AUTOMOBILE EVENT DATA RECORDERS, AND THE FUTURE OF THE FOURTH AMENDMENT

*Daniel Harper**

To determine whether there has been a violation of the Fourth Amendment, courts must first analyze whether there has been a "search" or "seizure." Current doctrine offers two methods of identifying a "search": the trespassory test and the Katz *test. Scholars have criticized the* Katz *test, which asks whether an individual has a reasonable expectation of privacy, as being difficult to apply. In* Carpenter v. United States*, Justice Gorsuch proposed discarding the current framework in favor of a new model. Under his suggested approach, an individual's Fourth Amendment rights would be determined on the basis of their property rights (the "strict property test"). To test the feasibility of the proposal, this Note applies Justice Gorsuch's framework to an issue that current doctrine appears to struggle with: Are downloads of Event Data Recorder (EDR) data Fourth Amendment searches? EDRs are computers installed in modern cars that record information on the vehicle's operation, and state courts have split on whether law enforcement downloads of the data stored on these devices constitute Fourth Amendment searches. After examining the issue of EDR data downloads through the lens of the strict property test, this Note suggests that Fourth Amendment law would be better served by a series of minor doctrinal shifts rather than the substantial modification that Justice Gorsuch advocated for in* Carpenter.

INTRODUCTION

Ninety-nine percent of registered vehicles in the United States are equipped with a little-known device: an event data recorder (EDR).[1] Usually embedded beneath the carpeting underneath the driver's seat,[2] these devices continuously measure information on a car's speed, braking,

* J.D. Candidate 2020, Columbia Law School. The author would like to thank Professor Daniel Richman for his guidance throughout the Note-writing process and the staff of the *Columbia Law Review* for their outstanding editorial assistance.

1. Richard Ruth, Ruth Consulting, LLC, Presentation at the Symposium on Traffic Safety: EDR Update 2018, at 4 (May 21–24, 2018), https://iptm.unf.edu/uploadedFiles/summit/handouts/Ruth%20R_2_EDR%20Update%202018.pdf [https://perma.cc/R83Q-QDAG].

2. How to Preserve Your Car Black Box (Event Data Recorder), Collision Sci. (Dec. 1, 2014), https://collisionsciences.ca/event-data-recorder-removal [https://perma.cc/Z653-L42P] (diagram depicting typical locations); see also Steven T. Kean, Va. State Police, Event Data Recorder: An Overview 6–7 (2015), https://cdn.ymaws.com/mcaa-mn.org/resource/resmgr/files/tsrp/Resources/EDR_Overview_2-2015_-_Virgin.pdf [https://perma.cc/7FEZ-DNGF] (providing images to demonstrate the location of the ports through which the EDR module can be accessed).

acceleration, angular momentum, and other similar data.[3] This information is generally not retained in permanent storage unless the car is in an accident, in which case the EDR will permanently save the data for the five seconds preceding the accident.[4] In the event of an accident, law enforcement can use data saved on an EDR to reconstruct the facts of the accident and support criminal cases brought by the state for charges such as involuntary manslaughter or driving under the influence.[5] To date, five state court systems—yielding six appellate court opinions—have ruled on what restraints the Fourth Amendment imposes on law enforcement efforts to obtain EDR data.[6]

The opinions feature an astonishing degree of variation on the threshold question of whether the Fourth Amendment protects EDR data at all.[7] The Fourth Amendment limits the government's ability to conduct a "search" or "seizure."[8] Thus, for the Fourth Amendment to protect EDR data, it must be a "search" to download EDR data.[9] Current doctrine provides two methods for determining if a search has occurred: the *Katz* test[10] and the

---

3. Federal regulations require that EDRs record at least fifteen data points. See 49 C.F.R. § 563.7(a) (2019).

4. See Michelle V. Rafter, Decoding What's in Your Car's Black Box, Edmunds (July 22, 2014), https://www.edmunds.com/car-technology/car-black-box-recorders-capture-crash-data.html [https://perma.cc/T9KT-T9XU]. The data is saved locally onto the EDR hard drive; these "black box" devices do not rely on cloud storage. See id.

5. See, e.g., People v. Diaz, 153 Cal. Rptr. 3d 90, 96–97 (Ct. App. 2013) (describing the evidence obtained from an EDR and its use by police to determine the conduct of the defendant in the moments before a fatal automobile accident); Chavis v. Commonwealth, No. 1029-16-2, 2017 WL 3026772, at *1–2 (Va. Ct. App. July 18, 2017) (describing the prosecution's use of EDR data to establish the defendant's speed in support of a charge of involuntary manslaughter); Miller v. Commonwealth, No. 0193-16-2, 2017 WL 3026782, at *1–2 (Va. Ct. App. July 18, 2017) (describing the prosecution's use of EDR data to establish that the defendant was not wearing a seatbelt at the time of a car accident and did not attempt to steer away from the accident to support a conviction for driving under the influence).

6. As of October 23, 2019, a Westlaw search querying <"event data recorder" & "Fourth Amendment"> for all federal and state courts, without any time limits, yields twenty cases, but only six of those opinions actually address the issue of Fourth Amendment limits on EDR data. See *Diaz*, 153 Cal. Rptr. 3d at 97–102; State v. Worsham, 227 So. 3d 602, 603–06 (Fla. Dist. Ct. App. 2017), cert. denied, 138 S. Ct. 264 (2017); Mobley v. State (*Mobley I*), 816 S.E.2d 769, 772–74 (Ga. Ct. App. 2018), rev'd, 834 S.E.2d 785 (Ga. 2019); State v. West, 548 S.W.3d 406, 414–18 (Mo. Ct. App. 2018); People v. Christmann, 776 N.Y.S.2d 437, 441–42 (Justice Ct. 2004). A sixth case, People v. Xinos, 121 Cal. Rptr. 3d 496, 506–13 (Ct. App. 2011), also analyzed EDR data downloads but was ordered not to be published. This Note focuses on the Fourth Amendment analyses of EDR data in appellate court opinions, as they offer more detailed explanations of relevant doctrinal points.

7. See infra sections II.A–.B.

8. U.S. Const. amend. IV.

9. Cf. Carpenter v. United States, 138 S. Ct. 2206, 2220–21 (2018) (finding that a "search" within the meaning of the Fourth Amendment had occurred when police obtained the defendant's cell-site location information).

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

trespassory test.[11] Applying this doctrine, two courts concluded that downloading EDR data does not constitute a search.[12] The other four courts to consider the issue came to the opposite conclusion but followed dramatically different analytical frameworks to arrive at their respective holdings.[13]

The divergence in results highlights the difficulty in applying current Fourth Amendment doctrine in the digital age, and it draws particular attention to three difficulties in the current doctrine: the subjectivity of the *Katz* test, the unpredictability of the *Katz* test, and the lack of clarity on the relationship between the *Katz* test and the trespassory test. Many scholars have criticized the *Katz* test, seizing on the test's "ambiguous meaning, . . . its unsuitability for judicial administration, and its potential circularity,"[14] in addition to lamenting the subjective and unpredictable nature of the test.[15]

---

11. See United States v. Jones, 565 U.S. 400, 407–08 & n.5 (2012); see also Florida v. Jardines, 569 U.S. 1, 8–12 (2013) (finding that a search occurred because a law enforcement officer exceeded the confines of the implied license to enter private property and knock on the door of such property); Kyllo v. United States, 533 U.S. 27, 40 (2011) (holding that use of a thermal imaging device constituted a search because it would have required a physical intrusion to obtain the information revealed by the device at the time of the Founding).

12. See People v. Diaz, 153 Cal. Rptr. 3d 90, 97–103 (Ct. App. 2013); *Mobley I*, 816 S.E.2d 769, 774–75 (Ga. Ct. App. 2018).

13. State v. Worsham, 227 So. 3d 602, 608 (Fla. Dist. Ct. App. 2017) (concluding that the Fourth Amendment applied because the defendant had a reasonable expectation of privacy in the EDR data downloaded), cert. denied, 138 S. Ct. 264 (2017); Mobley v. State (*Mobley II*), 834 S.E.2d 785, 791–92 (Ga. 2019) (holding that an individual had standing to bring a Fourth Amendment challenge because law enforcement physically intruded into the relevant vehicle to download EDR data); State v. West, 548 S.W.3d 406, 421 (Mo. Ct. App. 2018) (same); People v. Christmann, 776 N.Y.S.2d 437, 441–42 (Justice Ct. 2004) (holding that the Fourth Amendment does protect EDR data, but that law enforcement does not need to obtain a warrant to access the data). The total of four opinions also excludes the trial court opinions in states where the case at issue was heard by an appellate court (i.e. Florida, Georgia, Missouri, and California).

14. William Baude & James Y. Stern, The Positive Law Model of the Fourth Amendment, 129 Harv. L. Rev. 1821, 1825 (2016).

15. These critiques, and others, have been extensively developed by Fourth Amendment scholars. See, e.g., Ronald J. Allen & Ross M. Rosenberg, The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge, 72 St. John's L. Rev. 1149, 1149 (1998) (arguing that the Court's Fourth Amendment doctrine "lacks coherence and predictability"); Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 384 (1974) (criticizing the first prong of the *Katz* test as seemingly permitting the government to declare the boundaries of Fourth Amendment protection); Craig M. Bradley, Two Models of the Fourth Amendment, 83 Mich. L. Rev. 1468, 1468 (1985) (describing a significant lack of agreement among courts on cases involving the Fourth Amendment); Sherry F. Colb, What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy, 55 Stan. L. Rev. 119, 121 (2002) (criticizing the Fourth Amendment doctrine defining the meaning of a "search" as "untenable"); Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476, 479–82 (2011) (proposing an alternate theory to both explain existing Fourth Amendment cases and guide resolution of future cases after describing problems with the current outcomes and underlying theoretical framework); Donald R.C. Pongrace, Stereotypification of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity, 34 Am. U. L. Rev. 1191, 1208 (1985) (describing Fourth Amendment doctrine as being in a state of

Drawing on such arguments, in his dissent in the recent case *Carpenter v. United States*, Justice Gorsuch proposed discarding the *Katz* test in favor of a strict reliance on property rights to determine what constitutes a search.[16] Under this approach (which this Note refers to as the strict property test), courts would determine if a search occurred by "ask[ing] if a house, paper or effect" that the government sought to access is "*yours* under law."[17] This Note analyzes whether the strict property test actually offers a less subjective, more predictable alternative to current Fourth Amendment doctrine by applying the strict property test to the issue of EDR downloads.

Ultimately, this Note argues that the strict property test, as currently formulated, does not in fact offer a less subjective and more predictable framework for determining whether a Fourth Amendment search has occurred. Section I.A summarizes what an EDR is, how it works, and what it is used for. Next, section I.B.1 provides a review of the relevant current Fourth Amendment doctrine. Section I.B.2 describes the facts and holding of *Carpenter* and then explains the contours of Justice Gorsuch's proposed strict property test. Section I.B.3 describes federal laws and regulations specifically governing EDR data, and section I.B.4 does the same at the state level. Section II.A describes the facts and holdings of the state court decisions that have addressed the application of the Fourth Amendment to EDRs, and section II.B details the rationales each court relied upon in reaching their respective decisions. Section II.C reviews the problems with current doctrine that are highlighted by the state court decisions. Section III.A then analyzes the issue of EDR data downloads under Justice Gorsuch's proposed approach. Section III.B compares the strict property test analysis with analysis under current doctrine. Drawing on this comparative analysis, section III.B concludes that significant work remains to develop Justice Gorsuch's strict property test as a superior alternative to the current framework, and it suggests a number of relatively minor doctrinal adjustments that can address the problems raised in section II.C.

I. EDR FUNCTIONS, FOURTH AMENDMENT DOCTRINE, AND THE *CARPENTER* PROPOSAL

This Part presents background information on EDRs, current regulation of their use, and established Supreme Court Fourth Amendment doctrine.

"theoretical chaos"); Richard A. Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 Sup. Ct. Rev. 173, 188–89 (criticizing the Supreme Court's reasoning in policy spying cases as "absurd," "circular," and "threadbare"); Jed Rubenfeld, The End of Privacy, 61 Stan. L. Rev. 101, 103–04 (2008) (criticizing Fourth Amendment doctrine for its failure to acknowledge the nature of privacy interests that it seeks to protect); Silas J. Wasserstrom & Louis Michael Seidman, The Fourth Amendment as Constitutional Theory, 77 Geo. L.J. 19, 28–29 (1988) (describing the lack of coherent theoretical underpinnings for the Fourth Amendment).

16. See 138 S. Ct. 2206, 2264–68 (2018) (Gorsuch, J., dissenting).

17. Id. at 2268.

A. *EDR Functions and EDR Data Uses*

Generally, EDRs continuously record at least fifteen data points that describe a car's functioning.[18] The information is not permanently stored (and thus cannot be accessed) unless a car is involved in what's known as a deployment "event."[19] A deployment event is generally an accident or a particularly harsh braking event, and in the case of such an event an EDR will record, to permanent local storage, the data it monitors for the five seconds prior to the accident.[20] Federal regulations require that data regarding frontal airbag deployment cannot be overwritten by subsequent events, but the other elements need only be retained for up to two events.[21] So, if your vehicle had two deployment events after an accident it's possible the accident data could get overwritten in the local EDR memory (aside from information on frontal airbag deployment).[22]

Event data recorders are generally located beneath the carpeting of vehicles, making it difficult to access the devices (and therefore the data contained on them) without physically intruding in the vehicle owner's car to plug into the download port located in the car or to remove the EDR module for later inspection.[23] To download EDR data, a crash investigator generally needs to obtain a specific set of hardware that can communicate with the EDR software.[24] It appears, based on the number of instructional courses available, that use of the hardware requires previous training and is not accessible to the average consumer.[25] EDR data can be used for a

---

18. See Rafter, supra note 4.

19. See Event Data Recorder, Nat'l Highway Traffic Safety Admin., https://www.nhtsa.gov/research-data/event-data-recorder [https://perma.cc/M9ZZ-4JTE] [hereinafter NHTSA Event Data Recorder Overview] (last visited Jan. 30, 2020); Rafter, supra note 4.

