupants and drivers. Auto data includes "vehicle event data," revealing vehicle behavior such as when doors open and close, what gears shift and when, and even a car's location within a lane.[29] Some cars, including Teslas, now record live video when the vehicle is in transport or is approached.[30] Auto data can also tell a rich story about drivers and occupants, such as their location history, metadata from connected devices, texts and calls made in-vehicle, and music preferences.[31] Cars even know how much weight we gain.[32] Companies that aggregate and sell vehicle data offer bewildering categories of information such as "Driver Fatigue" and "Heart Rate," demonstrating just how intimate auto data can be.[33]

You might think, or at least hope, that all this information stays between you and your vehicle. But auto data is fed to the vehicle provider and other companies that provide components.[34] These companies have free rein to use and retain this data as they see fit, including funneling it to data analytics companies or selling it to data brokers.[35] Some of the biggest auto companies, including Toyota, admit to sharing

---

[29] *E.g.*, *id.*; Ángel Díaz, *Law Enforcement Access to Smart Devices*, Brennan Ctr. for Just. (Dec. 21, 2020), https://www.brennancenter.org/our-work/research-reports/law-enforcement-access-smart-devices [https://perma.cc/7KE3-Y8YW].

[30] Adam M. Gershowitz, *The Tesla Meets the Fourth Amendment*, 48 BYU L. Rev. 1135, 1138 (2023).

[31] *See* Ben LeMere & Carly McGee, *Vehicle Discovery – The Nuts and Bolts of Useful Data*, Digit. Mountain Newsl. (Digit. Mountain), Summer 2015, at 1, 1, https://digitalmountain.com/wp-content/uploads/2020/09/SUMMER_2015_Article2.pdf [https://perma.cc/2GXP-ZBQC] (detailing types of data that can be extracted from vehicles).

[32] *See, e.g.*, Bill Hanvey, Opinion, *Your Car Knows When You Gain Weight*, N.Y. Times (May 20, 2019), https://www.nytimes.com/2019/05/20/opinion/car-repair-data-privacy.html [https://perma.cc/ZS5K-9D66].

[33] *See* Jon Keegan & Alfred Ng, *Who Is Collecting Data from Your Car?*, The Markup (July 27, 2022), https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car [https://perma.cc/9RC4-4BSY].

[34] *See, e.g.*, Joseph Cox, *Cars Have Your Location. This Spy Firm Wants to Sell It to the U.S. Military*, Vice: Motherboard (Mar. 17, 2021), https://www.vice.com/en/article/k7adn9/car-location-data-telematics-us-military-ulysses-group [https://perma.cc/F76J-VT3S] (explaining how car manufacturers and Original Equipment Manufacturers automatically collect information from sensors in vehicle components).

[35] *See* Keegan & Ng, *supra* note 33 (identifying thirty-seven companies that monetize auto data); Joseph Cox, *Class-Action Lawsuit Targets Company that Harvests Location Data from 50 Million Cars*, Vice: Motherboard (Apr. 15, 2022), https://www.vice.com/en/article/y3v95k/car-location-data-otonomo-class-action-lawsuit [https://perma.cc/BRM6-586X] (detailing a class action lawsuit against Otonomo, a data broker which sells real-time location data from tens of millions of cars worldwide).

personal data with third parties for those parties' marketing purposes.[36] General Motors' OnStar, another one of the largest auto data companies in the country, suggests that it may never delete auto data unless required.[37] Even when owners or lessees of a vehicle request that data be deleted, "erased" information is sometimes still available through the internal memory and thus easily retrievable.[38] Opting out of such data collection is near-impossible.[39] Individual precautions, short of not using a car, are likely insufficient to keep you off the grid.

B. Cartapping

Auto data is a treasure trove of information that's fed to various parties, who can do with it what they will. Auto data companies might use this data to improve their products.[40] Third party advertisers may use it to understand driver behavior or target certain demographics.[41] Data brokers profit from aggregating and packaging data to such third parties.[42] And the police use this data, too.

---

[36] *Your Privacy Rights*, Toyota, https://www.toyota.com/support/privacy-rights [https://perma.cc/NDP3-GLKU]; *see also* Justin Kloczko, Connected Cars and the Threat to Your Privacy 2 (Consumer Watchdog ed., 2022), https://www.consumerwatchdog.org/sites/default/files/2022-03/CWD%20TELEMATICS%20REPORT%20March%202022.pdf [https://perma.cc/HAR5-FAS7] ("Car companies, including General Motors, Toyota, Ford, reserve the right to collect, use and share data in order to track and market products.").

[37] *See OnStar Privacy Statement*, OnStar, https://www.onstar.com/legal/privacy-statement [https://perma.cc/EPL7-VKQ8] ("We may keep the information we collect for as long as necessary to provide products or services to you, to operate our business, to enable us to communicate with you, for our safety, research, evaluation of use, or troubleshooting purposes, or to satisfy our legal or contractual obligations."); *see also* Díaz, *supra* note 29 (noting that OnStar puts the onus on users to delete their information before selling their vehicle).

[38] *See* Thomas Brewster, *Feds Can Dig Up 'Deleted' Location Data from Your Car Entertainment System*, Forbes (Oct. 17, 2018), https://www.forbes.com/sites/thomasbrewster/2018/10/17/feds-are-digging-up-deleted-location-data-from-car-entertainment-systems/?sh=44bd73b4a1b0 [https://perma.cc/PS89-SSDD] (explaining that only *references* to the information will be deleted, not the data itself).

[39] *See* Hanvey, *supra* note 32 ("But while you can turn off location data on your cellphone, there's no opt-out feature for your car.").

[40] *See, e.g.*, Jeff Peters, *Automakers Have a Choice: Become Data Companies or Become Irrelevant*, TechCrunch (May 23, 2019), https://techcrunch.com/2019/05/23/automakers-faced-with-a-choice-become-data-companies-or-become-irrelevant [https://perma.cc/UJT8-L3RD] (explaining how various industries want to use vehicle data).

[41] *See, e.g.*, McKinsey & Co., Monetizing Car Data 24 (2016), https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/monetizing%20car%20data/monetizing-car-data.ashx [https://perma.cc/H3V2-RUFY] (discussing how auto data companies are "generating revenue through the sale of products/services to customers, tailored advertising, and the sale of data to third parties").

[42] *See, e.g.*, Keegan & Ng, *supra* note 33 (discussing how companies leverage auto data "for applications including insurance, traffic management, electric vehicle infrastructure planning, fleet management, advertising, mapping, city planning, and location intelligence").

Law enforcement have engaged in "cartapping" since as early as 2001, when the FBI got a court order compelling an auto data company to provide "roving interceptions" of audible communications made from within a Mercedes Benz.[43] Perhaps the most prominent police uses of auto data have been in two mass shootings—French police accessed the vehicles used by the shooters in the Charlie Hebdo attacks, and the FBI enlisted the assistance of the same vehicle data access company following the San Bernardino shooting.[44] But cartapping is not limited to these rare high-stakes and time-sensitive circumstances. In many jurisdictions, cartapping is just another tool in an agency's arsenal. For example, in 2020, Michigan's State Police Computer Crimes Unit had a detective in charge of forensic extraction of auto data, and four offices across the state were extracting auto data regularly, "sometimes two to three times a week."[45]

EDRs, which serve the express function of documenting the conditions surrounding a crash, naturally lend themselves to police investigations of vehicle collisions. Case law shows police in a number of states accessing EDRs following a crash.[46] In 2009, for example, Texas police were downloading EDR data in sixty-six percent of any fatal or possibly fatal crashes and in forty-one percent of serious personal injury cases.[47] In 2016, Alabama police chased a car for failing to use its turn signal, leading to the driver fleeing and colliding in a crash that killed two—police accessed the EDR and used the speed history against the driver at trial.[48]

The narrow scope of EDR data means it's rarely applicable outside crash investigations, but law enforcement uses other auto data in broader contexts. Auto location data is particularly germane to law enforcement activity. Police commonly use real-time and historical auto location data, often in auto theft investigations but also any time they are trying to locate a suspect or map her prior movements.[49] For example,

---

[43] Thomas Brewster, *Cartapping: How Feds Have Spied on Connected Cars for 15 Years*, Forbes (Jan. 15, 2017), https://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/?sh=4d9fb3e52ef8 [https://perma.cc/4TFC-AGEL].

[44] Patrick Howell O'Neill, *Meet Berla, the Little-Known Company That Can Pull Smartphone Data from Your Car*, CyberScoop (Sept. 11, 2017), https://www.cyberscoop.com/berla-car-hacking-dhs [https://perma.cc/LJ3D-RCKU].

[45] Solon, *supra* note 6.

[46] A keyword search of Westlaw reveals at least ten states where EDR data has figured into a police investigation. *See infra* note 72 and accompanying text.

[47] *See* Daniel Harper, Note, *Automobile Event Data Recorders and the Future of the Fourth Amendment*, 120 Colum. L. Rev. 1255, 1260 (2020).

[48] Reese v. State, CR-18-0687, 2020 WL 5494475 (Ala. Crim. App. Sept. 11, 2020).

[49] *See, e.g.*, Christina Lobrutto, *Burglary Suspect Arrested in Camden After OnStar Tracks Stolen Vehicle*, Philly Voice (Nov. 2, 2015), https://www.phillyvoice.com/

Immigration and Customs Enforcement (ICE) agents demanded a telematics company turn over three months of location data from a freight truck they suspected of transporting marijuana.[50] Ohio police used real-time location information to apprehend a driver they believed to be holding his girlfriend against her will.[51] Officers in Montgomery County, Texas, obtained real-time location tracking data to find a twelve-year-old girl who had taken her grandmother's car for a drive.[52] One distinct feature of auto data is that companies who supply auto location data to police often also have the power to stop an individual at their known location. Law enforcement have used auto data companies' long electronic reach to disable vehicles and lock car doors.[53] In 2019, for example, police in Indiana called OnStar about a man who had escaped from state custody as he was escorted out of the local jail and who had found an SUV in a neighboring parking lot—OnStar gave police the vehicle's location and then disabled the car once police were close.[54]

Though frequently used, location information is not the only type of auto data attractive to police. After a woman disappeared in Colorado, investigators turned to her husband's truck, extracting data on when he put the truck in reverse and backed it near the house that evening, when the truck doors opened and closed in the middle of the night, and where he drove it early the next morning.[55] ICE requested speed and idle time statistics for a Volkswagen found with drugs inside.[56] And according to the industry leader in auto data extraction, police have used auto data

---

burglary-suspect-arrested-camden-onstar [https://perma.cc/3GXD-FATP]; People v. Jacques, B266138, 2016 WL 4482930, at *3 (Cal. Ct. App. Aug. 25, 2016) (using real-time auto location data to find a defendant suspected of several home burglaries); Solon, *supra* note 6.