20. See Rafter, supra note 4. This is an important point; no sources indicate that vehicle manufacturers are remotely storing the information from EDRs installed in the average passenger vehicle at this time.

21. See 49 C.F.R. § 563.9 (2019).

22. In the absence of specific federal regulation, the storage capacity of the EDRs is probably subject to the preferences of the vehicle manufacturer. Many EDRs have the ability to record up to three events. See Kean, supra note 2, at 15.

23. See id. at 6–7 (providing, in a report authored by a senior Virginia state police trooper, pictures of the typical location of EDR devices and the download port used to access EDR data while the EDR device is still attached to the vehicle).

24. See id. at 6. The most established hardware used for the downloads currently sells for $7,300. See Bosch CDR Pro Tool Kit, Crash Data Grp., http://www.crashdatagroup.com/bosch-cdr-pro-tool-kit [https://perma.cc/4EWN-RZ4B] (last visited Jan. 30, 2020). The device is compatible with EDRs installed by the following manufacturers: BMW, Daimler, Fiat Chrysler Automobiles, Ford, General Motors, Honda, Karma Automotive, Mazda, Mitsubishi, Nissan, Subaru, Suzuki, Toyota, Volkswagen Group, and Volvo. See Bosch CDR Tool Kit Configuration Options, Crash Data Grp., https://www.crashdatagroup.com/bosch-cdr-kit-options [https://perma.cc/5DBR-UB3N] (last visited Jan. 30, 2020).

25. The Northwestern University Center for Public Safety offers a variety of training courses to instruct law enforcement officers on the use of EDR data, and the methods for extracting such data. See CDR Technician, Nw. Univ. Ctr. for Pub. Safety, https://registration.

variety of purposes,[26] but because the Fourth Amendment restricts only state actors,[27] this Note focuses on the potential government uses of the data.[28]

Law enforcement officers routinely seek access to EDR data when investigating traffic accidents. In a 2009 study surveying Texas police departments, EDR data was downloaded sixty-six percent of the time in fatal or possibly fatal crashes, forty-one percent of the time in serious personal injury cases, eleven percent of the time in accidents involving property damage, and two percent of the time in minor injury accidents.[29] As of a recent state court decision, it was standard practice for highway patrol in Missouri to download EDR data without a warrant at the initial investigation of a car accident.[30] As of 2013, it was also standard practice for the California Highway Patrol's (CHP) Multidisciplinary Accident Investigation Team (MAIT) to download EDR data without obtaining a warrant.[31]

---

nucps.northwestern.edu/courseDisplay.cfm?schID=1305 [https://perma.cc/WC8J-XKU7] (last visited Jan. 30, 2020).

26. See Martin Kaste, Yes, Your New Car Has a 'Black Box.' Where's the Off Switch?, NPR (Mar. 20, 2013), https://www.npr.org/sections/alltechconsidered/2013/03/20/174827589/yes-your-new-car-has-a-black-box-wheres-the-off-switch [https://perma.cc/7FBF-EJKW] (explaining that while EDR data has been used for insurance investigations, lawsuits, and criminal cases, it was originally designed for safety purposes). EDR data is often used to determine and assign tort liability. See Jordan Pearson, How 'Black Boxes' in Autonomous Cars Will Be Used to Blame Humans, Vice (July 20, 2016), https://motherboard.vice.com/en_us/article/xygvj3/black-boxes-in-autonomous-cars-will-blame-humans-self-driving-event-data-recorder [https://perma.cc/84A2-TPYZ] ("While these devices are pitched as a way to improve car and driver safety, they've been increasingly used as evidence in court and by authorities to assign blame in a crash.").

For a brief review of the history of EDRs, see NHTSA Event Data Recorder Overview, supra note 19; see also Jaclyn Trop, A Black Box for Car Crashes, N.Y. Times (July 21, 2013), https://www.nytimes.com/2013/07/22/business/black-boxes-in-cars-a-question-of-privacy.html [https://perma.cc/YB2N-NA6S] ("[EDRs] have long been used by car companies to assess the performance of their vehicles. But data stored in the devices is increasingly being used to identify safety problems in cars and as evidence in traffic accidents and criminal cases."). Manufacturers have been installing EDRs since roughly the 1990s. See id.

27. See infra section I.B.1.

28. EDR data may be requested, it seems, by insurance investigators or private citizens pursuant to a civil proceeding. See 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 [https://perma.cc/572W-YYDF] ("In civil litigation, this data will help to determine the course of events and may help to determine which vehicle was responsible for the collision."); see also Trop, supra note 26. The insurance context is important, to be sure, but the Fourth Amendment has little application in governing the relationship between two private parties.

29. See Nhatthien Q. Nguyen, Traffic Crash Investigation Units, Telemasp Bull., May/June 2009, at 1, 5 fig.6 (on file with the *Columbia Law Review*).

30. See State v. West, 548 S.W.3d 406, 410, 421 (Mo. Ct. App. 2018).

31. People v. Diaz, 153 Cal. Rptr. 3d 90, 96 (Ct. App. 2013) (describing testimony from a member of MAIT noting that it was "standard protocol" to download EDR data as part of MAIT's vehicle inspection process).

EDR data can be used to support a variety of criminal charges.[32] For example, the data can be presented in criminal proceedings to prove criminally negligent operation of a vehicle by establishing the vehicle's speed in the moments prior to the crash.[33] The data can also be used to support more severe charges, such as depraved indifference murder, through data showing that the vehicle operator failed to apply pressure to the brakes in the moments before a crash.[34] Given the severity of these charges, the ability of law enforcement to access EDR data is of grave importance for the prosecution of traffic accidents.[35] However, the ability of police to access this data must be balanced with every individual's right to be free from unreasonable searches or seizures, as guaranteed by the Fourth Amendment.[36]

B. *Applicable Law: Constitutional Frameworks, EDR Statutes, and Traffic Safety Regulation*

1. *Current Fourth Amendment Doctrine.* — The Fourth Amendment offers protection against law enforcement efforts to obtain information when a "search" or "seizure" occurs.[37] Under current doctrine, courts determine whether a search has occurred by using either the *Katz* test or the trespassory test.[38] As a general matter, law enforcement must obtain a

32. See, e.g., Auman v. Commonwealth, No. 1783-13-1, 2014 Va. App. LEXIS 347, at *6 (Va. Ct. App. Oct. 21, 2014) (describing prosecution's use of EDR data to show that the defendant's brakes were not used appropriately in the moments before an accident, pursuant to a charge of vehicular involuntary manslaughter); Dupree v. Commonwealth, No. 0519-09-3, 2010 WL 1752581, at *3 (Va. Ct. App. May 4, 2010) (describing the prosecution's use of EDR data to show that the defendant did not attempt to brake or swerve, pursuant to a charge of aggravated involuntary manslaughter and driving under the influence); Nininger v. Commonwealth, No. 0450-09-3, 2010 WL 1752572, at *3 (Va. Ct. App. May 4, 2010) (same).

33. See, e.g., Commonwealth v. Zimmerman, 873 N.E.2d 1215, 1216–19 (Mass. Ct. App. 2007) ("Convicted of motor vehicle homicide by negligent operation . . . [,] the defendant . . . sought to exclude evidence taken from the vehicle's event data recorder (EDR). That evidence indicated that five seconds before the accident the defendant was traveling at a speed of fifty-eight miles per hour.").

34. See Gail Gottehrer, Connected Discovery: What the Ubiquity of Digital Evidence Means for Lawyers and Litigation, 22 Rich. J.L. & Tech., no. 3, 2016, at 1, 15.

35. Regulation of traffic safety is itself a significant public safety issue: In 2017 alone there were more than 37,000 deaths from car accidents. See U.S. Nat'l Highway Traffic Safety Admin., 2017 Fatal Motor Vehicle Crashes 1 (2018), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812603 [https://perma.cc/4CXL-4J3L].

36. See U.S. Const. amend. IV.

37. See id.

38. See Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (describing the two approaches for determining whether a search or seizure has occurred).

warrant prior to conducting a search or seizure,[39] although there are many exceptions under which warrantless searches are permitted.[40]

The *Katz* test is a two-part inquiry, dictating that a search occurs when an individual manifests a subjective expectation of privacy *and* society recognizes that expectation of privacy as reasonable.[41] To resolve the first prong, courts rely on the actions of the defendant and the judges' own common sense intuitions.[42] Supreme Court precedent provides three general principles to guide lower courts in addressing the second prong. First, the analysis should be "informed by historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.'"[43] Next, courts should consider that "the Amendment seeks to secure 'the privacies of life' against 'arbitrary power.'"[44] And third, courts should seek "to place obstacles in the way of a too permeating police surveillance."[45] At a less abstract level, the Court

39. See Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971).

40. There are so many exceptions to the warrant requirement that some commentators have wondered whether they have swallowed the warrant requirement entirely. See, e.g., Ronald Jay Allen, William J. Stuntz, Joseph L. Hoffman, Debra A. Livingston, Andrew D. Leipold & Tracey L. Meares, Comprehensive Criminal Procedure 449 (4th ed. 2016) ("Cumulatively, the exceptions may be the rule—and warrants the real exception.").

There are four exceptions in particular that are relevant to EDR searches, namely: the automobile exception, the exception for administrative searches, searches incident to arrest, and the inventory search exception. The automobile exception allows police to search a car, and any containers within it, when they have probable cause to believe that contraband or evidence of a crime is present. California v. Acevedo, 500 U.S. 565, 580 (1991). The administrative search doctrine permits warrantless searches when a basic balancing of the government and private citizen's interests deem the search reasonable and the search is governed by reasonable and administrative or legislative standards. See Camara v. Mun. Court of S.F., 387 U.S. 523, 534–39 (1967). The search incident to arrest exception allows police to search a vehicle incident to an arrest without a warrant only when the arrestee is unsecured and the area to be searched is within reach of the arrestee, or it is "reasonable to believe evidence relevant to the crime of the arrest might be found in the vehicle." Arizona v. Gant, 556 U.S. 332, 343 (2009) (quoting Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring in the judgment)). Finally, the inventory-search exception permits warrantless searches of vehicles that are lawfully impounded when the search is conducted as part of standard police inventory procedures. South Dakota v. Opperman, 428 U.S. 364, 372–73 (1976). While this Note focuses narrowly on how best to determine whether a search has occurred at all, the breadth of exceptions to the warrant requirement that descends when a search has occurred could significantly limit the effectiveness of the Fourth Amendment in preventing government access to EDR data.

41. Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

42. See, e.g., United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (holding that the defendant exhibited a subjective expectation of privacy in his emails given the "sensitive and sometimes damning substance" of the emails, and considering "people seldom unfurl their dirty laundry in plain view").

43. *Carpenter*, 138 S. Ct. at 2214 (alteration in original) (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

44. Id. (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

45. Id. (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)). The Court seems to derive these principles from a recent emphasis on organizing Fourth Amendment doctrine

has generally held that individuals do not have a reasonable expectation of privacy in information that is knowingly exposed to the public.[46] Similarly, under the third-party doctrine, the Court has held that an individual does not have a reasonable expectation of privacy in information voluntarily revealed to a third party.[47] However, recent cases limit the analytical force of this principle. [48] The exact point at which information knowingly exposed to the public or voluntarily conveyed to a third party begins to enjoy a reasonable expectation of privacy is not clear, but it seems that when the information accessed reveals a substantial amount about an individual's "familial, political, professional, religious, and sexual associations" then a court is more likely to find that an individual enjoys a reasonable expectation of privacy.[49]

The trespassory test dictates that government action is a search, for Fourth Amendment purposes, if the government "attempt[s] to find

around the idea that the judiciary should ensure the same level of protection against government interference as existed at the Founding of the United States. See id. at 2213–14; United States v. Jones, 565 U.S. 400, 406 (2012) ("At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (alteration in original) (quoting *Kyllo*, 533 U.S. at 34)).

46. See, e.g., United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding that the defendant did not enjoy a reasonable expectation of privacy in his car's movements on public roadways). The rationale for this principle draws on a concept borrowed from tort law: Individuals should not receive Fourth Amendment protection for information knowingly exposed to the public because they assumed the risk that the public could obtain such information because of its exposure to the public. *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting); *Knotts*, 460 U.S. at 283 (citing Smith v. Maryland, 442 U.S. 735, 744–45 (1979)). While a 2012 decision by the Court held that use of a beeper attached to a vehicle by law enforcement did require a warrant when the beeper tracked the defendant's movements for twenty-eight days, the Court's opinion explicitly refused to reject the idea that an individual enjoys no reasonable expectation of privacy in their movements on public roads. See *Jones*, 565 U.S. at 412. The Court instead relied on principles of property law, reasoning that attaching the beeper required trespassing onto the defendant's property (the underside of his car), and thus constituted a search as a physical intrusion on a constitutionally protected area. Id. at 404–11.