50 Thomas Brewster, *These Companies Track Millions of Cars—Immigration and Border Police Have Been Grabbing Their Data*, Forbes (Apr. 1, 2021), https://www.forbes.com/sites/thomasbrewster/2021/04/01/these-companies-track-millions-of-cars-immigration-and-border-police-have-been-grabbing-their-data [https://perma.cc/76HJ-S34G].

51 Lenhart v. Savetski, No. 1:21 CV 611, 2021 WL 2400946 (N.D. Ohio June 11, 2021).

52 *Video: 12-Year-Old Leads Police on High-Speed Chase*, ABC13 (July 1, 2016), https://abc13.com/12-year-old-chase-suspect-montgomery-county-girl-steals-grandmas-car/1409974 [https://perma.cc/CAX2-GUKE].

53 *Id.*; Gael Fashingbauer Cooper, *BMW Remotely Locks Alleged Thief in Car He's Trying to Swipe*, CNET (Dec. 6, 2016), https://www.cnet.com/news/bmw-traps-thief-by-remotely-locking-him-in-car-he-was-stealing/#ftag=CAD590a51e [https://perma.cc/6GPL-E22M].

54 Vic Ryckaert, *Police Stop Escaped Inmate Using Car's OnStar System*, Indy Star (May 8, 2019), https://www.indystar.com/story/news/crime/2019/05/08/onstar-tracking-used-find-then-shut-down-stolen-vehicle-escaped-inmate/1140335001 [https://perma.cc/AYX2-DPB7].

55 Peter Van Sant, *Authorities Hint They Know Location of Suzanne Morphew's Body: "She Is in a Very Difficult Spot," Says Prosecutor*, CBS News (July 2, 2023), https://www.cbsnews.com/news/suzanne-morphew-missing-colorado-barry-morphew-murder-charges-dismissed [https://perma.cc/YG46-LXD9].

56 Brewster, *supra* note 50.

to show that a driver was texting immediately before a crash; that a wife who claimed she accidentally ran over her husband had shifted gears in a way suggesting she backed over him twice; and that a home invasion was committed by two suspects because the passenger side door opened at the scene of the break-in.[57]

Again, auto data doesn't just capture the technical information about a vehicle's operation; automobiles also collect information on their drivers and occupants, information as personal as our voices. Sheriffs in Kalamazoo County, Michigan, arrested a man for murder based on a recording extracted from the victim's vehicle that captured the man using the hands-free system around the time of death to play an Eminem song.[58] In 2012, Illinois prosecutors successfully charged a driver with first-degree murder using a recording between him and an OnStar emergency operator where the driver, in the immediate aftermath of a fatal crash, admitted to using drugs.[59]

In sum, vehicles now perform many of the tasks we believe to be the domain of other devices. EDR data, infotainment data, location information, telematics records, even video—it shouldn't be surprising that law enforcement have tapped into this trove of information. Police are using all types of auto data in all types of investigations, accessing information about drivers, occupants, and the vehicles themselves. The question then becomes: How do police cartap, and are there any guardrails on this behavior?

C. Methods of Access

Much like with smartphone data, there are two main ways for police to access auto data, and the distinction between the two matters for doctrinal purposes. Police can obtain auto data from auto data companies, a process this Note refers to as indirect access. Alternatively, police can obtain the data themselves by extracting it from the vehicle hardware in a process this Note calls direct access.

As automobiles collect data, like when a door unlocks or a gas tank creeps toward empty, the vehicle transmits this information via cellular radio to the automobile manufacturer's servers.[60] Law enforcement can request auto data from these companies, a practice particularly useful when police cannot access or locate the vehicle. Although the idea of police directly scraping your data with state-of-the-art technology

---

57 Cornetto et al., *supra* note 6. For more on Berla, the extraction company, see *infra* Section I.C.

58 *See* Solon, *supra* note 6.

59 People v. Oelerich, 78 N.E.3d 992 (Ill. App. Ct. 2017).

60 Keegan & Ng, *supra* note 33.

may feel more scandalous, the reality is that indirect access occurs more often, since it comes at little cost to agencies. For example, police have regularly requested location tracking from General Motors' OnStar system,[61] an infotainment and telematics provider that boasted roughly 7.2 million worldwide subscribers as of 2016.[62] Other major telematics providers, Geotab and Spireon, have also received court orders to turn over information.[63] Law enforcement have requested SiriusXM, a company known for in-vehicle radio services, to both provide location information and activate a tracking device on a car that police believed to be involved in illegal gambling.[64]

Indirect access can occur several ways, including a consensual production of information upon request, although law enforcement agencies and auto data companies can voluntarily enact policies requiring subpoenas, warrants, or other court orders. The only exception to this self-regulated terrain is EDR data, for which the federal Driver Privacy Act of 2015 requires a court order.[65] Access to all other forms of auto data—including long-term or real-time location data—is entirely left up to individual agencies and companies. General Motors' privacy policy states that the company "may share your information to . . . allow recipients to use for marketing or other purposes subject to your consent when required."[66] This lenient policy means that OnStar doesn't even require a court order to turn over information. Some other auto data companies impose a higher standard, requiring a court order[67] or good-faith belief that disclosure is necessary to comply with "legally authorized" requests from authorities.[68] These requirements, robust in comparison to OnStar's lenient approach, nonetheless don't specify the kind of court order or legally authorized request that would suffice, suggesting that a warrant is sufficient but not necessary.

Alternatively, law enforcement can directly access auto data using extraction tools. This requires entering the vehicle and plugging

---

61 Brewster, *supra* note 50.

62 *Number of General Motors OnStar Subscribers Worldwide from FY 2013 to FY 2017*, Statista, https://www.statista.com/statistics/736921/general-motors-onstar-business-subscriptions [https://perma.cc/6XVJ-DDD2].

63 Brewster, *supra* note 50.

64 *Id.*

65 *See infra* note 95 and accompanying text.

66 *Privacy Statement*, OnStar (Jan. 2020), https://www.onstar.com/content/tcps/us/Jan_2020/privacy_statement.html [https://perma.cc/AG98-FX89]. Note that this general policy is slightly different for California residents given the state's more protective privacy laws.

67 Brewster, *supra* note 50.

68 *SiriusXM Services Privacy Policy*, SiriusXM (Dec. 15, 2021), https://www.siriusxm.com/content/dam/sxm-com/pdf/corporate-pdf/privacy-policy-english-dec2021.pdf [https://perma.cc/Y3YV-NGM6].

an extraction kit into the relevant hardware.[69] Although direct access requires more work on law enforcement's part, including locating the vehicle and paying for extraction tools, it is desirable when police want more comprehensive auto data. EDR data is accessible via direct access, with the Bosch Crash Retrieval Tool being the standard tool.[70] Once Bosch's tool is plugged into both a vehicle's airbag module and a laptop running Bosch's software, a user can see a report of the EDR.[71] Case law shows that police in a number of states have used Bosch's tool.[72] But as a reminder, and as discussed further below, federal law requires a court order before police can access EDR data.

Direct access to non-EDR data is harder and more expensive for law enforcement to achieve,[73] but of increasing concern to privacy advocates.[74] The industry leader here is Berla, a U.S. corporation offering what is currently the lone forensic toolkit that law enforcement uses to identify vehicles, retrieve software and hardware from infotainment and telematics modules, and parse the acquired data.[75] Berla began receiving funding from the Department of Homeland Security (DHS) in 2013—since then, their iVe kit has grown from accessing eighty car models to over 6,730.[76] The company's partnership with DHS has led to relationships with law enforcement across the country, including, at one point, quarterly "iVe Steering Committee" meetings with seventeen federal, state, and local law enforcement agencies.[77] In 2020, DHS contracted

---

69 LeMere & McGee, *supra* note 31.

70 *See* Gershowitz, *supra* note 30, at 1139 ("The standard black box extraction device—the Bosch Crash Data Retrieval Tool—is not particularly expensive and police departments large and small all over the country utilize them.").

71 *Original Instructions: Crash Data Retrieval Tool*, Bosch Diagnostics, https://cdr.boschdiagnostics.com/cdr/sites/cdr/files/english.pdf [https://perma.cc/2X5V-FPZD]; *see also* Gershowitz, *supra* note 30, at 1139.

72 *See, e.g.*, State v. Kellum, 460 P.3d 394 (Kan. Ct. App. 2020); Hale v. State, 95 N.E.3d 213 (Ind. Ct. App. 2017); Commonwealth v. Cornelius, No. 861 MDA 2022, 2023 WL 2518482, at *5 (Pa. Super. Ct. Mar. 15, 2023); Swann v. State, No. C-18-CR-21-000092, 2023 WL 2804852, at *4 (Md. Ct. Spec. App. Apr. 6, 2023); State v. Cast, No. 2020-10-1384, 2022 WL 16739223, at *8 n.7 (Ohio Ct. App. Nov. 7, 2022).

73 *See* Gershowitz, *supra* note 30, at 1139–40 & n.22 ("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.").

74 *See, e.g.*, *id.* at 1145 (describing the more sophisticated Berla device); Sam Biddle, *Your Car Is Spying on You, and a CBP Contract Shows the Risks*, The Intercept (May 3, 2021), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp [https://perma.cc/FF9T-SLAL].

75 *The iVe Ecosystem*, Berla, https://berla.co/ecosystem [https://perma.cc/P3YV-U2TN].

76 Patrick Howell O'Neill, *Meet Berla, the Little-Known Company That Can Pull Smartphone Data from Your Car*, CyberScoop (Sept. 11, 2017), https://www.cyberscoop.com/berla-car-hacking-dhs [https://perma.cc/NDD3-UN9N]; *Project iVe*, *supra* note 5.

77 *Project iVe*, *supra* note 5.

with Berla for a three-month, $175,000 license renewal.[78] Customs and Border Protection (CBP) recently established a nearly half-million dollar contract with Swedish data extraction firm MSAB, Berla's strategic partner since 2016,[79] for products including five iVe kits.[80] Berla's CEO has said that the company leverages its privacy knowledge to further its business model with a quid pro quo: Berla offers security consulting to auto companies on the condition that those companies allow law enforcement access.[81]

Using Berla allows law enforcement to access a bounty of information. Police can plug Berla's iVe tool into a USB port in the vehicle or remove the relevant hardware from the vehicle and attach it to the toolkit.[82] From there, Berla will extract data on vehicle events, location data, and connected devices. This data allegedly includes phone and infotainment data like "[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," as well as some deleted data.[83] As for vehicle event data, Berla's kit is claimed to extract information like "when and where a vehicle's lights are turned on, and which doors are opened and closed at specific locations as well as gear shifts, odometer reads, ignition cycles, speed logs, and more."[84] MSAB, Berla's strategic partner, even declares that the device can predict future plans, identify known associates, and estimate communication patterns.[85] Berla's founder, Ben LeMere, has recounted extracting data from an airport rental car and recovering data from seventy phones that had been connected at some point in

---

78 *Contract Summary: Department of Homeland Security (DHS) & Berla Corporation*, USA SPENDING, https://www.usaspending.gov/award/CONT_AWD_70CMSD20P00000117_7012_-NONE-_-NONE- [https://perma.cc/N3G9-MFP7].