47. See *Smith*, 442 U.S. at 741–46 (holding that an individual does not have a reasonable expectation of privacy in the numbers dialed on his telephone because he voluntarily conveyed that information to the phone company); United States v. Miller, 425 U.S. 435, 440–44 (1976) (holding that an individual does not have a reasonable expectation of privacy in his bank records because they are voluntarily conveyed to the bank). Both decisions rely on the idea that by conveying the information to a third party, an individual assumes the risk that law enforcement may access that information. See *Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 443.

48. For example, the Court held in *Carpenter* that an individual does enjoy a reasonable expectation of privacy in seven days or more of historical cell-site location information (CSLI), even though that information was held by a third party. See *Carpenter*, 138 S. Ct. at 2217. Of course, where an individual has traveled is, for the most part, necessarily revealed to the public in the course of traveling.

49. See id. (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

something or to obtain information" by physically intruding on a constitutionally protected area.[50] As articulated by Justice Scalia, "[O]btaining by sense-enhancing technology any information . . . that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where . . . the technology in question is not in general public use."[51] However, a physical trespass is not itself sufficient to a finding that a search has occurred; the trespass must occur into a constitutionally protected area.[52] Thus, the trespassory test is not grounded in a strict conception of property rights.[53]

The Court considers the two tests as complementary parts of the Fourth Amendment whole.[54] Justice Scalia wrote that "the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test."[55] Elaborating further on this in the same opinion, Scalia noted that "*Katz* . . . established that 'property rights are not the sole measure of Fourth Amendment violations,' but did not 'snuf[f] out the previously recognized protection for property.'"[56] The basis for the *Katz* holding itself is that a violation of property rights is not necessary for a finding that a search has occurred; meeting the requirements of the *Katz* test is thus sufficient by itself.[57] Justice Scalia's opinion in *United States v. Jones*, decided in 2012, seems to imply that when the requirements of the trespassory test are met, that is itself also sufficient

---

50. See *Jones*, 565 U.S. at 407, 408 n.5.

51. Kyllo v. United States, 533 U.S. 27, 34 (2001) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

52. See *Jones*, 565 U.S. at 410–11 (clarifying that the Fourth Amendment does not apply where there is merely a trespass, but that the trespass must be into a constitutionally protected area). The open-fields doctrine makes this quite clear, as police are not required to obtain a warrant to search areas that are sufficiently decoupled from a property owner's home to be considered an open field, even if they physically trespass by searching such areas. See United States v. Dunn, 480 U.S. 294, 300 (1987).

53. A wave of recent cases have been decided on property law principles. See, e.g., Florida v. Jardines, 569 U.S. 1, 11–12 (2013) (holding that bringing a drug-sniffing dog onto a suspect's porch exceeds the traditional implied license to approach a citizen's door and knock, and therefore constitutes a search); *Jones*, 565 U.S. at 404–11 (holding that installation of a tracking device on the defendant's car was a trespass of the defendant's effects and therefore was a search); *Kyllo*, 533 U.S. at 34 (holding that use of thermal imaging revealed evidence that would have required a physical trespass had the government not used "sense-enhancing technology" and that the use of such technology was therefore a search).

Prior to *Katz*, the Court relied almost exclusively on property law principles to determine whether a search had occurred, as best exemplified by the Court's ruling in Olmstead v. United States, 277 U.S. 438 (1928). In *Olmstead* the Court refused to find that a telephone wiretap constituted a search because "[t]here was no entry of the houses or offices of the defendants." Id. at 464. The trespassory test's resurgence is thus a revitalization of earlier Fourth Amendment doctrine.

54. See *Jones*, 565 U.S. at 409.

55. Id.

56. Id. at 407 (alteration in original) (quoting Soldal v. Cook County, 506 U.S. 56, 64 (1992)).

57. See United States v. Katz, 389 U.S. 347, 359 (1967).

for finding that a search occurred.[58] The Court has avoided addressing a situation where the defendant has no reasonable expectation of privacy but the trespassory test has been violated by simply refusing to perform the reasonable expectations analysis in cases that might set up such a conflict.[59] The two tests thus appear to be individually sufficient means for finding that a search occurred.

2. Carpenter *and Gorsuch's Strict Property Test.* — Responding to increased dissatisfaction with the Court's Fourth Amendment jurisprudence, Justice Gorsuch recently proposed a new approach for what constitutes a search.[60] Gorsuch outlined his proposal in *Carpenter v. United States*.[61] In *Carpenter*, the defendant asserted that: (i) a government subpoena of his historical cell-site location information (CSLI), which was held by his cell phone provider, should be considered a search; and (ii) because obtaining the CSLI should be considered a search, the government should have obtained a search warrant prior to accessing the data.[62] CSLI provides data points on a subscriber's location by cataloging the cell towers that a subscriber's phone connects to.[63] The majority opinion sided with the defendant, holding that an individual enjoys a reasonable expectation of privacy in greater than seven days of CSLI because of how much a comprehensive database of one's location can reveal about a person.[64] Finding the majority's opinion lacking, Gorsuch penned a dissent in which he proposed abolishing the *Katz* test entirely and replacing it with a test focused exclusively on property rights.[65] Essentially, Gorsuch's model dictates that an individual should enjoy Fourth Amendment protection only when the government seeks to access their *property*.[66]

Gorsuch identified five key elements to provide additional structure to the broader idea he articulated. First, third-party access to, or possession of, one's papers and effects should not necessarily eliminate one's property interest in such items.[67] The second and third elements provide

58. See *Jones*, 565 U.S. at 404–11. In response to the government's argument that the defendant in the case had no reasonable expectation of privacy and therefore no search had occurred, Scalia wrote, "[W]e need not address the Government's contentions, because Jones's [(the defendant's)] Fourth Amendment rights do not rise or fall with the *Katz* formulation." Id. at 406.

59. See id. at 406.

60. See Carpenter v. United States, 138 S. Ct. 2206, 2261–72 (2018) (Gorsuch, J., dissenting).

61. Id.

62. See id. at 2213 (majority opinion).

63. See id. at 2211–12.

64. See id. at 2216–19. The Court's opinion also noted the ubiquity of cell phone use in modern life, seemingly concluding that because CSLI collection is an unavoidable part of modern life it should be protected by the Fourth Amendment. See id.

65. Id. at 2261–72 (Gorsuch, J., dissenting).

66. See id. at 2267–68.

67. Id. at 2268. This tenet takes aim at the third-party doctrine, which dictates that information that is knowingly revealed to a third party does not receive Fourth Amendment

greater detail on what would be considered sufficiently one's property to receive Fourth Amendment protection. More specifically, the second element dictates that *complete* ownership of the property in question would not always be a necessary condition for finding that access to the property constitutes a search.[68] The third element identifies where judges employing Justice Gorsuch's model would look to identify what property rights an individual might have in a particular item, place, or piece of data: namely, state law, federal law, or state common law judgments.[69] Therefore, a law passed by the state of California that said individuals own all of the information they post on Facebook would in turn mean that California citizens would receive Fourth Amendment protection for such information.[70]

The final two elements identified by Justice Gorsuch delineate a rough limit on the power of legislation to set the extent of Fourth Amendment protection. First, Justice Gorsuch notes that "while positive law may help establish a person's Fourth Amendment interest[,] there may be some circumstances where positive law cannot be used to defeat it."[71] This statement implies that there is a floor level of protection created by the Fourth Amendment that cannot be circumvented by a state law granting law enforcement access. As Justice Gorsuch writes, "Legislatures cannot pass laws declaring your house or papers to be your property except to the

---

protection. See supra note 47. Thus, if adopted, Gorsuch's proposal would limit the extent of third-party doctrine by permitting individuals to receive Fourth Amendment protection for some information revealed to third parties.

68. *Carpenter*, 138 S. Ct. at 2269–70 (Gorsuch, J., dissenting). For example, "Where houses are concerned, . . . individuals can enjoy Fourth Amendment protection without fee simple title." Id. at 2269. Indeed, as Justice Gorsuch elaborates, a renter could still receive Fourth Amendment protection in their apartment under his approach. See id. The exact limit of this element of the model is not clear, though; Justice Gorsuch does not specify where the line between a sufficient and insufficient property interest falls.

This aspect of Gorsuch's model also demonstrates the greater importance that property law would acquire in a world governed by his proposal. Fee simple seems like a relatively arcane aspect of property law; asking criminal justice advocates to master the difference between fee simple and a fee simple determinable, and to subsequently parse the potential difference in Fourth Amendment protection, would likely be a significant undertaking.

69. Id. at 2270. As Justice Gorsuch notes, relying on state law property rights to determine the extent of the government's power echoes the recent approach to determining whether a taking has occurred in a Takings Clause analysis. Id. at 2270.

70. This is not to suggest that such a law would even be possible, but merely to provide an example for illustrative purposes. With that said, California has recently passed a data privacy bill that appears to grant significant rights to users in controlling their personal information. See California Consumer Privacy Act, Cal. Civ. Code § 1798.198(a) (2018). For an analysis of the potential impact of this Act, see Kristen J. Matthews & Courtney M. Bowman, The California Consumer Privacy Act of 2018, Proskauer: Privacy Law Blog (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018 [https://perma.cc/MJ99-P7JH]. See generally Sullivan & Cromwell LLP, California Consumer Privacy Act of 2018 (2018), https://www.sullcrom.com/files/upload/SC-Publication-New-Statute-Introduces-Privacy-Protections-for-California-Consumers-and-Subjects-Businesses-to-Potential-Liability.pdf [https://perma.cc/Y4ZN-QL3D].

71. *Carpenter*, 138 S. Ct. at 2270 (Gorsuch, J., dissenting).

extent the police wish to search them without cause."[72] For him, the floor level of protection stems from the level of protection against government intrusion that existed at the time the Fourth Amendment was adopted.[73] The fifth and final element Justice Gorsuch describes elaborates that this floor may bar efforts to circumvent Fourth Amendment protection through the use of a subpoena.[74]

3. *Federal Regulation of EDR Data.* — The strict property test proposed by Justice Gorsuch relies heavily on statutorily created property rights.[75] Similarly, as an (albeit indirect) expression of public opinion, the acts of the legislature and administrative agencies are a factor that courts consider when asked whether a reasonable expectation of privacy exists.[76] There are two sources of federal regulation of EDRs: the Driver Privacy Act of 2015 (DPA)[77] and regulations promulgated by the National Highway Traffic Safety Administration (NHSTA).[78]

---

72. Id. at 2270–71.

73. As Justice Gorsuch writes, the Fourth Amendment must, at a minimum, "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." Id. at 2271 (alteration in original) (internal quotation marks omitted) (quoting United States v. Jones, 565 U.S. 400, 406 (2012)).

74. Id. at 2271.

75. The positive law theory relies on what property rights nonconstitutional sources of law create. See id. at 2270 (noting that both state and federal law can create rights in intangible things, which can in turn be used to guide Fourth Amendment decisions for "evolving technologies").

76. The Supreme Court routinely uses the existence, or lack thereof, of federal regulation protecting the use of particular information as a proxy for whether society is prepared to recognize a particular expectation of privacy as reasonable. See, e.g., New York v. Class, 475 U.S. 106, 113–14 (1986) (reasoning that regulation requiring one's vehicle identification number (VIN) to be displayed in a location observable by someone outside the vehicle reduced an individual's expectation of privacy in the VIN). Although it is beyond the scope of this Note to analyze the exceptions to the warrant requirement that might be applicable, a search often does not require a warrant if it is executed as part of a broader civil regulatory scheme. As first articulated in *Camara v. Municipal Court of San Francisco*, the special needs doctrine permits judges to evaluate searches conducted by administrative agents as part of a broader regulatory or administrative scheme using a standard reasonableness framework. 387 U.S. 523, 534–39 (1967). A warrantless search justified under this authority must also be governed by reasonable administrative or legislative standards. See id. at 538. As this section details, there is a significant regulatory scheme surrounding EDRs and investigation of car accidents in general. It might well be possible to justify access to EDR data without a warrant even if downloading the data is determined to be a search.

In the context of vehicle and traffic safety regulation, the most significant application of *Camara* and the style of analysis it pioneered is *Delaware v. Prouse*. 440 U.S. 648 (1979). In *Prouse*, the Court held that discretionary spot checks of drivers' licenses and registrations could not be justified under the special needs doctrine of *Camara*. Id. at 663. Significantly for the issue of EDR data, the Court acknowledged that "the States have a vital interest in ensuring that only those qualified to do so are permitted to operate motor vehicles, that these vehicles are fit for safe operation, and hence that licensing, registration, and vehicle inspection requirements are being observed." Id. at 658.

77. 49 U.S.C. § 30101 note (Supp. III 2016) (Driver Privacy Act of 2015).

78. 49 C.F.R. § 563 (2019).

The DPA stipulates that any data "retained by an event data recorder . . . is the property of the [motor vehicle] owner, or, in the case of a leased vehicle, the lessee."[79] The statute also imposes restrictions on access to data "recorded or transmitted" by an EDR; it generally prohibits persons other than the owner or lessee of the relevant vehicle from accessing the data without authorization from a "court or other judicial or administrative authority having jurisdiction."[80] The DPA does not, however, require that manufacturers install EDRs in their cars.[81]

Federal regulations, issued by NHSTA, also do not mandate that manufacturers include EDRs in their new cars.[82] However, manufacturers must follow certain guidelines if they elect to install EDRs in their vehicles.[83] More specifically, if installed, EDRs must record fifteen identified data elements.[84] The data elements broadly provide a snapshot of a vehicle's essential mechanical functioning, its speed, and its direction.[85] Manufacturers must also: (i) disclose in the vehicle manual that an EDR is installed in the vehicle, (ii) provide a description of the information recorded by the EDR, and (iii) warn the vehicle owner or operator that law enforcement may access the data.[86]

4. *State Regulation.* — State-level regulation is important for Fourth Amendment analysis for the same reasons that federal regulation is

---

79. 49 U.S.C. § 30101 note (Driver Privacy Act of 2015). The definition of the event data recorder is as specified in section 563.5 of title 49 of the Code of Federal Regulations. Id. Section 563.5 defines an event data recorder as "a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event . . . or during a crash event . . . intended for retrieval after the crash event . . . . [T]he event data do not include audio and video data." 49 C.F.R. § 563.5(b).

80. See 49 U.S.C. § 30101 note (Driver Privacy Act of 2015). The statute also permits access in a number of scenarios that are less directly relevant to the focus of this Note. More specifically, retrieval of EDR data is permitted if the owner or lessee has provided consent to such access, if the access is "for the purpose of determining the need for, or facilitating, emergency medical response in response to a motor vehicle crash," or if the data is provided for "traffic safety research" (provided that it is anonymized). Id.

81. NHSTA in fact contemplated a proposal to require EDRs to be installed in all new vehicles. See Jim Motavalli, Safety Agency Proposing Mandatory Event Data Recorders, N.Y. Times: Wheels (Dec. 7, 2012), https://wheels.blogs.nytimes.com/2012/12/07/safety-agency-proposing-mandatory-event-data-recorders (on file with the *Columbia Law Review*); Rafter, supra note 4. The agency ultimately abandoned the proposal; the current federal regulations do not mention any requirement that EDRs be included in new vehicles. See 49 C.F.R. § 563.

82. See 49 C.F.R. § 563 (including no requirement that EDRs be installed in new vehicles).

83. See id. The overwhelming majority of new cars do in fact have EDRs installed. As of 2014, ninety-six percent of all new cars had EDRs. See Rafter, supra note 4.

84. See 49 C.F.R. § 563.7.

85. See id.

86. See 49 C.F.R. § 563.11. The regulation actually spells out the exact language that must be included in the owner's manual. Id.

relevant. As of November 18, 2019, seventeen states had enacted legislation specifically governing the ownership and acquisition of EDR data.[87] Of the states considered explicitly in this Note, two have statutes that regulate EDR data: California and New York.[88]

California's statute largely mirrors the provisions of the federal DPA.[89] Most importantly, the statute dictates that data largely cannot be retrieved from an EDR by anyone other than the registered owner of the motor vehicle in which the EDR is installed unless the owner consents or the data is retrieved "[i]n response to an order of a court having jurisdiction to issue the order."[90] The New York statute is essentially the same as the California statute; the only substantive difference is that the New York statute defines "owner" broadly whereas the California equivalent applies only to "registered owner[s]."[91] None of the other three states examined

87. Privacy of Data from Event Data Recorders: State Statutes, Nat'l Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx [https://perma.cc/5263-BJDN] [hereinafter State Statute EDR Guide] (last updated Nov. 18, 2019). State constitutional provisions can also serve to impose limits on law enforcement authority to obtain EDR data. The interaction between state and federal constitutional standards is an important area of law. However, this topic is too complex to address in this Note. Indeed, it is itself the subject of a distinct line of scholarship. See generally Mark Silverstein, Privacy Rights in State Constitutions: Models for Illinois?, 1989 U. Ill. L. Rev. 215 (framing the approach to state constitutional privacy provisions in relation to federal constitutional privacy protections in three general categories, and describing those categories with reference to a variety of specific states).

88. See Cal. Veh. Code § 9951 (2020); N.Y. Veh. & Traf. Law § 416-b (McKinney 2018). California's constitution also includes an explicit protection for the right of privacy, although this does not on its face seem to have any impact on the extent of property protections recognized for electronic data. See Ca. Const. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

89. There are a few differences in the California statute that are worth mentioning, though they are not central to the analytical thrust of this Note. First, the statute applies to "recording devices commonly referred to as 'event data recorders (EDR)' or 'sensing diagnostic modules (SDM).'" Cal. Veh. Code § 9951(a). Recording devices are in turn broadly defined as devices installed by the manufacturer that perform one of several functions "for the purposes of retrieving data after an accident." Id. at § 9951(b). One of the functions specified is recording the history of where the vehicle has traveled. Id. at § 9951(b)(2). A broad interpretation of this statute could reasonably sweep in onboard GPS navigation devices in modern automobiles.

90. Id. at § 9951(c). There are two exceptions to this statement. First, the data can also be shared "for the purpose of improving motor vehicle safety." Id. at § 9951(c)(3). When data is shared pursuant to that purpose, it must be anonymized, although in contrast to the federal statute, disclosure of the owner's VIN does not constitute identifying information. Compare 49 U.S.C. § 30101 note (Supp. III 2016) (Driver Privacy Act of 2015), with Cal. Veh. Code § 9951(c)(3). Second, "[A] licensed new motor vehicle dealer . . . or an automotive technician" may also retrieve this data "for the purpose of diagnosing, servicing, or repairing the motor vehicle." Cal. Veh. Code § 9951(c)(4).

91. See Cal. Veh. Code § 9951; N.Y. Veh. & Traf. Law § 416-b.

in this Note (Florida, Missouri, and Georgia) have a statute specifically regulating EDR data.[92]

As EDRs are a component of nearly all modern vehicles, state statutes generally regulating vehicle safety and traffic accident investigation can also play a role in determining what expectations of privacy are reasonable and what property rights may exist in EDR data. Such laws in Georgia, Missouri, California, and Florida all empower law enforcement to investigate traffic accidents but do not seem to impose *affirmative* duties for them to do so.[93] Only California law specifically allows the police to inspect vehicle equipment.[94] The Missouri State Highway Patrol is empowered to investigate any crime,[95] enforce traffic laws,[96] and promote highway safety.[97] But Missouri law does not appear to specifically require the investigation of traffic accidents.[98] New York is an exception to this pattern. Police officers are *required* to conduct an investigation of any accident resulting in

92. See State Statute EDR Guide, supra note 87.

93. In Florida, motorists are required to provide basic information to any police officer investigating a car accident but are not required to permit an inspection of their vehicle. See Fla. Stat. § 321.05(1) (2018). Similarly, the Florida Highway Patrol is empowered to "investigate traffic accidents." See id.; see also id. at § 316.062 (requiring motorists to report their name, address, registration number, and present their license). The requirement to provide information is limited to accidents involving the injury of any person or damage to any property. See id. As nearly every car accident would seem to involve at least some minor property damage, this provision seems to apply to virtually every accident. Motorists are required to stop and remain at the scene of any accident until they fulfill the requirements of this section. See id. at § 316.027. Mirroring this requirement, any law enforcement officer in Florida investigating a "motor vehicle crash" must complete a report with roughly the same information as required by § 316.062. See id. at § 316.066.

In Georgia, there are fewer statutory grants of authority to investigate traffic accidents; drivers are required to report certain information for more serious accidents. See Ga. Code Ann. § 40-6-273 (2019). But information they must report is not related to equipment of their vehicle. See id. at § 40-6-273.1. Implicit mention of law enforcement's authority to perform initial accident investigations is included in a statute that prohibits moving a vehicle incapacitated as a result of an accident "until the enforcement officer has made the necessary measurements and diagrams required for the initial accident investigation." See id. at § 40-6-275. All sheriffs or chief executive officers of a law enforcement agency other than a sheriff are also required to report to the commissioner of transportation the "circumstances relating" to any traffic accident resulting in death that occurs within their jurisdiction. See id. at § 40-6-277.

94. See Cal. Veh. Code § 2806 (empowering local law enforcement to perform vehicle equipment investigations). The California Highway Patrol (CHP) is authorized to inspect vehicle equipment in order to "investigate accidents resulting in personal injuries or death and gather evidence for the purpose of prosecuting the person or persons guilty of any violation of the law contributing to the happening of such accident." Id. at § 2412. The CHP is also authorized to inspect vehicle equipment when an officer has a "reasonable belief that any vehicle is being operated in violation of any provisions of [the Vehicle Code] or is in such unsafe condition as to endanger any person." Id. at § 2804.

95. Mo. Ann. Stat. § 43.180 (West 2019).

96. See id. at § 43.025.

97. See id.

98. The Missouri statute specifying the duties of the Missouri State Highway Patrol does not make any mention of traffic accident investigation. See id. at § 43.160.

"serious physical injury or death to a person."[99] When conducting such an investigation, officers are required to determine "the facts and circumstances of the accident; . . . the contributing factor or factors; . . . and, the cause of such accident, where such cause can be determined."[100] In many instances, EDR data can provide valuable information on the causes of an accident.[101] Reconciling such affirmative duties with Fourth Amendment limits is a challenge that courts must confront.

II. STATE COURT SPLIT, UNIFORMITY, AND THE DIFFICULTY OF THE REASONABLE EXPECTATIONS TEST

In the context of this patchwork of federal and state regulation, five state court systems (yielding six appellate court opinions) have addressed the issue of whether law enforcement downloads of EDR data constitute a Fourth Amendment search.[102] Two courts determined that such downloads are not searches, and four came to the opposite conclusion.[103] Section II.A summarizes the facts and holdings of each case. Section II.B examines the rationales that the courts relied upon to reach their respective decisions. Finally, section II.C introduces three issues with current Fourth Amendment doctrine that this disagreement among state courts on the issue of EDR data highlights.

A. *Case Summaries*

In 2004, a New York court addressed the Fourth Amendment implications of accessing EDR data.[104] In *People v. Christmann*, the defendant was charged with speeding and failure to exercise due care when his vehicle struck and killed a pedestrian.[105] Upon arriving at the scene of the accident, a New York state trooper downloaded EDR data from the defendant's vehicle.[106] The trooper did not have a warrant, nor did he seek or receive consent from the defendant to download the data.[107] The evidence obtained from the EDR was used at trial to establish that the defendant's vehicle had been traveling thirty-eight miles per hour in the second before impact.[108] The speed limit in the area of the collision was thirty miles per hour.[109] The defendant moved to suppress the EDR data on Fourth

99. N.Y. Veh. & Traf. Law § 603-a(1) (McKinney 2019).
100. Id. at § 603-a(1)(a).
101. See supra notes 32–34.
102. See supra note 6 and accompanying text.
103. See supra notes 12–13 and accompanying text.
104. See People v. Christmann, 776 N.Y.S.2d 437 (Justice Ct. 2004).
105. Id. at 438.
106. Id.
107. Id.
108. Id. at 438–40.
109. Id. at 442.

Amendment grounds.[110] The court's opinion does not engage directly with the question of whether or not there was a search; the discussion proceeds immediately to considering exceptions to the general warrant requirement.[111] It therefore seems that the court assumed that downloading the EDR data was a search, although there is no rationale given for why the court arrived at that conclusion.[112] Relying on a combination of a general reasonableness inquiry and an exigency rationale, the court ultimately found "that the immediate download of information from the Defendant's [EDR] is permitted and required by [Vehicle and Traffic Law] Sections 603-a and is not violative of Defendant's rights to be free from unreasonable searches pursuant to the United States or New York Constitution."[113]

A California court was the next to consider the issue, and arrived at a similar conclusion.[114] The case, *People v. Diaz*, stemmed from a fatal car crash: Driving home from a bar, the defendant's vehicle struck a second car, killing that car's driver.[115] The first officer to arrive on the scene conducted field sobriety tests and found indications that the defendant was intoxicated.[116] Following these tests, the defendant's vehicle was impounded for evidence and brought to a towing company's secure lot.[117] A member of California Highway Patrol's Multidisciplinary Accident Investigative Team supervised an inspection of the vehicle at the lot; data from the vehicle's EDR was downloaded during this inspection.[118] The data obtained from the EDR was used to establish the speed of the defendant's vehicle in the moments before impact, which was in turn used to support charges of involuntary manslaughter and vehicular manslaughter while intoxicated.[119] The defendant moved to suppress the EDR data on Fourth Amendment grounds.[120] The court's response to the motion is confusing. There is first an extended discussion of the diminished expectations of privacy that individuals enjoy in automobiles.[121] After the discussion, the court concludes that "the vehicle is protected by the Fourth Amendment, and an individual's reasonable expectation of privacy as to the vehicle yields only as to places where there is probable cause to search. The scope

110. Id. at 440–41.

111. See id. at 441–42.

112. See id.

113. Id.

114. See People v. Diaz, 153 Cal. Rptr. 3d 90, 101–02 (Ct. App. 2013).

115. Id. at 92–94.

116. See id. at 93.

117. See id.

118. See id. at 93–94. The defendant conceded that her vehicle was "'essentially totaled and was lawfully in police possession' when MAIT investigators downloaded data from the [EDR]." Id. at 96.