79 Berla Staff, *Berla and MSAB Announce Strategic Partnership*, BERLA (Nov. 9, 2016), https://berla.co/berla-and-msab-announce-strategic-partnership [https://perma.cc/55JG-3L78].

80 *Synopsis of J&A - U.S. Customs and Border Protection (CBP) Laboratories and Scientific Services (LSS) Technology & Technical Support Services*, SAM.GOV (Feb. 22, 2021), https://sam.gov/opp/28e69f99d22440418297dbb0820e86d3/view?sort=-modifiedDate&index=opps&is_active=1&page=1 [https://perma.cc/34HS-QLF7].

81 *See* DHS Science and Technology Directorate, *2016 R&D Showcase: Project iVe: Forensics for Vehicle Infotainment and Navigation Systems*, YOUTUBE (Sept. 15, 2016), https://www.youtube.com/watch?v=E0DQEVgJY5k [https://perma.cc/4A9A-3S9P] ("[W]e only [educate manufacturers on privacy] as a part of an agreement that they'll let law enforcement in.").

82 *Id.*

83 Biddle, *supra* note 74.

84 *Id.*

85 *Id.*

time—their call logs, contacts, SMS history, music preferences, and social media activity.[86]

Outside of government contracts, some advertising materials, and the rare interview, not much about Berla is publicly available. The company doesn't even make public the price of the iVE toolkit, although a sheriff's office in Texas revealed it paid $15,000 for Berla equipment and a North Carolina Police State Trooper told Professor Adam Gershowitz that the devices cost tens of thousands of dollars, require extensive training, and therefore are not widely used.[87] One can't just go to Berla's website and buy a toolkit; the company, who is known to limit sales to corporations and state agencies, requires interested buyers to contact their team to purchase a product.[88]

Because of the limited information available on Berla, this Note does not purport to provide a comprehensive review of the tool's deployment or its capabilities. But even if Berla's extraction tools are in lower circulation than Bosch's EDR tool, the growing law enforcement interest in using such devices should raise concern. Berla's iVe is more troubling than a tool like Bosch because its extraction is not limited to a few seconds surrounding a triggering event and it extracts many more types of data—infotainment and telematics systems may contain years of information, depending on the retention policies of the auto data company. The direct access industry is also growing. Although MSAB and Berla still lead the market in auto data retrieval outside of EDRs, other companies are starting to offer auto data services to both state and private actors.[89]

In illustrating how police access auto data, it's worth mentioning the few legislative restraints. The Stored Communications Act (SCA) is a federal law that requires law enforcement to obtain a subpoena before accessing certain kinds of information stored with third parties (i.e., through someone besides the data subject).[90] Specifically, it only applies to "communications" stored by public providers of electronic

---

[86] *Id.*

[87] Henry Ramos, '*Brain of the Car' Technology Used in Two High-profile Death Investigations, Sheriff Salazar Says*, KENS 5 (Feb. 23, 2021), https://www.kens5.com/article/news/local/law-enforcement/brain-of-the-car-tech-explained/273-e4dc1b7c-2ad7-43e8-b281-b153d4c10a20 [https://perma.cc/WF2H-3326]; Gershowitz, *supra* note 30, at 1147–48.

[88] *What's Included?*, Berla, https://berla.co/whats-included [https://perma.cc/ZV6X-NCCQ].

[89] *See, e.g.*, Joseph Cox, '*Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go*, Vice (June 10, 2021), https://www.vice.com/en/article/4avagd/car-location-data-not-anonymous-otonomo [https://perma.cc/HJY8-FHT2] (describing a company that sells auto location data to any organization that makes an account on its platform); Cox, *Cars Have Your Location*, *supra* note 34 (describing a company that has pitched real-time location tracking of over 15 billion vehicles worldwide and suggested the product could serve military intelligence purposes).

[90] Stored Communications Act, 18 U.S.C. § 2703 (2012).

communication or remote storage: Think Gmail or iCloud.[91] While auto data companies may qualify as such public providers, not all the data that they collect will qualify as a wire or an electronic communication—the calls recorded by a car likely qualify, but location information, technical auto data, and silent video surveillance do not.[92] Even for the data that qualifies, law enforcement does not necessarily need to obtain a warrant, and can use subpoenas or similar court orders much of the time.[93] The Wiretap Act, which applies to live interceptions of electronic communications rather than interceptions of stored communcations, similarly requires a court order.[94] But again, these few restraints only apply to a slice of auto data and often require less than the probable cause standard of a warrant, leaving much of the data unregulated.

Another federal law, the Driver Privacy Act of 2015 (DPA), puts some statutory limits on police access to EDR data specifically: The statute generally requires authorization from a court "or other judicial or administrative authority" (though it does not require a warrant) before someone besides the owner or lessee of a car can access EDR data, unless the owner or lessee has given consent.[95] The DPA's narrow scope doesn't address Berla's tools, or the data that police can access through auto data companies.

These few statutory limits only touch the surface of what is otherwise a cartapping goldmine for law enforcement across the country. Through directly extracting the data from vehicles or indirectly obtaining it through auto data companies, the police can easily access a wealth of information—and the technology facilitating this access is only improving. The question remains whether any robust protections shield us from unfettered cartapping.

---

91 18 U.S.C. § 2703(b)(2); Electronic Communications Privacy Act, 18 U.S.C. § 2510(14) (1986) (defining electronic communications service); 18 U.S.C. § 2711(2) (defining remote computing service).

92 *See* 18 U.S.C. § 2510(1), (2), (12) (defining the wire, oral, and electronic communications that are protected under ECPA).

93 The SCA effectively only requires a warrant for accessing recently stored communications content like phone call recordings or texts, and only requires a warrant for older content if the data subject is not notified. 18 U.S.C. § 2703. A loophole allows law enforcement to warrantlessly access older content without notification through a "delayed notice" provision. *Id.* § 2705. Other stored content and non-content (like records about the data subject stored by the provider) can be obtained just through a subpoena or a § 2703(d) order. *Id.* § 2703(c)(1–2). Note, however, that some jurisdictions have expanded the warrant requirement to all stored contents. *See* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010) (holding that the government must obtain a warrant to access email through a third-party provider). The Supreme Court has not ruled on the issue.

94 18 U.S.C. § 2518.

95 Driver Privacy Act of 2015, Pub. L. No. 114-94, § 24301–03, 129 Stat. 1712 (2015).

II
The Fourth Amendment Applied

Law enforcement has caught on to the fact that auto data may reveal as much information as smartphone data and may be similarly easy to retrieve. The question is whether the Constitution has anything to say about cartapping. This Part surfaces the Fourth Amendment doctrines most relevant to auto data, starting with doctrines relevant to indirect access before moving to those relevant to direct access. It then surveys the haphazard application of Fourth Amendment doctrine to auto data access happening in state and federal courts. Courts' inconsistency and uncertainty as to both indirect and direct access to auto data has resulted in a morass where neither drivers nor law enforcement know what rights are at stake.

A. Fourth Amendment Doctrines

Fourth Amendment analysis calls for two separate inquiries. First, there's the initial question of whether government conduct amounts to a Fourth Amendment search at all. If it does, then comes the inquiry into whether such a search is reasonable. On the first question, the Supreme Court lays out two standards to evaluate whether state action qualifies as a Fourth Amendment search: a trespassory test based on whether a person's property interest has been violated,[96] and a reasonableness test emerging from Justice Harlan's concurrence in *Katz v. United States*.[97]

Police access to auto data implicates both the threshold question and the reasonableness-of-the-search inquiries. When law enforcement indirectly accesses auto data through an auto data company, the first-order question is whether such access even implicates the Fourth Amendment at all. Here, the third-party doctrine will critically determine if auto data subjects enjoy any constitutional protection. But when law enforcement directly accesses auto data, the intrusion on property definitively amounts to a Fourth Amendment search. The question in direct access cases then becomes whether the search was reasonable. Here, exceptions to the warrant requirement may permit law enforcement to access auto data without a warrant.

---

[96] *See* United States v. Jones, 565 U.S. 400, 406–07 (2012).

[97] 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (asserting that Fourth Amendment protections apply to contexts where a person has a reasonable expectation of privacy).

1. Doctrines Relevant to Indirect Access

Recall how law enforcement often accesses auto data through the companies collecting it firsthand. In such instances, police do not physically enter a vehicle user's car or other property. The *Katz* standard, a "paradigm shift" away from previous doctrine that only asked whether a physical trespass has occurred,[98] is thus our guiding test as to when such indirect access amounts to a Fourth Amendment search. *Katz* creates "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[99] If there is no reasonable expectation of privacy, there is no Fourth Amendment protection.

The Court has scaffolded the indeterminacy of *Katz* reasonableness with some firmer guidelines for when Fourth Amendment protections kick in. One such guideline is the third-party doctrine, which provides that, "if a person voluntarily provides access to that individual's personal information, then there is no reasonable expectation of privacy and thus, no protection pursuant to the Fourth Amendment."[100] Taken at face value, the third-party doctrine permits law enforcement access to any personal information knowingly and voluntarily shared with a third-party, no Fourth Amendment strings attached.

The third-party doctrine emerged in two cases, one about bank records and the other about phone call logs. In *United States v. Miller*, the Court held that a defendant had no protectable Fourth Amendment interest in account records that the government subpoenaed from his bank.[101] The Court effectively stated that a defendant who knowingly and voluntarily shares otherwise-private information to a third party, even in a qualified capacity, forfeits that privacy.[102] The Court reasserted the third-party doctrine three years later, holding in *Smith v. Maryland* that a defendant had no expectation of privacy in the numbers he dialed from his home, which his telephone services provider stored in records that the police accessed.[103] Again, the Court applied the knowing and

---

98 Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1303 (2002).

99 389 U.S. at 361 (Harlan, J., concurring).

100 Brian L. Owsley, *Cell Phone Tracking in the Era of* United States v. Jones *and* Riley v. California, 48 TEX. TECH L. REV. 207, 217 (2015).

101 425 U.S. 435, 437 (1976).

102 *Id.* at 443 (finding the Fourth Amendment doesn't apply to acquiring information through a third party to whom that information was revealed, "even if the information [was] revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

103 442 U.S. 735, 742 (1979).

voluntary prongs, finding that the defendant "assumed the risk" that the telephone company could then reveal this information to law enforcement.[104]

Conventional wisdom, then, might dictate that the Fourth Amendment does not even apply in indirect access cases thanks to the third-party doctrine. But the new age of constant, extensive data collection has tested the Court's comitment to such an absolute rule. The Court cabined the third-party doctrine in *Carpenter v. United States*, holding that a defendant had a reasonable expectation of privacy in his cell site location information (CSLI) even though it did not belong to him and had been shared with his wireless carriers.[105] Chief Justice Roberts's majority opinion in *Carpenter* declared that "the nature of the particular documents sought" matters to the third-party doctrine determination,[106] giving courts another axis of analysis. Claiming "a world of difference" between the "limited" bank and phone number records at issue in *Smith* and *Miller* and the extensive location information captured through CSLI, the Court sidestepped striking down its precedent by instead claiming *Carpenter* presented "a significant extension of [the third-party doctrine] to a distinct category of information."[107]

To justify its holding in *Carpenter*, the Court named a few factors distinguishing CSLI from the bank records and phone call logs at issue in *Smith* and *Miller*: the nature of the data, the ease with which it could be accessed, its retrospectivity, and the questionable voluntariness of sharing it. Referencing the depth of information revealed by time-stamped CSLI, the Court held that allowing government access to this "intimate window into a person's life" would "provide[] an all-encompassing record" that is qualitatively distinct.[108] In the Court's eyes, long-term CSLI implicated the reasonable expectation of privacy we enjoy in the whole of our physical movements—an expectation that persists despite most movements being public because nobody in the pre-digital era expected law enforcement to closely tail a suspect for such extended periods of time.[109] Turning away from the nature of the data, the Court also remarked that CSLI is "remarkably easy, cheap, and efficient compared to traditional investigative tools."[110] The Court was similarly concerned with companies' yearslong retention of CSLI, which creates a

104 *Id.* at 744.
105 138 S. Ct. 2206 (2018).
106 *Id.* at 2219 (quoting *Miller*, 425 U.S. at 442).
107 *Id.* at 2219.
108 *Id.* at 2217.
109 *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment)).
110 *Id.* at 2218.

retrospective archive allowing the government to "travel back in time" and reconstruct an individual's movements from before they were even suspected of criminal activity.[111] Lastly, the Court found that CSLI is not truly shared voluntarily, and therefore does not satisfy the voluntary prong of the third-party doctrine. Cellphones are "indispensable to participation in modern society," and because cellphones collect CSLI "without any affirmative act on the part of the user beyond powering up," the majority held that CSLI is not voluntarily shared.[112]

Armed with these factors and with a functional understanding of voluntariness, the *Carpenter* Court seemingly opened the door to renewed protections against police access to data. But questions linger. The majority took pains to narrow its holding, refusing to discuss real-time CSLI, overturn *Smith* and *Miller*, or address other business records that "might incidentally reveal location information," never mind address the implications for non-location data.[113] Furthermore, the *Carpenter* dissents raised some valid critiques of the majority's reasoning. How meaningful is the distinction between CSLI and *Smith* or *Miller* records, really? Financial records, as Justice Kennedy's dissent points out, can similarly reveal intimate affairs, political or religious associations, and more; accessing financial records is as cheap as accessing CSLI; companies keep large archives of this information allowing law enforcement to peek back in time; and having a bank account or credit card is hardly voluntary these days.[114]

Part III will look closer at whether and how auto data mirrors CSLI, but the permeability of the *Carpenter* Court's factors leaves plenty of room for confusion as to what qualifies as a search. If the doctrine feels shaky, that might be because it simply is. One takeaway, however, is clear: Information being shared with another is no longer an automatic bar against Fourth Amendment protections.

2. Doctrines Relevant to Direct Access

The Fourth Amendment analysis looks a bit different when police enter a vehicle and directly extract the data themselves. Although we still have to ask whether the direct access amounts to a search, there is a clearer answer. A property-based test recently revived in *United States v. Jones* accompanies the *Katz* standard and provides that a Fourth Amendment search occurs when the government physically intrudes

111 *Id.*
112 *Id.* at 2220.
113 *Id.*
114 *Id.* at 2222–23, 2232–33 (Kennedy, J., dissenting).

on private property for the purpose of obtaining information.[115] In *Jones*, even the relatively minimal intrusion of attaching a GPS tracking device on the undercarriage of a car was a trespass on property sufficient to trigger Fourth Amendment protections.[116] A defendant challenging this kind of Fourth Amendment search must have a possessory interest in the trespassed property,[117] but once that's established, it settles the first-order hurdle of proving law enforcement has performed a Fourth Amendment search or seizure.

So, when police enter a defendant's car to directly access her auto data, a Fourth Amendment search has occurred. The question then becomes whether the search was reasonable. For a search to be reasonable, the Fourth Amendment imposes a presumptive warrant requirement.[118] But a number of doctrinal exceptions cut against this so-called presumption, including the automobile exception.

The automobile exception dates back nearly 100 years. The Supreme Court decided its first automobile case in 1925 with *Carroll v. United States*, where it issued a new rule: To search an entire vehicle, police only need probable cause to believe it contains contraband or evidence of a crime.[119] No warrant necessary. The Court later expanded the automobile exception, holding that officers can warrantlessly search a car even after it's been moved to a police station and is no longer under the driver's control.[120] Even after a vehicle is impounded, the automobile exception can apply.[121] Furthermore, police can stop a vehicle on the basis of reasonable suspicion alone (a lower standard than probable cause) and then search the vehicle if the officer develops probable cause during the stop.[122]

The scope of a warrantless automobile search can encompass both the vehicle itself and containers found in it, depending on the probable cause given. Where the probable cause is to the vehicle itself (e.g., probable cause to believe a car was used in a crime), police can search the

115 565 U.S. 400, 404–05 (2012); *id.* at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

116 565 U.S. 400 (2012).

117 *See, e.g.*, Byrd v. United States, 138 S. Ct. 1518, 1528 (2018) (holding that a driver of a rental car who has the renter's permission to drive it has a reasonable expectation of privacy against government searches of the vehicle); Rakas v. Illinois, 439 U.S. 128 (1978) (holding a passenger of a vehicle, who did not own or rent the vehicle, had no standing to challenge a police search of the vehicle).

118 *See, e.g.*, United States v. Karo, 468 U.S. 705, 714–15 (1984).

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

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

121 *See id.* at 51–52.

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

entire automobile and containers in it,[123] including a container belonging to someone for whom the police have no individualized suspicion.[124] Where police have probable cause as to just an item or container in the car (e.g., an agent believes a bag contains contraband and then watches someone enter the car with the bag), they can still warrantlessly search the vehicle to locate the container, and then search within the container.[125] These searches can include disassembling or destroying parts of the vehicle—after all, the first automobile case, *Carroll*, concerned agents ripping open the seat upholstery.[126] Lower courts have run with the automobile exception's expansive scope, permitting warrantless disassembling of dashboards, glove compartments, and other vehicle modules.[127] Not all containers, however, can be warrantlessly searched just because they are lawfully seized from a vehicle. Although *California v. Acevedo* seemingly eliminated the warrant requirement for closed containers found in automobiles,[128] it didn't overrule *United States v. Chadwick*, which had previously ruled it unconstitutional to search a locked footlocker in a trunk.[129] In *Chadwick*, the Court reasoned that locked luggage still enjoyed a robust expectation of privacy despite being found in a vehicle.[130]

It thus appears that, at least for now, police can warrantlessly search a vehicle for a container and then open it, except in the rare instance where that container is locked luggage, in which case police must obtain a warrant. What could rationalize such lenient rules for cars? The *Carroll* Court justified warrantless automobile searches as necessary "where it is not practicable to secure a warrant[] because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought."[131] The Court, in subsequent cases, has continued to point to the automobile's essentially mobile nature to justify warrantless searches, claiming the time and logistics of securing a warrant would permit someone to move or hide an incriminating vehicle.[132]

---

123 United States v. Ross, 456 U.S. 798, 825 (1982) ("If probable cause justifies the search of a lawfully stopped vehicle, it justifies the search of every part of the vehicle and its contents that may conceal the object of the search.").

124 Wyoming v. Houghton, 526 U.S. 295, 302 (1999).

125 California v. Acevedo, 500 U.S. 565, 580 (1991).

126 *See* Carroll v. United States, 267 U.S. 132, 134 (1925).

127 *See* Gershowitz, *supra* note 30, at 1154–56 (citing cases).

128 *See* 500 U.S. 565 (1991).

129 433 U.S. 1 (1977).

130 *Id*. at 13.

131 *Carroll*, 267 U.S. at 153.

132 *See, e.g.*, Chambers v. Maroney, 399 U.S. 42, 51 (1970) ("[T]he opportunity to search is fleeting since a car is readily movable."); United States v. Johns, 469 U.S. 478, 484 (1985) ("The justification to conduct such a warrantless search does not vanish once the car has been immobilized.").

But mobility alone does not explain the Court's permissive rulings on automobile searches, many of which include cases where the vehicle has been taken into state custody and is no longer under a suspect's control.[133] The Court thus also embraced the idea that a diminished expectation of privacy rationalizes the automobile exception.[134] The Court's reasoning is that much of a vehicle is "relatively open to plain view."[135] And parts of a vehicle that aren't in plain view, like a locked car trunk, nonetheless also have a reduced expectation of privacy because of "the pervasive regulation of vehicles capable of traveling on the public highways."[136] This conception of the automobile—as mobile and less private—has granted law enforcement more discretion in this context than in most others.[137]

If the automobile exception were the only doctrine that governed direct access cases, it might look like warrantless extractions of auto data are reasonable so long as police have probable cause. But the automobile exception intersects, for our purposes, with emerging case law concerning when and how law enforcement may directly search electronic devices. The Court recently imposed a limit to its application of the automobile exception in *Riley v. California*, where police stopped Riley for driving with expired tags, discovered he had a suspended license, and impounded his car. After discovering firearms in the car, law enforcement arrested Riley and searched him incident to arrest, finding a smartphone in his pocket which they warrantlessly accessed.[138] Despite a general rule that police can search containers found on a person's body during a search incident to arrest, the Court held that police must obtain a warrant before searching a cellphone found on or near an arrestee's person.[139] Chief Justice Roberts's opinion emphasizes

---

133 *See, e.g.*, South Dakota v. Opperman, 428 U.S. 364 (1976) (holding police can warrantlessly inventory a vehicle that has been lawfully impounded). Note that the Court has also said that exigency is determined at the time of vehicle seizure, where even a later-impounded vehicle's mobility at the time of seizure justifies subsequent searches. *See Chambers*, 399 U.S. at 51–52.