119. See id. at 93–95.

120. See id. at 95.

121. See id. at 98–99.

of the search did not exceed probable cause."[122] The language here appears to imply that the court considered the download of the EDR data to be a search. However, later in the opinion, in a section titled "Expectation of Privacy," the court seemingly concludes that the defendant had no subjective expectation of privacy in the EDR data itself, meaning that no search would have occurred.[123] Here is the court's language:

> [T]he specific data obtained from the [EDR] was the vehicle's speed and braking immediately before impact. We agree that a person has no reasonable expectation of privacy in speed on a public highway because speed may readily be observed and measured . . . . Similarly, a person has no reasonable expectation of privacy in use of a vehicle's brakes because statutorily required brake lights . . . announce that use to the public. Thus, defendant has not demonstrated that she had a subjective expectation of privacy in the [EDR's] recorded data because she was driving on the public roadway, and others could observe her vehicle's movements, braking, speed, either directly or through the use of technology . . . . We conclude there was no Fourth Amendment violation in the admission of the [EDR] evidence.[124]

Although this language seems to conflict with the earlier portion of the opinion, the court clearly states its conclusion that the defendant had no subjective expectation of privacy in the EDR data. As this means the first prong of the *Katz* test is not met,[125] the court therefore seems to have decided that downloading the EDR data was not a search.

An appellate court in Florida was the next court to address the EDR issue, and concluded that accessing EDR data constitutes a search.[126] The case, *State v. Worsham*, featured a defendant whose passenger was killed after a high-speed accident.[127] Following the accident, the defendant's vehicle was impounded.[128] Twelve days after the crash, and without obtaining a warrant, "law enforcement downloaded the information retained on the vehicle's [EDR]."[129] The defendant moved to suppress the information obtained from the EDR, arguing that accessing the data was a search and that accessing it without a warrant or his consent therefore violated his Fourth Amendment rights.[130] In response, "[t]he state defended the search on

122. Id. at 99.

123. See id. at 101–02.

124. Id.

125. For a description of the first prong of the *Katz* test, see supra notes 41–42 and accompanying text.

126. See State v. Worsham, 227 So. 3d 602, 608 (Fla. Dist. Ct. App. 2017). *Worsham* is the first case of the relevant results from a Westlaw search conducted to determine the existence EDR-related cases to reach such a conclusion. For a description of the Westlaw search conducted, see supra note 6.

127. *Worsham*, 227 So. 3d at 603.

128. Id.

129. Id.

130. See id.

the sole ground that Worsham had no privacy interest in the downloaded information, so no Fourth Amendment search occurred."[131] The court sided with the defendant, holding that a search occurred and that a warrant was required, so the EDR evidence had to be suppressed.[132]

In finding that a search occurred, the court relied on four separate reasons. First, the court noted that the Driver Privacy Act of 2015 (DPA) enhanced the notion that a driver enjoys a reasonable expectation of privacy in EDR data due to the protections that the statute provides.[133] Second, the court dismissed the persuasive effect of *Diaz* because "[i]t relied on *Smith v. Maryland*, which found no expectation of privacy in information 'voluntarily conveyed' to a third party" and "when addressing digital devices, the Supreme Court has moved away from the *Smith* rationale."[134] Third, the court noted the "constant, unrelenting black box surveillance of driving conditions" conducted by EDRs.[135] Finally, the court noted, "[C]onsidering that the data is difficult to access and not all of the recorded information is exposed to the public, Worsham had a reasonable expectation of privacy."[136]

In line with the *Worsham* court, roughly a year later a Missouri court of appeals also concluded that downloading EDR data constitutes a search.[137] In *State v. West*, the defendant was charged with involuntary manslaughter after the semitruck he was driving, which was owned by his employer, hit a pickup truck and the truck driver died.[138] A member of the Missouri State Highway Patrol (MSHP) downloaded information from the vehicle's EDR at the scene of the accident.[139] The defendant moved to suppress the EDR data, arguing that downloading the information was a Fourth Amendment search and, having been conducted without a warrant, should therefore be excluded from evidence during the trial.[140] The state responded to the

131. Id.

132. See id. at 608. The court's statement of its holding does not explicitly state that the EDR evidence should be suppressed, but the ruling affirmed a lower court decision in favor of the defendant's motion to suppress. See id. at 603. Thus, the court's decision effectively concluded that the EDR data had to be suppressed.

133. See id. at 607. For a discussion of the DPA, and the protections it provides, see supra section I.B.3.

134. See *Worsham*, 227 So. 3d at 607. The court based its ruling on the Supreme Court's ruling in United States v. Jones, 565 U.S. 400 (2012), and the fact that the Court relied on the trespass test rather than the fact that information (the vehicle's position) had been voluntarily conveyed to the public. See *Worsham*, 227 So. 3d at 607. For a description of *Smith* and *Miller*, see supra note 47 and accompanying text.

135. See *Worsham*, 227 So. 3d at 608.

136. Id. For a discussion of the methods through which EDR data can be accessed, and the training required to execute such methods, see supra notes 24–25 and accompanying text.

137. See State v. West, 548 S.W.3d 406, 414–18 (Mo. Ct. App. 2018).

138. Id. at 409.

139. Id. at 410. A MSHP officer testified that "it was 'standard practice' to download ECM data without a warrant" at the time of the accident (July 2015). Id.

140. See id. at 409–10.

motion by arguing that the defendant did not have a reasonable expectation of privacy in the data collected by the EDR, and therefore did not have standing to challenge downloading of the EDR data.[141] Fourth Amendment standing is a different doctrinal question than whether or not there was a search, but the two are resolved by the same inquiry: Did the defendant have a reasonable expectation of privacy in the information searched?[142] The court's analysis reflects this, as the opinion examines whether the defendant has standing by addressing the *Katz* test and then the trespassory test.[143] Recognizing difficulty in applying the *Katz* test, the court held that the defendant had standing because the MSHP officer entered the semitruck to download the EDR data, and thus physically intruded into a constitutionally protected area.[144]

In the final case, *Mobley I*, the defendant's vehicle collided with a second car, killing both passengers of the second vehicle.[145] The state charged the defendant with reckless driving, homicide by vehicle, and speeding.[146] The prosecution relied upon evidence obtained from the EDR in the defendant's vehicle to establish that he was traveling at ninety-seven miles per hour five seconds before the collision.[147] The police downloaded the relevant data at the scene of the collision without obtaining a warrant.[148] At trial, the defendant moved to suppress the information obtained from the EDR on the grounds that the police had violated the Fourth Amendment by accessing the EDR data without a warrant.[149] Expressly rejecting the defendant's attempts to invoke the holding in *Worsham*, the court found "that Mobley [(the defendant)] did not have a reasonable expectation of privacy with respect to the data captured by his vehicle's [EDR], and the retrieval of the data was therefore not a search or seizure protected by the Fourth Amendment."[150] The Georgia Supreme Court subsequently reversed the appellate court's decision.[151] Relying on the fact that an investigator physically intruded into the defendant's motor vehicle to retrieve the EDR data, the court held that a search had occurred.[152]

---

141. Id. at 411–12.

142. See Rakas v. Illinois, 439 U.S. 128, 148–49 (1978).

143. See *West*, 548 S.W.3d at 417–18.

144. See id. This is an application of the trespassory test; for a description of that test, see supra notes 50–53 and accompanying text.

145. See *Mobley I*, 816 S.E.2d 769, 770 (Ga. Ct. App. 2018).

146. Id.

147. Id.

148. Id. at 772.

149. Id. at 770–71.

150. Id. at 774.

151. *Mobley II*, 834 S.E.2d 785, 791–92 (Ga. 2019).

152. Id. at 792.

B. *Competing Fourth Amendment Justifications and Different Reasonable Expectations*

There is a notable divergence in analysis among the six opinions on the threshold question in any Fourth Amendment case: Was there a search in the first place?[153] The courts are not consistent on whether the trespassory test or the *Katz* test is appropriate to provide an answer, nor are they consistent even when they apply the same test.

There was not even a consensus in answering the first prong of the *Katz* test: whether the defendant had exhibited a subjective expectation of privacy.[154] The *Diaz* court concluded that the defendant had neither a subjective nor reasonable expectation of privacy because "she was driving on the public roadway, and others could observe her vehicle's movement, braking, and speed . . . . [T]echnology merely captured information defendant knowingly exposed to the public . . . ."[155] The majority in both *Worsham* and *Mobley I* ignored entirely the first prong of the *Katz* test, moving straight to the second prong of *Katz*.[156] The dissenting judge in *Worsham* seized on this oversight, observing that it was incorrect to find that the defendant satisfied the first prong of the *Katz* test because "it is likely that [the defendant] did not even know the vehicle he was driving had an EDR. Therefore, it would be quite a stretch to conclude that [the defendant] sought to preserve [the EDR] information as 'private.'"[157]

There is a similar lack of consensus on the second prong of the *Katz* test: Is an expectation of privacy in EDRs an expectation society is prepared to recognize as reasonable? The *Mobley I* court relied on the same reasoning as the judge in *Diaz*: "There is no reasonable expectation of privacy in such information [referring to EDR data] because an individual knowingly exposes such information to the public."[158] In contrast, the *Worsham* majority concluded that the defendant did have a reasonable expectation of privacy in the EDR data "[b]ecause the recorded data is not exposed to the public, and because the stored data is so difficult to extract and interpret."[159] Remarkably, the courts seem to disagree on basic factual underpinnings, perhaps due to the unique nature of EDR data. As the

---

153. See supra notes 37–38 and accompanying text.

154. For a description of the first prong of the *Katz* test, see supra notes 41–42 and accompanying text.

155. People v. Diaz, 153 Cal. Rptr. 3d 90, 102 (Ct. App. 2013).

156. See State v. Worsham, 227 So. 3d 602, 604–06 (Fla. Dist. App. 2017); *Mobley I*, 816 S.E.2d 769, 773–74 (Ga. Ct. App. 2018).

157. *Worsham*, 227 So. 3d at 609 (Forst, J., dissenting).

158. 816 S.E.2d at 774. In a fascinating twist, immediately following this passage, and in support of its proposition, the opinion cites to a case that upheld "warrantless monitoring of defendant's cell phone location . . . because it revealed the same information that could be obtained through visual surveillance." Id. (citing Devega v. State, 689 S.E.2d 293 (Ga. 2010)). Of course, *Carpenter*, handed down five days *before* the opinion in *Mobley I*, essentially directly rejected this idea. See Carpenter v. United States, 138 S. Ct. 2206, 2217–20 (2018).

159. *Worsham*, 227 So. 3d at 606.

Mobley I court noted, technically an individual does expose information on braking, the speed of a vehicle, the angular momentum, and whether they are wearing a seatbelt (these are all variables recorded by EDRs), to the public: An observer on the sidewalk could obviously see all of this information.[160] The *Worsham* court instead sought to characterize the information recorded by the EDR as different from merely examining external aspects of the car, such as tires; this move allowed it to conclude that EDR data is not exposed to the public.[161]

Four courts have addressed whether the trespassory test indicated that a search had occurred. The *Diaz* court dismissed the trespass theory because no device had been installed to obtain information from a constitutionally protected area.[162] The *West* majority concluded that by physically intruding in the defendant's vehicle, as is necessary to download EDR data even if the device is not physically removed, the officer clearly trespassed and thus triggered Fourth Amendment protection for the defendant.[163] The concurrence in *Mobley I* relied on similar rationale in arguing that a search occurred when the law enforcement officer accessed EDR data,[164] and the *Mobley II* court found a clear violation of the trespassory test (thereby making application of the *Katz* test unnecessary).[165]

In contrast, the New York state court did not substantively engage with the question of whether a search occurred, seemingly assuming that one did. Rather, the court's analysis focused largely on a doctrine that permits warrantless searches.[166] After reviewing the potential exceptions to the general warrant requirement, the court concluded "that the immediate download of information from the Defendant's [EDR] is permitted *and required* by [Vehicle and Traffic Law] Sections 603-a and is not violative of Defendant's rights to be free from unreasonable searches pursuant to the United States or New York Constitution."[167] Section 603-a requires an officer that discovers an accident that involves a serious physical injury or death to investigate the causes of the accident.[168] The most striking element of this sentence is the implication that Section 603-a not only allows New

160. *Mobley I*, 816 S.E.2d at 774. The *Mobley II* court noted that this aspect of EDR data made the resolution of the *Katz* test a "close question" and did not reach a conclusion on the issue, further highlighting the difficulty of applying the *Katz* test to EDR data retrieval. 834 S.E.2d 785, 792 n.9 (Ga. 2019).

161. *Worsham*, 227 So. 3d at 606.

162. People v. Diaz, 153 Cal. Rptr. 3d 90, 101 (Ct. App. 2013).

163. State v. West, 548 S.W.3d 406, 417–18 (Mo. Ct. App. 2018). The court actually analyzed this as a question of Fourth Amendment standing, but then proceeded to consider exceptions to the warrant requirement without separately reaching the question of whether a search occurred. Id. at 417–21. This highlights the confusing relationship between standing and determining whether there was a search in Fourth Amendment doctrine.

164. See *Mobley I*, 816 S.E.2d at 777 (Dillard, J., concurring).

165. *Mobley II*, 834 S.E.2d at 792.