134 California v. Carney, 471 U.S. 386, 391 (1985) ("Even in cases where an automobile was not immediately mobile, the lesser expectation of privacy resulting from its use as a readily mobile vehicle justified application of the vehicular exception."); *see also* David A. Harris, *Car Wars: The Fourth Amendment's Death on the Highway*, 66 Geo. Wash. L. Rev. 556, 566 (1998).

135 *Carney*, 471 U.S. at 391.

136 *Id.* at 392.

137 *See, e.g.*, *id.* (contrasting regulation and inspection of automobiles and homes); Tracey Maclin, *Cops and Cars: How the Automobile Drove Fourth Amendment Law*, 99 B.U. L. Rev. 2317, 2324 (2019) ("[T]he Court's logic in car cases is often based on fictitious claims about motorists' privacy interests, intellectually dishonest reasoning, and a candid desire to expand the discretion and power of law enforcement officers to stop and search motorists.").

138 Riley v. California, 573 U.S. 373, 378–79 (2014).

139 *Id.*

that the search-incident-to-arrest doctrine came about before smartphones were conceivable technology and stresses that cellphones are both qualitatively and quantitatively different from the physical items considered by the doctrine's originators.[140] Cellphones are "minicomputers" that function not only as telephones, but also as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[141] The Court also mentions the sheer amount of information contained in cellphones, noting that their storage capacity would be equivalent to a person lugging around a trunk of every communication they have made in recent months.[142] With these distinct privacy concerns in mind, *Riley* held that the rationales for a search-incident-to-arrest exception to a presumptive warrant requirement—officer safety and evidence preservation—did not justify cellphone searches when officers recover phones from an arrestee's body or immediate surroundings.[143]

Riley introduces the possibility that some digital devices are so privacy-implicating, so distinct from conventional physical items, that existing exceptions to the warrant requirement cannot apply to them. But Chief Justice Roberts's opinion makes no mention of how cellphones fare in other contexts, such as under the automobile exception.[144] *Riley* similarly leaves unanswered whether other "minicomputers" enjoy similar protections, or if cellphones, for some reason, are singularly exceptional.

B. Doctrinal Confusion in Auto Data Cases

Making sense of the above doctrines isn't easy, especially without a clear answer from the Supreme Court. This Section traces the scattered case law on whether and to what extent the Fourth Amendment protects against police access to auto data and reveals a morass of varying interpretations among different courts. No doctrinal consensus emerges. The stakes of this confusion are material. In indirect access cases, engaging in the traditional third-party doctrine analysis would mean that police can order your automobile provider to turn over months of your location data, with no Fourth Amendment protections at play. And in direct access cases, application of the traditional automobile exception would mean that police can pull you over in a

140 *Id.* at 385.
141 *Id.* at 393.
142 *Id.* at 393–94.
143 *Id.* at 387–91.
144 *See* Gershowitz, *supra* note 30, at 1160 ("The *Riley* decision is silent on whether police can rely on the automobile exception to conduct a warrantless search of a cell phone.").

routine traffic stop, gather "probable cause" of a crime in the process, and extract auto data that includes your emails, texts, turn signal history, and more. Consider that courts have already authorized the search of cell phones found in vehicles during a probable cause search, on the basis that there was probable cause to believe the cell phone was used in drug transactions—little stops courts from applying the same logic to auto data hardware.[145] In other words, whether and to what extent a person has rights to their auto data vis-à-vis police access depends entirely on how a court understands the Fourth Amendment's guardrails on digital searches and automobile searches. And for now, courts can't seem to agree on a shared understanding.

Courts are divided on whether the third-party doctrine applies to law enforcement's indirect access to auto data. Thus far, indirect access cases have been limited to automobile location data, leaving wholly unanswered how courts should treat indirect access to non-location auto data. Taking the *Smith-Miller* doctrine to its logical conclusion would permit warrantless indirect access to all manner of other auto data, such as call logs, that could be construed as business records voluntarily ceded to auto data companies.[146] In 2010, a federal district court in Louisiana embraced such a capacious understanding of the third-party doctrine, finding that "the receipt of satellite tracking information [of a rental car] from a third-party monitoring service subscribed to by the vehicle owner does not constitute a 'search' or 'seizure' under the Fourth Amendment."[147]

Carpenter has since instructed judges that the third-party doctrine is bounded in scope, but it nonetheless leaves the precise limits of the third-party doctrine undefined, even if it suggests that capacious interpretations of the third-party doctrine are no longer in favor. Courts dealing with auto data cases have differed in how they incorporate *Carpenter* into their analysis. A federal district court in Illinois held that

---

145 *See, e.g.*, State v. Boyd, 992 A.2d 1071, 1088–90 (Conn. 2010) (holding that seizure and search of the defendant's cellphone was valid under the automobile exception because the police had probable cause to believe that defendant was selling drugs, the defendant's phone was visible in his car when the police arrested him, and police had probable cause to believe that the phone contained evidence of drug activity). The Court's decision in *Riley* made no mention of cellphone searches pursuant to the automobile exception. *See* Gershowitz, *supra* note 30, at 1137.

146 *See, e.g.*, United States v. Dantzler, No. CRIM. 10-0024, 2010 WL 2740003, at *6 (W.D. La. June 16, 2010), *report and recommendation adopted*, No. CRIM 10-0024, 2010 WL 2737178 (W.D. La. July 9, 2010) ("Dantzler either knew or should have known that he was renting an OnStar[-]equipped vehicle that was capable of transmitting the vehicle's location to a monitoring service. . . . [D]efendant accepted the risk . . . .").

147 *Id.* at *3, *4–5 (finding that the defendant had no reasonable expectation in the movement on public thoroughfares of his rented vehicle which was also shared with a third party).

the combination of *Jones* and *Carpenter* requires police to get a warrant to access extensive auto location data, regardless of whether they access the data through the auto data company.[148] But a year later, a federal district court in Florida held that *Carpenter* only applies to CSLI, and that a vehicle's GPS data is qualitatively different.[149] Unsure of what distinguishes CSLI from *Smith-Miller* records, and subsequently where auto data lands on the spectrum, lower courts have reached no clear consensus regarding law enforcement's company-facilitated access to auto data.

Case law concerning direct access to auto data is similarly confused. Direct access cases have largely focused on EDR data from the seconds surrounding a crash. As mentioned above, the federal Driver Privacy Act has recently put some statutory limits on police access to EDR data, generally requiring a judicial or administrative order before someone besides the owner or lessee of a car can access that car's EDR data (if the owner or lessee has not given consent).[150] But the EDR case law remains relevant, notwithstanding the DPA's independent protections. For one, the DPA only requires judicial authorization, and does not impose a warrant requirement.[151] Furthermore, because it's limited to EDR data,[152] the DPA does not affect police's ability to indiscriminately access infotainment and telematics data. The existing jurisprudence on direct access to EDR data is thus still relevant since courts' position on EDR extraction may inform future rulings on non-EDR auto data extraction. And because no court has yet addressed law enforcement access to infotainment and telematics auto data, the confused logic of EDR cases is our only lodestar for direct access to any type of auto data.

Again, courts differ in whether they believe the automobile exception exempts direct access to auto data from a warrant requirement. At least one court has avoided applying the automobile exception altogether: In *People v. Diaz*, a California court held that the Fourth Amendment simply doesn't apply to direct access of EDR data since the information contained within—like speed and time of crash—was

148 *See* United States v. Diggs, 385 F. Supp. 3d 648 (N.D. Ill. 2019) (holding that the defendant had a reasonable expectation of privacy in his physical movements as revealed by his wife's car's GPS data, and that turning over that data to the car dealership did not defeat this expectation).

149 *See* Bailey v. State, 311 So. 3d 303 (Fla. Dist. Ct. App. 2020) (holding that the defendant did not have a reasonable expectation of privacy in his GPS records).

150 *See supra* note 95; Driver Privacy Act of 2015, Pub. L. No. 114-94, § 24302(b), 129 Stat. 1712 (2015).

151 *Id.* § 24302(b)(1).

152 *Id.* § 24302(a).

all observable by the public and therefore did not enjoy a reasonable expectation of privacy.[153] In more recent years, other courts have recognized that direct access constitutes a search, but their holdings suggest that the automobile exception would apply. In *Mobley v. State*, the Georgia Supreme Court held that direct access to EDR data constituted a Fourth Amendment search under the trespass theory revived in *Jones*.[154] The *Mobley* court chose to rule the search unconstitutional on trespass grounds, given that the intruding officer didn't obtain a warrant and the State had failed to meet an exception to the warrant requirement.[155] In noting that exceptions weren't satisfied, *Mobley* implies that EDR data could be warrantlessly searched if it satisfied the requirements of a carve-out like the automobile exception.[156] Another court in Missouri similarly ruled that direct access to EDR data constituted a Fourth Amendment search but suggested that the automobile exception could apply.[157]

But while some courts have suggested the automobile exception could turn warrantless direct access into a reasonable search under proper circumstances, at least one court has altogether rejected the automobile exception's application to EDR data extraction. In *State v. Worsham*, a Florida court declared that a warrant is required to search an impounded vehicle's EDR absent exigent circumstances.[158] Citing *Riley*, the *Worsham* court ruled that the module that stores EDR data is qualitatively like a cellphone and thus maintains a legitimate expectation of privacy that requires a warrant.[159] Once again, we're left with lower court decisions contradicting each other on what constitutes a search and what would make that search reasonable.

In both direct and indirect access cases, different jurisdictions are reaching different conclusions on the permissibility of warrantless access to auto data. Technological innovation seems to be outpacing

---

153 153 Cal. Rptr. 3d 90, 101–02 (Ct. App. 2013) ("In this case, technology merely captured information defendant knowingly exposed to the public—the speed at which she was travelling and whether she applied her brakes before the impact.").

154 834 S.E.2d 785 (2019).

155 *See id.* at 793 n.10 ("The automobile exception is inapplicable because the evidence is undisputed that, at the time Investigator Hatcher retrieved the data from the crashed Charger, the Charger not only was already in the custody and control of law enforcement officers but, more importantly, was not operable.").

156 Note that the court avoided ruling that the extraction also qualified as a *Katz* search, demurring on whether the defendant maintained a reasonable expectation of privacy in his EDR data except for a footnote stating that it "strikes us as a close question." *Id.* at 792 n.9.

157 State v. West, 548 S.W.3d 406 (Mo. Ct. App. 2018) (holding that the State did not have probable cause and therefore committed an unreasonable search).

158 227 So. 3d 602 (Fla. Dist. Ct. App. 2017).

159 *Id.* at 606 (holding that the amount of information recorded in EDRs and the difficulty of extracting this information create an expectation of privacy).

antiquated precedent, and courts hearing auto data cases are unsure how to rule. As cartapping is set to become more commonplace, this confusion cannot stand. The question for us, then, is whether there is a clear path forward.

III
A Digital Search Principle

Notwithstanding the confusion illustrated above, the Court's opinions in recent digital search cases reveal that cellphones embody some set of traits that qualify them for special treatment. This Part synthesizes those traits and argues that Supreme Court decisions actually present a coherent logic for when digital searches trigger the Fourth Amendment. The Court is wary of unfettered police access to devices that collect intimate information with little to no human direction or control. An animating principle emerges: If a device collects diaristic data—that is, information revealing day-to-day activities and intimate associations—*and* collects such data automatically, robust Fourth Amendment protections apply.

Part I illustrated how automobiles are now like smartphones, performing some of the same functions. But the "automatic diary" principle, as I call it, should provide more clarity on whether and when auto data is *enough* like smartphone data for Fourth Amendment purposes. This final Part teases out a principle from the doctrines discussed above and argues that, applied to indirect and direct access to auto data, there are clear answers as to when the Fourth Amendment bars warrantless access. At the very least, police can neither warrantlessly request auto location history from auto data companies nor warrantlessly extract auto data from vehicles.

A. The Automatic Diary Principle

The morass of auto data case law coming out of lower courts evinces broader uncertainty around when to find a reasonable expectation of privacy in the wake of *Carpenter*, *Jones*, and *Riley*. How does Fourth Amendment protection vary based on the type of data accessed? The length of time implicated by the data? The method of access?

These questions become more manageable if we discern an articulable principle that categorizes a device as more like a cellphone than a wallet or a bank record, such that certain data from that device enjoys a reasonable expectation of privacy, just like CSLI. The Court's anxiety spikes when a technology collects information that reveals intimate facts and daily activities—information that can be described as diaristic. But many warrantless searches uncover diaristic information without raising

any Fourth Amendment issues;[160] something else makes a cellphone and location history particularly worthy of protection. In practice, the Court intervenes when a device collects this diaristic information in the background of providing other services, without any affirmative direction or guidance from the data subject. In other words, the technologies that have thus far prompted Court action are *automatic* diaries. This characteristic, perhaps not unique to digital devices but certainly rare otherwise, captures the combination of concerns motivating the Court's application of the Fourth Amendment to recent digital searches.

The Court has expressed strong discomfort with warrantless access to devices that collect diaristic information. "Diaristic" used here refers to the general understanding of a diary as containing detailed records of activities, allowing an inference into a diary subject's day-to-day life, relationships, and beliefs, but not necessarily archiving every moment of a person's life. This definition hopefully rings familiar after Section II.A. Justice Sotomayor's concurrence in *Jones* recognized that long-term GPS tracking of a vehicle may implicate a reasonable expectation of privacy because it "reflects a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations."[161] The *Carpenter* majority cited this language in finding CSLI similarly "provides an intimate window into a person's life."[162] The *Riley* Court was more explicit: "A decade ago police officers . . . might have occasionally stumbled across a highly personal item such as a diary. . . . Today, by contrast, . . . many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives . . . ."[163]

The *Riley* Court's direct comparison of a cellphone to a diary was not the first time someone made this connection. Influential technologists have strived to make this conflation a reality. In 1995, Bill Gates declared that computers would soon record anything that its user has read, seen, or heard in her lifetime.[164] Soon after, Microsoft Research began a "life-logging" experiment through MyLifeBits, a project aiming to create an exhaustive digital archive on and about the test subject,

---

160 Justice Kennedy made this point in his dissent to *Carpenter*, pointing out that financial records arguably reveal more intimate information than location data. Carpenter v. United States, 138 S. Ct. 2206, 2232 (2018) (Kennedy, J., dissenting).

161 United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

162 *Carpenter*, 138 S. Ct. at 2217 (majority opinion).

163 Riley v. California, 573 U.S. 373, 395 (2014).

164 Leo Hickman, *Dear Digital Diary – Lifelogging in the Internet Age*, The Guardian (Aug. 12, 2012) (citing Bill Gates, The Road Ahead 405–06 (1995)), https://www.theguardian.com/technology/2012/aug/12/lifelogging-dear-digital-diary [https://perma.cc/YV5K-BY3L].

Gordon Bell.[165] By 2014, the year that *Riley* was published, one peer-reviewed study claimed that no special technology is needed to create these digital archives: Smartphones so comprehensively document a user's activities and personality that an analysis of resulting data can produce a "smart diary."[166] The authors of the study noted that smartphones provide an "ideal platform" because they contain a range of sensors generating multiple data sources: "motion activities, location data, app usage, calendar events, phone calls or SMS messages, and web history."[167] But even one data stream can produce diaristic information—other studies have discussed the potential benefits of replacing travel diaries with GPS data or Google Location history due to their lack of compliance issues and self-reporting inaccuracies, with one study even noting that it is "feasible to derive trip *purpose* from the GPS data."[168]

The diaristic nature of GPS tracking, location information, and cellphone contents lurks in the Court's digital search reasoning.[169] The *Riley* Court noted how cellphones collect "many distinct types of information that reveal much more in combination than any isolated record" and that, given a phone's storage capacity, "even just one type of information . . . convey[s] far more than previously possible."[170] The *Carpenter* Court called CSLI "encyclopedic" and a "detailed chronicle."[171] CSLI, as both comprehensive and a routinely updated archive, can thus be understood as diaristic. The framing of the diary addresses two of the factors the *Carpenter* Court names as determinative—the nature of the information and retrospectivity. The information contained in cellphones and CSLI records effectively allows a reader to infer the

---

165 Gordon Bell & Jim Gemmell, *A Digital Life*, Sci. Am. (Mar. 1, 2007), https://www.scientificamerican.com/article/a-digital-life [https://perma.cc/RL8L-YRZ6] ("For the past six years, we have attempted to record all of Bell's communications with other people and machines, as well as the images he sees, the sounds he hears and the Web sites he visits—storing everything in a personal digital archive that is both searchable and secure.").

166 Jilong Liao, Zhibo Wang, Lipeng Wan, Qing Charles Cao & Hairong Qi, *Smart Diary: A Smartphone-Based Framework for Sensing, Inferring and Logging Users' Daily Life*, 15 IEEE Sensors J. 2761 (2014).

167 *Id.* at 2763.

168 Jean Wolf, Randall Guensler & William Bachman, *Elimination of the Travel Diary: Experiment to Derive Trip Purpose from Global Positioning System Travel Data*, 1768 Transp. Rsch. Rec.: J. Transp. Rsch. Bd. 125, 125 (2001) (emphasis added); *see also* Dillan Cools, Scott Christian McCallum, Daniel Rainham, Nathan Taylor & Zachary Patterson, *Understanding Google Location History as a Tool for Travel Diary Data Acquisition*, 2675 Transp. Rsch. Rec.: J. Transp. Rsch. Bd. 238, 240, 242 (2021) (finding that GPS and location history lacked the compliance problems and inaccurate recollection found in travel diaries).

169 *See* Riley v. California, 573 U.S. 373, 375, 396 (2014) (pointing out the ability of GPS to track down to the minute location data and cellphones to store thousands of intimate pictures, texts, and videos as playing an important role in privacy concerns).

170 *Id.*

171 Carpenter v. United States, 138 S. Ct. 2206, 2209, 2220 (2018).

day-to-day chronological activities of the data subject and from there infer occupations, relationships, political affiliations, and more.

But the key characteristic for the cellphone in *Riley* and the location records in *Carpenter* cannot merely be containing diaristic information. Though digital devices are much more likely to be diaristic than analog items, some analog items also catalog a wealth of detail about our lives—after all, physical diaries exist. Justices have occasionally cited the diary as an item whose unfettered search would outrage the public sensibility.[172] But diaries hardly dominate Fourth Amendment jurisprudence, often appearing more in Fifth Amendment cases.[173] If an officer found an address book on a person during a search incident to arrest, that officer could flip through the pages.[174] If someone gives their diary to a third party, that diary loses a certain expectation of privacy.[175] And a list of credit card transactions may be just as revealing of someone's activities, relationships, and beliefs as location histories or a diary. Intimate information does not enjoy an absolute protection from law enforcement searches just by nature of its intimacy.

This Note offers that the Court's recent opinions evince anxiety about searches of diaristic digital devices when their users did not direct them to be diaries. An analog diary is written by its subject, who self-reports her activities, feelings, and opinions. But digital devices often serve primary functions besides documentation. The diary subject is not an active or intentional archivist—rather, the diary is the diarist. These devices gather information automatically, without user prompting.[176] The *Carpenter* majority names automation as a reason why CSLI

---

172 *E.g.*, Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 545 n.1 (1977) (Rehnquist, J., dissenting) ("A dictabelt tape or diary may be 'private' . . . in the sense that the Fourth Amendment would prohibit an unreasonable seizure of it . . . ."); Couch v. United States, 409 U.S. 322, 350 (1973) (Marshall, J., dissenting) ("Diaries and personal letters that record only their author's personal thoughts lie at the heart of our sense of privacy.").

173 *See, e.g.*, Fisher v. United States, 425 U.S. 391, 427 (1976) (Brennan, J., concurring) ("Papers in the nature of a personal diary are *a fortiori* protected under [Fifth Amendment] privilege."); *Couch*, 409 U.S. at 350 (comparing diaries to tax records, where the majority found that taxpayer's ceding of tax records to an independent accountant eliminated any Fifth Amendment privilege to the records).

174 *See, e.g.*, United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993) (holding that searching and photocopying the contents of defendant's address book were permissible searches incident to arrest).

175 *See, e.g.*, State v. Andrei, 574 A.2d 295, 296–97 (Me. 1990) (holding that defendant's husband presenting defendant's open diary to police for police to read did not constitute a Fourth Amendment search); People v. Willey, 303 N.W.2d 217, 217–18 (Mich. Ct. App. 1981) (holding that there was no Fourth Amendment search when relatives of defendant's deceased husband brought defendant's diary to the prosecutor's office and pointed out sections in which defendant expressed hatred for the deceased).

176 *Passive Data Collection*, Int'l. Ass'n. Priv. Pros., https://iapp.org/resources/article/passive-data-collection [https://perma.cc/D5GT-R78G].

does not fit under the third-party doctrine: "[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up."[177] Under these circumstances, a digital device can amass a wealth of information about its user without the user commanding the device to create such an archive. The trigger for information collection is simply being on.