166. See People v. Christmann, 776 N.Y.S.2d 437, 442–43 (Justice Ct. 2004).

167. Id. (emphasis added).

168. See supra notes 99–100 and accompanying text.

York officers to download EDR data without a warrant, but that it *requires* it. The idea that the legislature could pass a law that, in imposing certain investigate duties on officers, would permit law enforcement to circumvent the Fourth Amendment is a radical notion.

C. *Problems Presented and Potential Paths Forward*

The division in opinions highlights the difficulty in applying Fourth Amendment doctrine during the digital age. Fourth Amendment doctrine, and the *Katz* test in particular, has been extensively attacked by multiple scholars: Classic criticisms focus on the test's "ambiguous meaning, its subjective analysis, its unpredictable application, its unsuitability for judicial administration, and its potential circularity."[169] The cases examined in the previous section emphasize two of these arguments, the subjectivity and unpredictability of the test, while also demonstrating the lack of clarity in current doctrine on the relationship between the *Katz* test and the trespassory test.

The different conclusions reached by the *Mobley I* and *Worsham* courts over whether a reasonable expectation of privacy existed in EDR data lays bare the subjectivity and unpredictability of the second prong of the *Katz* test.[170] As a district court observed in 1999, whether an expectation of privacy is reasonable requires courts to perform open-ended analysis without much guidance:

> The objective reasonableness prong of the privacy test is ultimately a value judgment and a determination of how much privacy we should have as a society. In making this constitutional determination, this court must employ a sort of risk analysis, asking whether the individual affected should have expected the material at issue to remain private.[171]

With that said, when new technology is clearly equivalent to an older tool that courts have previously addressed, determining whether an expectation of privacy is reasonable can be a straightforward exercise.[172] However, this is unlikely to resolve issues related to emerging digital technology, as highlighted by EDR data. Indeed, EDRs record information that was not possible to record prior to modern technology. In such situations, the Supreme Court has suggested that courts look to secure the level of

---

169. See Baude & Stern, supra note 14, at 1825. For additional scholarship on the shortcomings of the *Katz* model, see supra note 15.

170. See supra notes 158–161 and accompanying text.

171. United States v. Hambrick, 55 F. Supp. 2d 504, 506 (W.D. Va. 1999).

172. The best example of this is the Sixth Circuit's ruling in *United States v. Warshak*, in which the court held that an individual enjoys a reasonable expectation of privacy in the contents of their emails by drawing on precedent that imposed Fourth Amendment protection for the contents of an individual's letters. See 631 F.3d 266, 285 (6th Cir. 2010).

protection that existed at the time of the Founding.[173] Yet, neither the *Worsham* nor the *Mobley I* court relied on this framework.[174] For judges not equipped with the time or resources to conduct a fulsome investigation into the relative level of security as existed at the time of the Founding and that which would exist if the information in question was not protected (presumably the vast number of judges at the state level), this originalist approach is perhaps not of much assistance.[175] The principle that information knowingly exposed to the public does not enjoy a reasonable expectation of privacy appears to be one that can be manipulated to reach a court's own value judgment; both the *Worsham* court and the *Mobley I* court relied on this principle to reach opposite conclusions.[176]

The dissent in *Worsham* highlights another looming difficulty for the first prong of the *Katz* test, a difficulty that is already producing unpredictable and subjective results: If an individual does not know that data about them is being recorded, can they exhibit a subjective expectation of privacy?[177] The *West* court appears to have found this question so vexing that it avoided addressing it entirely, relying instead on the trespassory test to reach a decision.[178] At the very least, this seems to be a logical puzzle for the *Katz* approach that is only likely to grow in significance as more of public life is recorded digitally.

The different conclusions reached by the courts can also be seen as an illustration of a more fundamental problem with current Fourth Amendment

---

173. See United States v. Jones, 565 U.S. 400, 406 (2012) ("At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001))).

174. See supra notes 137–150 and accompanying text.

175. Even if state court judges had the time and resources to conduct investigations into Founding era levels of security against government interference, it may still prove a fruitless exercise. As the dissenting judge in *Worsham* aptly observed, "Obviously, searches of EDRs in motor vehicles were not on the minds of the first United States Congress when the Fourth Amendment was introduced in 1789." State v. Worsham, 227 So. 3d 602, 608 (Fla. Dist. App. 2017) (Forst, J., dissenting).

176. See *Worsham*, 227 So. 3d at 606; *Mobley I*, 816 S.E.2d 769, 774 (Ga. Ct. App. 2018). The *Mobley II* court also found it a "close question" whether the defendant had a reasonable expectation of privacy in the EDR data. 834 S.E.2d 785, 792 n.9 (Ga. 2019).

177. See *Worsham*, 227 So. 3d at 609 (Forst, J., dissenting). The prosecution in *West* actually sought to defeat the defendant's Fourth Amendment challenge on standing grounds by relying on this same argument. See State v. West, 548 S.W.3d 406, 414–16 (Mo. Ct. App. 2018). However, the court avoided addressing the issue and decided the standing issue by finding that the law enforcement officer trespassed into the defendant's vehicle to obtain the data and therefore the defendant had standing to raise a Fourth Amendment challenge. See id. This does not seem to be an entirely correct application of precedent, as the trespass theory arose in *Jones* to answer the question of whether a search had occurred, which is a separate question from whether a defendant has standing to bring a Fourth Amendment challenge in the first place. See United States v. Jones, 565 U.S. 400, 412–14 (2012).

178. See *West*, 548 S.W.3d at 414–16 (refusing to decide the issue of whether a "non-owner driver's expectation of privacy with respect to a vehicle generally extends to include an [EDR] housed within that vehicle whose data the driver cannot access").

doctrine: It is not clear for lower courts whether they should be applying the *Katz* test, the trespassory test, or both. Strikingly, neither the *Mobley I* court nor the *Worsham* court relied on the trespassory test.[179] Indeed, it would have not only been appropriate, but seemingly offers a straightforward answer to the EDR question, as a concurring judge in *Mobley I* and the court opinion in *Mobley II* noted.[180] The configuration of EDRs is such that it is essentially impossible to access the devices without physically intruding into the vehicle.[181] It is well established that cars are a constitutionally protected area.[182] The requirements of the *Jones* test thus seem to offer a more concrete analytical framework. And yet, neither court relied on it.[183] This reflects the difficulty of applying the current regime with its two tests, as judges, short on time, are not clear which test is to be applied and when. The *Mobley II* court explicitly highlighted the apparent confusion on this doctrinal point, noting that the state had previously advanced an argument "premised on the misguided notion that 'reasonable expectations of privacy' have supplanted private rights under the common law as the sole standard by which we determine whether a government act amounts to a search."[184] Indeed, it may be asking too much of state judges dealing with crowded dockets to parse the intricacies of this doctrine.[185]

The strict property test proposed by Justice Gorsuch is a serious attempt to blaze a new doctrinal path out of these issues. As detailed in section I.B.2, this approach suggests abandoning the *Katz* test in favor of a model that relies exclusively on an individual's property rights as the source for determining what constitutes a search. But such a significant doctrinal shift should only be accepted following rigorous comparative analysis to the existing regime.

---

179. See supra notes 126–136, 145–150 and accompanying text.

180. See *Mobley II*, 834 S.E.2d at 792 ("Although Mobley disputes the idea that he had no reasonable expectation of privacy in the data retrieved from the [EDR] on the Charger, we find it unnecessary to resolve that question."); *Mobley I*, 816 S.E.2d at 777 (Dillard, C.J., concurring specially).

181. See supra note 23 and accompanying text.

182. See *Jones*, 565 U.S. at 404 ("It is beyond dispute that a vehicle is an 'effect' as that term is used in the [Fourth] Amendment.").

183. The *Mobley I* court's refusal to rely on the *Jones* line of doctrine seemingly cannot be explained by the lawyers' failure to raise such an argument; the concurrence of Chief Judge Dillard specifically notes the *Jones* reasoning as an easy method for deciding the case, from which it can reasonably be concluded that the argument was presented by the lawyers for the state. See 816 S.E.2d at 777 (Dillard, C.J., concurring specially).

184. *Mobley II*, 834 S.E.2d at 792.

185. State court judges are likely to have limited resources and time; South Carolina state judges each heard 4,374 nontraffic cases in 2006. See State Court Caseload Statistics, Bureau of Justice Statistics, https://www.bjs.gov/index.cfm?ty=tp&tid=30 [https://perma.cc/4MLQ-8252] (last visited Jan. 30, 2020). These judges likely do not have much time to parse the finer points of Fourth Amendment doctrine.

III. THE PATH FORWARD

This Part applies the strict property test to the question of EDR data as a case study on whether Justice Gorsuch's proposed model avoids the subjectivity, unpredictability, and lack of overall clarity generated by current Fourth Amendment doctrine.[186] Section III.A analyzes whether downloading EDR data constitutes a search under the strict property test put forward by Justice Gorsuch. Following this discussion, section III.B describes the relative strengths and weaknesses of Justice Gorsuch's approach and the existing approach (drawing heavily on the analysis performed in section II.C). Section III.B then presents conclusions on which model offers a better approach to the issue of EDR data and offers a variety of suggestions on how Fourth Amendment doctrine can best evolve to deal with the issues of current doctrine highlighted by this Note, ultimately arguing that minor doctrinal shifts in the prevailing framework are superior to abandoning the *Katz* test entirely.

A. *Applying the Strict Property Test*

The strict property test proposed by Justice Gorsuch dictates that a search occurs when the government seeks to obtain access to something, intangible or tangible, that an individual owns.[187] State law, federal law, and federal regulation are the primary sources for determining the property rights for vehicle operators in intangible information such as EDR data.[188] Fortunately, there is significant legislation on the topic of EDR data at both the federal and state level to guide the analysis.[189]

Federal legislation appears to establish clear property rights in EDR data on the part of vehicle owners or lessees through the DPA, implying that accessing EDR data is a clear search under the strict property test. The relevant statutory text reads: "Any data retained by an event data recorder . . . is the property of the owner, or in the case of a leased vehicle, the lessee of the motor vehicle in which the event data recorder is installed."[190] Notably, the statute does not define "owner" nor "lessee."[191]

---

186. See generally Baude & Stern, supra note 14, where Professors William Baude and James Stern proposed a form of the strict property test as an alternative to *Katz*, advocating that their approach (which they call the positive law model) can solve many of the problems that plague the *Katz* doctrine. In addition to Justice Gorsuch, Justice Thomas also sees a property-based approach as a superior alternative to *Katz*. See Carpenter v. United States, 138 S. Ct. 2206, 2235–46 (2018) (Thomas, J., dissenting). Justice Thomas's qualms with the *Katz* test are heavily rooted in textual and historical arguments. See id. at 2238–41. However, his view is also based on concerns regarding the lack of clarity and predictability that the test offers. See id. at 2244–46.

187. See supra section I.B.2.

188. See supra sections I.B.3–.4.

189. For a review of the federal regulation, see supra section I.B.3. For a review of the state-level regulation, see supra section I.B.4.

190. 49 U.S.C. § 30101 note (Supp. III 2016) (Driver Privacy Act of 2015).

191. See id. at § 30102.

In cases where an individual holds full legal title in a vehicle, this imprecision is not likely to be an issue. However, the ownership of a given vehicle involved in an accident will not always be so clear. An individual could become involved in an accident while driving a vehicle that she jointly owned with her spouse. Would shared ownership be sufficient to qualify her as an "owner" under the statute? It seems unlikely, but without a definition of "owner" in the statute it is hard to say definitively. Federal law seems to establish ownership rights in EDR data, but who exactly receives those rights is unclear. The interaction of state laws on EDR data with the DPA further complicates the analysis.

1. *States with EDR Statutes.* — The strict property test encounters significant difficulty when applied to the two states that have EDR statutes of their own: New York and California.[192] New York's statute, while broadly similar to the DPA, differs somewhat and thus complicates the resolution of Fourth Amendment rights for EDR data under the strict property test.[193] New York's statute prohibits anyone other than the owner from accessing data recorded on an EDR, subject to five exceptions.[194] The language of the statute allows only the owner of the vehicle to restrict access.[195] And, unlike the DPA, the statute does not specify who *owns* the data held in an EDR.[196] Further differing from the DPA, the New York statute also defines owner.[197] The first questions stemming from these divergences is whether the New York definition of "owner" should supplement the DPA (which does not define owner). This question is important because it dictates the extent of the property right and therefore Fourth Amendment protection under the strict property test. The other question is how the lack of a clear property right in the New York statute affects the property rights seemingly granted by the DPA. California has an EDR statute that mirrors the language of the New York statute and thus presents the same thorny issues.[198] Justice Gorsuch's dissent does not provide guidance on how to resolve such conflicts between federal and state law. As currently formulated, the strict property test appears to have hit a dead end.

New York statutes regulating traffic safety highlight another difficulty for the strict property test: How far could a legislature go in passing laws

192. See supra section I.B.4.

193. For a summary of the New York statute, see supra section I.B.4.

194. N.Y. Veh. & Traf. Law § 416-b.3(a)–(e) (McKinney 2019). Summarized broadly, the five exceptions are: (i) if the owner consents to the access, (ii) if the access is pursuant to a court order or administrative authority, (iii) if the data is accessed for traffic safety research, provided that the information is anonymized, (iv) if the data is accessed by a licensed automobile professional and for the purposes of vehicle repair or maintenance, and (v) if the data is accessed pursuant to emergency medical needs. Id.