There are a few reasons why automatic diaries provoke unease and catapult certain technologies into distinct Fourth Amendment categories. Our precedents accounted for how certain items may reveal intimate information about us. They didn't quite fathom that something could amass such information about us without our knowledge or control, short of the surreptitious surveillance prohibited in *Katz*.[178] Automatic diaries collect information in the course of providing other services to a perhaps unaware user. The device, not the user, decides what information gets collected. This lack of autonomy changes the nature of the information collected: In the Court's words, "[u]nlike the nosy neighbor who keeps an eye on comings and goings, [CSLI collectors] are ever alert, and their memory is nearly infallible."[179] These devices collect information that a user might not have chosen to record, like sensitive location information. And with their many sensors, these devices often collect information that a subject might not even have known about herself.[180]

Automation also sets diaristic digital devices apart from analog diaries because it changes the relationship between the data subject and her "diary." When the *Riley* Court compared cellphones to diaries, it was in the context of a broader point that these devices exploded the limits that "physical realities" previously imposed on a search.[181] Most people don't bring physical diaries around with them everywhere they go. Nor would they regularly share their diary contents with third parties. But automatic diaries often serve other important functions—the car in *Jones* drives its user around and the cellphone in *Carpenter* allows its user to communicate with others. The resulting

---

177 Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

178 Katz v. United States, 389 U.S. 347 (1967) (concerning FBI agents attaching a bug to a telephone booth so as to eavesdrop on defendant's phone call).

179 *Carpenter*, 138 S. Ct. at 2219.

180 *See* Bell & Gemmell, *supra* note 165 ("Digital memories can do more than simply assist the recollection of past events, conversations and projects. Portable sensors can take readings of things that are not even perceived by humans . . . ."); Zoë Corbyn, *The Dawn of Tappigraphy: Does Your Smartphone Know How You Feel Before You Do?*, The Guardian (Nov. 7, 2021), https://www.theguardian.com/technology/2021/nov/07/the-dawn-of-tappigraphy-does-your-smartphone-know-how-you-feel-before-you-do [https://perma.cc/C7RR-ALBX] (discussing the applicability of the smartphone to detect medical conditions, like upcoming epileptic episodes, from a person's keystrokes).

181 Riley v. California, 573 U.S. 373, 375 (2014).

"digital record" is incidental to these other functions.[182] While the user is in control of when she deploys those functions, she does not exercise as much control over the diary that's generated as she uses the device. Automation of information collection and transmission is in large part why it is so easy for police to access information from such devices through third parties.

Cellphones raised red flags for the Court because they contain intimate information rivaling traditional diaries—even information that the subject does not know—without the conventional user control over what about her life gets chronicled. It is useful to conceptualize the Court's decisions in these terms because it clarifies that, although the revealing nature of accessed information matters, that's not the whole ballgame: Cellphones and CSLI are distinct because they collect this intimate information on their own. Automation thus captures the *Carpenter* majority's "voluntariness" concern, as well as the nature of the information and the ease of police access. Justice Kennedy, and others, criticized the majority's voluntariness argument that cellphones are essential to modern life in a way distinct from bank accounts or credit cards.[183] A more fruitful analysis of voluntariness is to consider whether a device user is truly consenting to the device generating a wealth of information on her if that collection is so attenuated, so background, from her actual use of the device. This framework more cleanly differentiates financial records from CSLI. Bank and credit card transactions are discrete, affirmative actions that individuals undertake for their very function; the resulting records documenting such transactions are not capturing information incidental to use, but core to it.

I make no claim that the automatic diary principle is the only way to elucidate the Court's jurisprudence on digital searches. If anything, it provides a floor and not a ceiling to understanding how the Court may protect digital data from warrantless access. But understanding the core feature of CSLI records and cellphones that drove the Court to impose robust Fourth Amendment protections will make it much easier to sort out which other digital devices similarly satisfy the *Carpenter* factors or the *Riley* logic. A device must routinely collect information revealing enough about a person's life to infer day-to-day activities and associations, and it must collect that information

---

182 *See id.* (pointing out that a cellphone collects nearly every aspect of one's life by virtue of being on one's person).

183 *See Carpenter*, 138 S. Ct. at 2210; *id.* at 2233 (Kennedy, J., dissenting) (noting that "the decision whether to transact with banks and credit card companies is no more or less voluntary than the decision whether to use a cell phone" because "it is impossible to participate in the economic life of contemporary society without maintaining a bank account." (quoting United States v. Miller, 425 U.S. 435, 451 (1976))).

automatically, with little human direction or control beyond turning on the device.

B. Applying the Principle to Indirect Access

How does the automatic diary principle shake out in auto data cases? This Note does not granularly assess the principle's application to each type of auto data, but it does offer a sketch. The *Carpenter* Court cleared the way for Fourth Amendment protections to apply even when a defendant has shared the accessed information with a third party. The Court did not hold that CSLI is the only type of data falling outside the bounds of the third-party doctrine, instead pointing to a number of generalizable factors—nature of the information, ease of access, potential for retrospectivity, and voluntariness—that created a category different from *Smith* and *Miller* records.[184]

Indirect access to auto data is as cheap, easy, and efficient as accessing CSLI through cell service providers. Law enforcement can cheaply and quickly request auto data from auto data companies by contacting them through available channels.

Analyzing the other factors requires a bit more work and is where lower courts disagree. Although case law currently only addresses auto location data, auto data encompasses many different types of data, as detailed in Part I. Assessments of the two other factors must be data-specific, since the analysis may produce different results. Discerning a larger principle gives us a launching pad to assess requests for different types of data spanning different lengths of time.

Auto location histories seem comparable to CSLI, but courts disagree on whether the two data types are similar enough for constitutional purposes.[185] These conflicting decisions don't even address when police request real-time location information instead of an archive, or when they ask for other types of data like speed history or voice recordings.[186]

---

[184] *Id.* at 2220 ("We do not express a view on matters not before us . . . [n]or do we address other business records that might incidentally reveal location information."); *id.* at 2217–18 (comparing the nature of CSLI information to GPS data on the basis of factors like retrospectivity, ease of access, and intrusiveness).

[185] *Compare* Bailey v. State, 311 So. 3d 303, 304 (Fla. Dist. Ct. App. 2020) (holding that Defendant had no reasonable expectation of privacy in GPS records), *with* United States v. Diggs, 385 F. Supp. 3d 648 (N.D. Ill. 2019) (holding that *Jones* and *Carpenter* require police to secure a warrant before accessing extensive auto location data, whether through a company or the vehicle itself).

[186] *See, e.g.*, *Bailey*, 311 So. 3d at 304; United States v. Dantzler, No. CRIM. 10-0024, 2010 WL 2740003, at *6 (W.D. La. June 16, 2010), *report and recommendation adopted*, No. CRIM. 10-0024, 2010 WL 2737178 (W.D. La. July 9, 2010) ("Dantzler either knew or should have known that he was renting an OnStar[-]equipped vehicle that was capable of transmitting the vehicle's location to a monitoring service . . . . [D]efendant accepted the risk . . . ."); *id.* at *4–5

Using the automatic diary principle, it becomes clear that auto location data is enough like CSLI to garner Fourth Amendment protections. Even if people are not physically in their vehicles for most of the day, most Americans drive to work, school, homes of significant others, doctors' offices, religious sites, political demonstrations, and countless other places associated with our deeply held beliefs or private affiliations. A vehicle's GPS location data provides even more precise location data than CSLI.[187] And once individuals drive to a place, they're likely to stay there until they return to their vehicle to drive to the next place: Law enforcement can infer individuals' locations in between changes in auto location. This location data is generated in the background as soon as a vehicle is turned on.[188] Of course, like with CSLI, the timespan of requested data matters as to whether the accessed information is in fact diaristic. But even if the precise line is hard to draw, it seems evident that law enforcement seeking days' or weeks' worth of auto location data will access a "detailed chronicle" and therefore must seek a warrant.[189]

As to the "voluntariness" prong, we should ask whether auto data subjects truly consent to sharing location data, or if data sharing happens in the background and without user prompting in a way that attenuates it from the actual use of the vehicle. Of course, vehicles primarily serve to drive from place to place, and in that sense, location is germane to the primary use. But this only means that drivers and passengers have a location in mind when they get into a car, and perhaps a way to get to that location. It does not mean that drivers expect their location to be recorded every step of the way, and certainly doesn't mean they expect their location to be stored long after they have arrived at their destination. Again, *Carpenter* is informative. CSLI is generated every time a phone connects to nearby cell towers—these connections are

(finding that the defendant had no reasonable expectation of privacy in the movement on public thoroughfares of his rented vehicle which was also shared with a third party); United States v. Diggs, 385 F. Supp. 3d 648 (N.D. Ill. 2019) (holding that Defendant had a reasonable expectation of privacy in his physical movements as revealed by his wife's car's GPS data, and that turning over that data to the car dealership did not defeat this expectation).

187 *See Carpenter*, 138 S. Ct. at 2218 (discussing how cell site location information is less precise than GPS information).

188 In fact, up until recently it seemed like there was no effective way to opt out of location tracking; with the recent enactment of the California Privacy Rights Act, California residents may be among the first in the country to enjoy an opt-out right. Jamie Court, *California Poised to Be First State to Stop Geolocation Tracking, New Report Shows Need For Privacy Protections from Connected Cars*, Consumer Watchdog (Mar. 30, 2022), https://www.consumerwatchdog.org/privacy-technology/california-poised-be-first-state-stop-geolocation-tracking-new-report-shows-need [https://perma.cc/E4BX-YPRC].

189 *See Carpenter*, 138 S. Ct. at 2220 (finding that such a chronicle implicates greater privacy concerns than in *Smith* and *Miller*).

what allow cellphones to get signal.[190] CSLI thus plays a critical role in facilitating nearly all useful functions of the device. But the role the data plays in active use of the device doesn't mean that cellphone users meaningfully consent to the location tracking—this information is still collected indefinitely, in the background and without users affirmatively choosing to have it collected. The same can be said for auto location data.

What about indirect access to other types of auto data? It will depend. Just as what is revealed through a data subject's aggregate movements, other auto data like text messages or voice recordings may "provide[] an intimate window into a person's life."[191] This, of course, may not apply to all auto data. Speed histories,[192] say, don't necessarily provide an intimate window into the life of a driver or occupant. A data-specific approach may be necessary in parsing which forms of auto data are more like CSLI than like bank records. After all, the existing case law suggests that law enforcement have mainly been concerned with accessing real-time and historical location data thus far.[193] Auto data companies are likely only able to provide limited types of information, both by nature of capability and federal laws prohibiting disclosure of stored communications[194]: The case law may be focused on location

---

190 *Id.* at 2208.

191 *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

192 *See* Brewster, *supra* note 50.