195. Id.

196. Compare 49 U.S.C. § 30101 note (Driver Privacy Act of 2015) (defining the property ownership in the DPA), with N.Y. Veh. & Traf. Law § 416-b.3 (lacking a definition of who owns the data).

197. N.Y. Veh. & Traf. Law § 416-b.2(b).

198. See supra notes 89–90 and accompanying text.

that limit or undermine property rights? Passing a law limiting property rights in particular data would, under the strict property test, limit the likelihood that such data would receive Fourth Amendment protection. New York's traffic safety statutes do not go so far as to remove property rights in EDR; they only require officers to investigate the *causes* of accidents involving serious physical injury or death.[199] It could be argued that these statutes require officers to access EDR data, as such data is often essential to determining the cause of traffic accidents.[200] Although Justice Gorsuch does not specify as much in his dissent, drawing on the well-established norms of constitutional avoidance in statutory interpretation,[201] one can reasonably infer that where a statute may or may not *require* law enforcement to access certain property, that statute would be interpreted so as not to create a conflict with potential Fourth Amendment rights. But what if New York passed a statute requiring drivers to disclose their EDR data to law enforcement? Justice Gorsuch's dissent acknowledged that positive law may purport to grant law enforcement access to data that is otherwise owned by an individual.[202] Noting that this is problematic, Gorsuch suggested that legislatures should not be able to pass laws granting access where the Fourth Amendment would otherwise be triggered by the existence of property rights; for Gorsuch, there is a "constitutional floor below which Fourth Amendment rights may not descend."[203] It appears that the location of the floor would be set at a level that would assure "that degree of privacy against government that existed when the Fourth Amendment was adopted."[204] It is quite difficult to apply this concept to the question of EDR data; obviously neither cars, nor anything like them, were in existence at the Founding. Furthermore, this proscription relies on one of the foundational principles of the very *Katz*

199. See N.Y. Veh. & Traf. Law § 603-a(1). The investigations are required to determine "the facts and circumstances of the accident . . . [;] the contributing factor or factors; whether it can be determined if a violation or violations of [the New York Vehicle and Traffic Laws] occurred . . . and, the cause of such accident, where such cause can be determined." Id. at § 603-a(1)(a). EDR data would be helpful in reconstructing the facts, which specific provisions were violated (by showing the exact speed of the motorist in the seconds prior to an accident), and the cause (by showing, for example, whether a motorist failed to use their brakes or unreasonably applied pressure to the gas pedal in the moments before an accident).

200. For a review of how EDR data can be important for investigating the causes of traffic accidents, see supra section I.A.

201. See Philip P. Frickey, Getting from Joe to Gene (McCarthy): The Avoidance Canon, Legal Process Theory, and Narrowing Statutory Interpretation in the Early Warren Court, 93 Cal. L. Rev. 397, 399 (2005) (noting the existence of "the familiar canon of statutory interpretation that a serious constitutional challenge to a statute should be avoided if the statute can plausibly be construed in a manner that makes the constitutional question disappear").

202. See Carpenter v. United States, 138 S. Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting).

203. Id. at 2270.

204. Id. at 2271 (quoting United States v. Jones, 565 U.S. 400, 406 (2012)).

test that Justice Gorsuch proposed to replace.[205] Once again, the positive law model does not seem to offer a clear answer.

To summarize, when applied to the issue of EDR data in New York and California, the positive law model does not appear to provide a clear resolution of whether a search has occurred due to a lack of guidance on how to resolve conflicts between state and federal law. Although likely not implicated by New York's current statute, the traffic safety laws in New York also highlight the potential for difficult questions regarding the significance of positive law that imposes affirmative duties on law enforcement to access certain data. Justice Gorsuch's proposal, which was admittedly offered with the caveat that it was not a fully developed theory,[206] does not seem to include prescriptive guidance that would allow a court employing his model to arrive at a clear conclusion on either of these issues.

2. *States Without EDR Statutes.* — The strict property test does, however, provide a straightforward answer when applied to EDR downloads in states without an EDR statute of their own. Florida, Georgia, and Missouri all lack a state law governing EDR data.[207] The DPA appears to offer a clear conclusion, namely that downloading EDR data in each state constitutes a search, although there remain some difficulties with the strict property test due to the lack of definitions in the DPA for key terms.[208]

In *Worsham*, the Florida case addressing EDR data, the defendant asserting Fourth Amendment rights appeared to be the owner of the vehicle.[209] Thus, the DPA dictates that the defendant was the owner of the EDR data.[210] As the owner of the EDR data, the defendant clearly would enjoy Fourth Amendment protection for the data, and thus a search would be deemed to occur when law enforcement accesses the data. The analysis is also not undermined by any affirmative duties imposed on law enforcement to investigate traffic accidents in Florida, as no such affirmative duties exist.[211] Applied to the facts of the Florida case, the strict property test yields an easy, clear answer.

The strict property test is similarly straightforward to use, and yields the same conclusion, when applied to the facts of *Mobley* (the Georgia

---

205. See supra notes 173–176 and accompanying text.

206. See *Carpenter*, 138 S. Ct. at 2268 ("I do not begin to claim all the answers today . . . .").

207. See supra section I.B.4.

208. See 49 U.S.C. § 30101 note (Supp. III 2016) (Driver Privacy Act of 2015).

209. The opinion does not actually make this clear, but the prosecution would have likely raised a standing challenge to the defendant's assertion of Fourth Amendment rights if he was not at least the owner or lessee of the vehicle. See State v. Worsham, 227 So. 3d 602, 603 (Fla. Dist. Ct. App. 2017) (describing the facts of the case and failing to mention the exact nature of the defendant's property interest in the vehicle in question).

210. See 49 U.S.C. § 30101 note (Driver Privacy Act of 2015) (specifying that the "owner" of a vehicle in which an EDR is installed is the owner of the data recorded by the EDR).

211. See supra note 93.

case). Like Florida, Georgia does not have a state statute that regulates access to EDR data, nor do state statutes impose affirmative duties on law enforcement to investigate the causes of accidents.[212] Unburdened by potential conflicts between state and federal law, the strict property test analysis can proceed quite easily. First, the DPA establishes that data retained by an EDR is the property of the owner or lessee of the vehicle in which the EDR is contained.[213] As with *Worsham*, the *Mobley I* court did not specify the nature of the defendant's property interest in the vehicle containing the EDR, but the defendant appeared to be the owner of the vehicle.[214] Assuming that this were indeed the case, the strict property test dictates that, as the owner of the EDR data, the defendant would receive Fourth Amendment protection for that data.[215] Any attempt by law enforcement to access the data would constitute a search, and law enforcement would need to get a warrant to access it.[216]

When applied to the facts of *West* (the Missouri case), the strict property test yields a less clear answer due to the lack of a definition for "owner" in the DPA and the relationship between the defendant and the vehicle containing the accessed EDR. There are no statutes in Missouri that appear to impose affirmative duties on law enforcement to access EDR data,[217] which avoids any complications like those examined regarding

212. See supra note 93. Georgia law enforcement officers are required to report the "circumstances relating" to an accident that results in a death. Ga. Code Ann. § 40-6-277 (2018). This language does not impose as clear an obligation on officers to investigate the *causes* of an accident and thus does not seem to impose a duty on officers to access EDR data in the same way that New York law does. See supra note 199 and accompanying text.

213. See 49 U.S.C. § 30101 note (Driver Privacy Act of 2015).

214. This conclusion relies on a similar rationale as noted for the analysis of the *Worsham* case: The prosecution would have likely raised a standing challenge to the defendant's assertion of Fourth Amendment rights if he was not at least the owner or lessee of the vehicle. See *Mobley I*, 816 S.E.2d 769, 770–73 (Ga. Ct. App. 2018).

215. Justice Gorsuch's dissent makes clear that an individual need not hold exclusive title to information in order to receive Fourth Amendment protection. See Carpenter v. United States, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting) ("I doubt that complete ownership or exclusive control of property is always a necessary condition to the assertion of a Fourth Amendment right."). In this case, there does not appear to be a question of the vehicle owner's property interest in the data; the DPA says that it is the "property of the owner." See 49 U.S.C. § 30101 note (Driver Privacy Act of 2015). So, the defendant's ownership interest in the vehicle is relevant only to determining whether the DPA even applies to the defendant initially. Without a definition of "owner" or "lessee," it would be difficult to evaluate whether an individual with an attenuated relationship to a vehicle (e.g., an employee using an employer's vehicle) would have a sufficiently close connection to the vehicle to fall under the DPA.

216. Unless, of course, an exception to the warrant requirement existed. It is beyond the scope of this Note to consider how the exceptions to the warrant requirement might apply to the case of EDR data. There are a number of exceptions, however, that could plausibly justify a warrantless search. For a description of the major exceptions to the warrant requirement and the exceptions that are most relevant to the EDR data cases, see supra note 40.

217. See supra section I.B.4.

New York's statute.[218] Missouri also does not have a statute governing EDR data,[219] so the only potential source for property rights is the DPA. The DPA deems any data recorded by an EDR the property of the "owner" or "lessee" of the vehicle in which the EDR is installed.[220] In *West*, the defendant was driving a semitruck owned by his employer when the vehicle hit a pickup truck and killed the pickup truck's driver.[221] The defendant was thus the lawful, permissive, user of the vehicle, but appears to have held no legal title to the vehicle.[222] As noted above, "owner" and "lessee" are not defined in the DPA.[223] However, a plain text reading indicates that West does not have any property rights in the EDR data through the DPA. An employee seems to clearly not be a lessee; the average employment relationship does not involve such documentation.[224] Common understandings of "owner" would also indicate that a temporary, permissive user, essentially acting under a limited license,[225] would not be considered an owner.[226] The defendant would thus have no source of property rights in the EDR data, and therefore would not receive Fourth Amendment protection against law enforcement attempts to access the data. Although slightly complicated by the nature of the defendant's relationship to the vehicle housing the EDR, when applied to the facts of *West*, Gorsuch's model provides a relatively clear and well-functioning framework for analysis that yields a clear answer.

B. *Comparing the Strict Property Test to the Current Approach, and Suggestions for the Future*

The strict property test is clearly not without problems, but is it an improvement on the current doctrine? More specifically, is it less subjective, more predictable, and less beset by a fundamental lack of clarity than the two complementary approaches the Court uses now (the *Katz* test and the trespassory test)?[227]

---

218. See supra notes 199–205 and accompanying text.

219. See supra section I.B.4.

220. See 49 U.S.C. § 30101 note (Driver Privacy Act of 2015).

221. State v. West, 548 S.W.3d 406, 409 (Mo. Ct. App. 2018).

222. See id. at 409–12, 417.

223. See supra notes 190–191 and accompanying text.

224. See William C. Martucci, Missouri Practice Series: Employment Law and Practice §§ 2.1–2.37 (2018–2019 ed.), Westlaw (describing the standard elements of employment agreements in Missouri).

225. See 25 Am. Jur. 2d Easements and Licenses § 107 (2019) (noting that a license gives a licensee the authority to engage in acts that would otherwise be unlawful but it "does not give" the licensee any property interests).

226. See 63C Am. Jur. 2d Property § 30 (2019) ("Ownership is the legal right to use and enjoy property and to exercise *exclusive dominion and control* over a particular piece of property." (emphasis added)).

227. Proponents of the strict property test also argue that it is superior to the *Katz* test on historical and textual grounds. See Baude & Stern, supra note 14, at 1837–50. It is outside the scope of this Note to address such arguments, as the specific case of EDR data does not

When a clear statutory scheme governing property rights exists, the strict property test offers a predictable and objective method for determining whether a search has occurred. In Georgia, Florida, and Missouri, the DPA offered a relatively clear answer that any download of EDR data would be a search conducted with respect to the relevant car's owner or lessee.[228] But the statutory scheme governing the individual property at stake in Fourth Amendment challenges will not always be straightforward.

As highlighted by the examination of EDR data in California and New York, the strict property test, as currently formulated, could produce unpredictable results when confronted by federal and state law conflicts.[229] Justice Gorsuch's opinion does not provide information on how to resolve this issue, so courts would be left without guidance on how to proceed; this in turn might lead to unpredictable results. There are mechanisms available to resolve federal and state law conflicts that the strict property test could adopt to avoid unpredictable and subjective results. The most obvious method to adopt would be to utilize preemption doctrine, as this is the traditional framework for resolving disputes between federal and state law.[230] However, even if preemption doctrine is indeed the answer, the

---

help shed any new light on this aspect of the debate. Other scholars have also defended the strict property test on philosophical grounds. See, e.g., Trevor Burrus & James Knight, *Katz* Nipped and *Katz* Cradled: *Carpenter* and the Evolving Fourth Amendment, 2018 Cato Sup. Ct. Rev. 79, 101–10. Once again, it is outside the scope of this Note to address such arguments, although they are important aspects of the debate over the future of the Fourth Amendment.