193 *See, e.g.*, Bailey v. State, 311 So. 3d 303 (Fla. Dist. Ct. App. 2020); United States v. Dantzler, No. CRIM. 10-0024, 2010 WL 2740003, at *6 (W.D. La. June 16, 2010), *report and recommendation adopted*, No. CRIM 10-0024, 2010 WL 2737178 (W.D. La. July 9, 2010) ("Dantzler either knew or should have known that he was renting an OnStar[-]equipped vehicle that was capable of transmitting the vehicle's location to a monitoring service . . . . [D]efendant accepted the risk . . . ."); *id.* at *4–5 (finding that the defendant had no reasonable expectation in the movement on public thoroughfares of his rented vehicle which was also shared with a third party); United States v. Diggs, 385 F. Supp. 3d 648, 652 (N.D. Ill. 2019) (holding that Defendant had a reasonable expectation of privacy in his physical movements as revealed by his wife's car's GPS data, and that turning over that data to the car dealership did not defeat this expectation).

194 The SCA effectively only requires a warrant for accessing recently stored communications content like phone call recordings or texts, and only requires a warrant for older content if the data subject is not notified. *See* Stored Communications Act, 18 U.S.C. §§ 2703, 2703(b)(2), 2510(1), 2510(12), 2510(14) (defining electronic communications service under 2510(14) and remote computing service under 2711(2)). A loophole allows law enforcement to warrantlessly access older content without notification through a "delayed notice" provision. *See id.* § 2705. Other stored content and non-content (like records about the data subject stored by the provider) can be obtained just through a subpoena or a § 2703(d) order. *See id.* § 2703(d). Note, however, that some jurisdictions have expanded the warrant requirement to all stored contents. *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (holding that the government must obtain a warrant to access email through a third party provider). The Supreme Court has not ruled on the issue.

data both because it's what law enforcement seeks most often, and also because it is what auto data companies are capable of providing.

The automatic diary principle therefore clarifies how to use the *Carpenter* factors, revealing what about the nature of the information or the level of voluntariness will make data more like CSLI than like bank records. For auto data, it reveals that at least some categories of auto data, and the type most frequently obtained from auto data companies, is protected by a warrant requirement.

C. Applying the Principle to Direct Access

Carpenter squarely applies to indirect access, but whether it applies outside that context is still an open question.[195] That leaves direct access murkier, since the looming doctrine here—the automobile exception—has yet to grapple with the idea of automobiles as digital devices.

There are a few ways to situate auto data in larger automobile search jurisprudence. One possibility is that auto data modules are a part of the automobile and not subject to special rules: The automobile exception applies as usual. Another possibility is that auto data modules are still just part of the automobile, but their automated and diaristic capabilities transform the entire vehicle into a protected digital device: Then the automobile exception not only doesn't apply to the auto data module, but also doesn't apply to the entire car. Perhaps more likely, and as suggested by lower courts, the auto data module is its own distinct device[196]: Then the module is a container, which may still be subject to warrantless search or may enjoy special protections under *Riley* or *Chadwick* as an automatic diary.

Let's start with the possibility voiced by the Florida District Court of Appeal in *Worsham*, that auto data modules are discrete devices falling under *Riley*'s scope such that law enforcement must obtain warrants to access them.[197] The implication is that *Riley* broadly bars warrantless access to certain digital devices, not just to cellphones and not just in the search-incident-to-arrest context. The *Worsham* court diagnosed auto data modules as "analogous to other electronic storage devices for which courts have recognized a reasonable expectation of privacy" and required a warrant on the basis that these modules contain "constant,

---

195 *See, e.g.*, Matthew Tokson, *The* Carpenter *Test as a Transformation of Fourth Amendment Law*, 2023 U. Ill. L. Rev. 507, 511 (contending that the *Carpenter* test should be the primary test for Fourth Amendment searches going forward).

196 *See* State v. Worsham, 227 So. 3d 602, 604 (Fla. Dist. Ct. App. 2017) (comparing the EDR data module to a cellphone).

197 *Id.* at 606 (holding police could not access EDR data, either through extraction or through a third party, without a warrant).

unrelenting . . . surveillance."[198] The automatic diary principle is instructive in parsing just what makes auto data modules "analogous" to cellphones. Just like cellphones, auto data systems are minicomputers that ostensibly serve one function (driving) but in practice collect diaristic data in the background: photos, videos, calendars, albums, maps, rolodexes, the list goes on.[199] These modules collect many disparate strands of information, some that a driver may not even be aware of, such as throttle or brake statistics. And just like a cellphone extraction, an auto data extraction allows law enforcement to access all these strands of information with the technology not yet capable of narrowly limiting the scope of extraction: Plugging into the auto data module would give police full access to the wealth of diaristic information contained therein.

Of course, one could read *Riley* narrowly to only address searches incident to arrest. Then, *Riley* may still require police to obtain a warrant before searching auto data incident to arrest, since (as demonstrated above) auto data is an automatic diary like a cellphone. But then what about outside of the arrest context? It would seem a perverse interpretation of the doctrine to allow police to warrantlessly search auto data in a routine traffic stop before arrest, pursuant to the automobile exception, but to require a search warrant to access that same data after arrest. Yet Adam Gershowitz has argued that this disparity may make sense, given that searches incident to arrest require no level of individual suspicion that someone is carrying evidence of crime or dangerous instruments, while searches of automobiles do still require probable cause.[200]

If *Riley* does not apply, the auto data analysis rests entirely on whether auto data falls under the automobile exception. The automobile exception is justified on the grounds that (1) automobiles are inherently mobile; and (2) automobiles enjoy a diminished expectation of privacy because they are pervasively regulated and their movements are knowingly exposed to the public.[201] As applied to auto data hardware, neither rationale makes much sense. Say the auto data module is a container within the automobile, such that we can think of it separately from the vehicle itself—lower courts have found as such for gas tanks and other vehicle compartments.[202] An auto data module is

198 *Id.* at 604, 608.

199 *Id.* at 604.

200 Gershowitz, *supra* note 30, at 1161–67 (arguing that *Riley* is unlikely to extend to automobiles because vehicles hold less information than cellphones, a lot of vehicle data is already visible to the public, cars receive less privacy protection, and the automobile exception still requires probable cause).

201 *See supra* notes 131–37 and accompanying text.

202 *See, e.g.*, United States v. Urbina, 431 F.3d 305, 310 (8th Cir. 2005) (noting that the auxiliary gas tank was like an "unlocked container[] within the vehicle").

hardly mobile: Class action lawsuits have pointed out the very fact that Berla only sells its toolkits to government entities and private companies, leaving individuals with no recourse to remove the hardware and extract data about themselves.[203] Auto data modules may also retain a reasonable expectation of privacy because they are essentially locked containers, impenetrable to most. In this sense, they're arguably analogous to the locked luggage found in a car trunk in *Chadwick*.[204]

But the analysis gets trickier if auto data modules cannot be conceptually separated from the vehicle. One could argue that, in the era of digital automobiles, automobiles are themselves automatic diaries, such that the entire vehicle is a device worthy of more fulsome protection. Courts may be resistant to, if not outright horrified by, effectively overruling the automobile exception in this way. The uncertainty of how to think about direct access within the automobile exception framework reveals that the automatic diary principle doesn't as neatly apply in this context as it does with the third-party doctrine. This is precisely because the automobile exception has not caught up with modern technology. But even then, we can still discern that auto data hardware—which is difficult to access or modify, contains a wealth of information, and collects information in the background as soon as a vehicle is turned on—meets the criteria for an automatic diary. Understanding *Riley* to protect all automatic diaries from warrantless searches would extend the same protections to auto data hardware, but even if later Court precedent limits *Riley* to the search-incident-to-arrest context, there is reason to believe that the characteristics of auto data that make it like an automatic diary give it a full expectation of privacy under *Chadwick* as well.

Conclusion

Most Americans drive cars, and most of those cars collect and retain intimate information about them.[205] If law enforcement can exploit an exception meant for physical records to gather far-reaching data from auto data companies, then the Fourth Amendment's presumed

---

[203] *See, e.g.*, John Fitzgerald, *Toyota Vehicles Unlawfully Intercept Smartphone Data, Class Action Says*, Westlaw Today (Sept. 28, 2021), https://today.westlaw.com/Document/I05647940209111ecbea4f0dc9fb69570/View/FullText.html [https://perma.cc/LHD5-TSP7] (discussing a lawsuit alleging that Toyota's infotainment system stores a copy of all texts from connected smartphones to the car's memory system, where plaintiffs argue the average user cannot access downloaded information even though the government can); First Amended Complaint ¶ 83, Jones v. Ford Motor Co., No. 3:21-CV-05666-DGE, 2022 WL 1423646, at *14 (W.D. Wash. May 5, 2022) ("Berla specifically restricts access to its systems, making them available primarily to law enforcement and private investigation service providers.").

[204] *See* United States v. Chadwick, 433 U.S. 1, 3–4 (1977).

[205] *See supra* note 20 and accompanying text.

warrant requirement is rendered toothless. And if law enforcement can extract extensive, private information during traffic stops, the automobile exception becomes a doctrine permitting deeply invasive searches on probable cause alone. The breadth and depth of auto data fits into the larger digital landscape, right alongside an emerging economy of Internet of Things devices, where similar concerns about our data are growing every day.[206]

Existing Fourth Amendment doctrine correctly applied would prevent such discretionary and overbroad access to auto data. *Carpenter*'s limit on the third-party doctrine for certain digital data and *Riley*'s imposition of robust protections for certain digital devices reveal that the Supreme Court is developing a set of Fourth Amendment rules specific to digital searches. The principle behind these new rules is this: Digital devices are worthy of concern when they operate like automatic diaries, collecting intimate information about their users without user direction or control. Auto data—in vacuuming up information on how you drive, how you live, and who you know, all because you turn on the engine and plug in your phone—satisfies the automatic diary principle and requires a warrant to access.

A warrant requirement for police access to auto data, as argued for in this Note, would materially curb police discretion and impose a standard of probable cause and external authorization. But a warrant requirement alone is not sufficient. Warrant requests are often rubber-stamped and may not in and of themselves provide meaningful protections.[207] Nonetheless, such a warrant requirement for auto data access will do real work in ensuring that cartapping is one fewer shortcut that police can take to access some of our most personal information.[208]

---

[206] *See, e.g.*, Andrew G. Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547 (2017) (discussing how the Fourth Amendment could apply to protect data collected by smart devices).

[207] Especially in the age of electronic warrants, it appears that magistrate judges functionally rubber stamp most warrant applications with little pushback. *See* Tim Cushing, *Disrupting The Fourth Amendment: Half of Law Enforcement E-Warrants Approved in 10 Minutes or Less*, TECHDIRT (Jan. 25, 2018), https://www.techdirt.com/articles/20180119/17394739046/disrupting-fourth-amendment-half-law-enforcement-e-warrants-approved-10-minutes-less.shtml [https://perma.cc/5YR3-8RWN].

[208] *See, e.g.*, State v. Smith, 278 A.3d 481, 497 (Conn. 2022) ("[T]he search warrant . . . did not sufficiently limit the search of the contents of the cellphone by description of the areas within the cellphone to be searched, or by a time frame reasonably related to the crimes.").