There are also independent reasons why a complete focus on property rights may not be desirable. First, one could reasonably be concerned that an emphasis on the property would create a regressive effect in Fourth Amendment doctrine. Of course, poorer members of society will hold fewer property rights. Without the *Katz* framework, poorer individuals could be left with little doctrinal basis for asserting Fourth Amendment rights. Second, premising Fourth Amendment protection on property rights would likely spur a renewed focus on property law and prompt a push to promote privacy in digital information by creating property rights in such data. This may not be a desirable outcome; creating extensive property rights in data is likely to impair free speech and technological development. See Lothar Detterman, No One Owns Data, 70 Hastings L.J. 1, 34–39 (2018). Perhaps this is a tradeoff worth making, but at the very least it is one that should be analyzed in greater detail before adoption of the strict property test.

228. See supra section III.A.2.

229. See supra section III.A.1. The theory that Justice Gorsuch outlined was developed in a greater detail in an article by Professors Baude and Stern. See generally Baude & Stern, supra note 14. Baude and Stern acknowledged that conflict of laws may pose a complication for the theory but focused on horizontal conflict of laws rather than vertical conflict of laws, while also suggesting the issue was best left for analysis by scholars specializing in the field. See id. at 1863. They did not, however, discuss in any depth the potential problems of preemption that a reliance on positive law might pose. It seems that handling issues of preemption is another area that, if the positive law model is to supplant *Katz*, is best addressed by preemption scholars.

230. See American Tort Reform Ass'n, Summary of Preemption and the Current State of the Law 6–8 (2016), https://www.atra.org/wp-content/uploads/2016/11/Preemption.pdf [https://perma.cc/W4QJ-GHKD]. It is outside the scope of this Note to fully address the

issue of preemption in privacy regulation is a complicated and hotly debated issue.[231] Indeed, the DPA itself is silent on the topic of preemption.[232] It seems far from certain that such a nuanced issue would yield predictable results. Furthermore, preemption is not the only possible answer; it might also be the case that if the underlying charge is based on state criminal law, and the case is heard in state court, then state law should govern and federal law is irrelevant. Or, if the case was being heard in federal court, it might be that federal law would govern and state law would be irrelevant. As legislation on intangible data increases, this issue seems likely to assume greater importance.[233] Although there are methods to address conflicts of federal and state law, as currently formulated, the strict property test has not adopted any of the methods and thus would not lead to predictable results when such conflicts exist.

The strict property test also suffers from a lack of clarity, and thus objectivity and predictability, in establishing the limits of what legislatures can do in passing laws to remove protections or property rights. As the case of the New York traffic accident statute illustrated, states may pass laws that require law enforcement to access certain data.[234] Justice Gorsuch's opinion implies that this should not be sufficient to destroy Fourth Amendment protection for such data, but also seems to imply that legislatures could pass some laws to remove property rights.[235] The exact extent of legislative power is a crucial issue; a test that proposes to impose no limits on legislative power to remove property rights would seemingly obliterate constitutional protections meant specifically to check the power of the legislature. The lack of clarity on this point is another significant weakness for the strict property test. While these are significant problems, they should be considered in comparison to the problems of the current approach as elucidated by application of that approach to the issue of EDR data.

Although the state courts largely ignored it, the trespassory test seems to provide a more natural analytical frame for addressing EDR data downloads. The trespassory test dictates that a physical intrusion into a

---

extent to which the DPA preempts state laws, as this would be a complicated inquiry unto itself, and it is not clear this would indeed be the method for resolution.

231. See Peter Swire, US Federal Privacy Preemption Part 1: History of Federal Preemption of Stricter State Laws, IAPP (Jan. 9, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws [https://perma.cc/3P62-SUQV]; Peter Swire, US Federal Privacy Preemption Part 2: Examining Preemption Proposals, IAPP (Jan. 10, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-2-examining-preemption-proposals [https://perma.cc/2YX4-AH46].

232. See 49 U.S.C. § 30101 note (Supp. III 2016) (Driver Privacy Act of 2015).

233. Congress is, for example, considering a bill titled the "Security and Privacy in Your Car Act of 2017" or the "SPY Car Act of 2017," which would grant car owners additional rights to limit the use of data collected by car manufacturers. See Security and Privacy in Your Car Act of 2017, S. 680, 115th Cong. § 27.

234. See supra notes 200–204 and accompanying text.

235. See supra notes 202–205 and accompanying text.

constitutionally protected area constitutes a Fourth Amendment search.[236] In order to access EDR data, one must physically intrude into the relevant automobile.[237] The question thus becomes whether the EDR is a constitutionally protected area.

Although the trespassory test is framed as an independent test, answering this question quickly requires reliance on principles that seem to draw heavily on the *Katz* formulation. In the Court's own articulation, "[w]hile the interior of an automobile is not subject to the same expectations of privacy that exist with respect to one's home, a car's interior as a whole is nonetheless subject to Fourth Amendment protection from unreasonable intrusions by the police."[238] Although this formulation is more than thirty years old, more recent cases affirm the proposition that automobiles are indeed constitutionally protected areas; in *Jones*, decided in 2012, the Court explicitly noted that "[i]t is beyond dispute that a vehicle is an 'effect' as that term is used in the [Fourth] Amendment."[239] The sphere of constitutional protection for automobiles does not extend to information that is required by federal law to be "placed in the plain view of someone *outside* the automobile,"[240] even when that information is within a car and obscured by papers placed on top of the document displaying the relevant information.[241]

The exact effect of a defendant's particular ownership relationship complicates the application of these principles. In *Jones*, when the Court found that a search occurred, the defendant was not the owner of the vehicle although he was the exclusive driver.[242] The Court noted that this would have been sufficient to establish the defendant as a bailee of the vehicle, but specifically declined to address the D.C. Circuit's determination that such status did not prevent the defendant from raising a Fourth Amendment challenge.[243]

EDR data is not required to be displayed publicly, nor are car manufacturers even required to include an EDR in the automobiles they

---

236. See United States v. Jones, 565 U.S. 400, 406–07 (2012) (holding that attaching a GPS tracking device to the underside of a vehicle was a physical intrusion on a constitutionally protected area).

237. See supra note 23 and accompanying text.

238. See New York v. Class, 475 U.S. 106, 114–15 (1986). The use of the reasonable expectations framework in this articulation highlights how the trespassory test and the *Katz* test easily merge together under the Court's current approach.

239. See *Jones*, 565 U.S. at 404.

240. *Class*, 475 U.S. at 111.

241. See id. at 114 ("[B]ecause of the important role played by the VIN [Vehicle Identification Number] in . . . governmental regulation of the automobile and the efforts by the . . . Government to ensure that the VIN is placed in plain view, we hold that there was no reasonable expectation of privacy in the VIN.").

242. See *Jones*, 565 U.S. at 404 n.2.

243. See id. at 404.

produce.[244] It therefore seems that the EDR device itself, and the concomitant data contained within it, is a constitutionally protected area. The EDR device is part of a vehicle, and vehicles are generally constitutionally protected "effects" under the Fourth Amendment.[245] There is no federal or state regulation that establishes sufficient access requirements to extract the EDR from that realm.[246] Thus, under the trespassory test, which is itself seemingly sufficient for determining that a search has occurred,[247] accessing EDR data appears to constitute a Fourth Amendment search.

The *Katz* test yields a far less clear answer. The first prong of the *Katz* test is problematic. The average car owner is probably unlikely to know that their car contains an EDR device. As the dissenting judge in *Worsham* noted, if an individual is unaware that information is being recorded, how can they exhibit a subjective expectation of privacy in that information?[248] It seems natural to conclude that if one is unaware that information is even being recorded that one could not exhibit a subjective expectation of privacy in that information, and therefore could not receive Fourth Amendment protection through the *Katz* test for such information. This would, however, eliminate Fourth Amendment protection for much of the information recorded on individuals in the modern age; there is a seemingly constant stream of revelations about information and data that modern cell phones, automobiles, and other internet-enabled devices record about their users without the user's knowledge.[249] If someone didn't know their Apple Watch was recording their blood alcohol content level, would that necessarily defeat any Fourth Amendment protection for that information? If so, far too much information would be unprotected by the Fourth Amendment. Aside from this practical objection, it is reasonable to argue that a driver is of course aware of their speed when braking and whether or not they

244. See supra note 82 and accompanying text.

245. See *Jones*, 565 U.S. at 404.

246. See supra section I.B.3–.4.

247. See *Jones*, 565 U.S. at 404–11 ("Jones's [(the defendant's)] Fourth Amendment rights do not rise or fall with the *Katz* formulation.").

248. See State v. Worsham, 227 So. 3d 602, 609 (Fla. Dist. Ct. App. 2017) (Forst, J., dissenting).

249. See Devin Coldewey, Google Keeps a History of Your Locations Even When Location History Is Off, TechCrunch (Aug. 13, 2018), https://techcrunch.com/2018/08/13/google-keeps-a-history-of-your-locations-even-when-location-history-is-off [https://perma.cc/48ZY-NY8W]; Internet of Things (IoT), epic.org, https://epic.org/privacy/internet/iot [https://perma.cc/9AQW-3EHR] (last visited Mar. 1, 2020); Lily Hay Newman, Medical Devices Are the Next Security Nightmare, WIRED (Mar. 2, 2017), https://www.wired.com/2017/03/medical-devices-next-security-nightmare [https://perma.cc/GQ2E-2Q72]; Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (on file with the *Columbia Law Review*); Sam Nichols, Your Phone Is Listening and It's Not Paranoia, Vice (Jun. 4, 2018), https://www.vice.com/en_au/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia [https://perma.cc/QJK6-MCWH].

are wearing a seatbelt, so the existence of a device recording that information is irrelevant. This seems an equally plausible interpretation of this issue.

The second prong of the *Katz* test is equally vexing. Individuals do not have a reasonable expectation of privacy in information that is knowingly exposed to the public,[250] as long as that information does not reveal too much about an individual's life.[251] EDR data records information that is indeed technically exposed to the public: One can view whether a car is accelerating or decelerating, or whether a driver is wearing their seatbelt, merely by standing on the street near the car. And whether or not a driver is using their brakes in the moments before impact hardly reveals too much information about their personal associations and predilections. The information recorded, however, could not be accessed to the level of detail (e.g., the exact speed of the car, the angular rate of momentum, or the yaw rate) obtained through accessing an EDR by the bystander on the street; it is therefore quite plausible to argue that the information was not in fact exposed to the public.

Federal and state legislation, as an expression of public opinion, is also an indicator of what society views as a reasonable expectation of privacy. The DPA provides protections against law enforcement access (a court must "authorize[] the retrieval of the data").[252] Congress, however, specifically declined to require a warrant in order to access the data. This implies that a subpoena, which is generally insufficient when the Fourth Amendment is triggered,[253] could be sufficient to grant law enforcement access to EDR data. This in turn leads to the conclusion that Congress, and therefore the people, do not believe that it is reasonable to have an expectation of privacy in EDR data. With that said, the statutory protections could quite plausibly be read to reach the opposite conclusion. The mere fact that Congress, as well as a number of states,[254] have enacted protections for EDR data at all signals that the public believes there should be some expectation of privacy in EDR data. Overall, the *Katz* approach does not seem to provide clear guidance on whether a search occurs by downloading EDR data.

Since the *Katz* test might lead to the determination that accessing EDR data is not a search, one must consider how current doctrine would handle a situation in which the *Katz* test dictates that no search has occurred but the trespassory test indicates the opposite. While it is true that the

250. See United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding that the defendant did not enjoy a reasonable expectation of privacy in his car's movements on public roadways).

251. See Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

252. See 49 U.S.C. § 30101 note (Supp. III 2016) (Driver Privacy Act of 2015).

253. See Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971) (holding that, as a general rule, a warrant is required when the Fourth Amendment is triggered).

254. See supra sections I.B.3–.4.

trespassory test is itself sufficient, the Court has not squarely addressed how judges should rule if the *Katz* test indicates one conclusion while the trespassory test indicates another.[255] This is indeed a significant issue.

Yet, in comparison to the fundamental difficulties of the strict property test, these problems are relatively minor and can be addressed by a number of similarly minor doctrinal moves. First, the Court could clarify the respective roles of the trespassory test and the *Katz* test, and place a greater emphasis on the trespassory test. Current doctrine does not exclude property rights from providing guidance.[256] Indeed, a violation of the trespassory test appears to be a sufficient condition for finding that a search has occurred.[257] In future Fourth Amendment cases, the Court could make the status of the trespassory test clearer by explicitly noting that both the trespassory test and the *Katz* test are sufficient to find that a search has occurred.[258]

The Court could also require that lower courts look first to the trespassory test. In this formulation, if the trespassory test requirements were met, a court would not need to reach the *Katz* analysis. Such a framework would remove the potential for situations in which the two tests indicate different conclusions, as a court would only need to conduct the *Katz* analysis if the trespassory test did not yield a clear answer. The *Katz* test would therefore become a secondary test, to be relied upon only when the trespassory test does not yield a clear answer. This would in turn mitigate the deleterious effects of the *Katz* test's subjective and unpredictable character, while preserving the flexibility of the test for addressing circumstances that cannot easily be resolved through the trespassory test.

Second, the Court could remove the requirement that an individual exhibit a subjective expectation of privacy where the information in question was recorded involuntarily and without the individual's knowledge.[259] For example, in the case of EDR data, car purchasers do not have a meaningful choice as to whether EDRs are installed in their vehicle, as over ninety-six percent of new vehicles come equipped with an EDR.[260] The only way for a buyer to know, however, that their car comes equipped with

255. See, e.g., *Jones*, 565 U.S. at 406.

256. See supra notes 50–53 and accompanying text.

257. See supra note 58 and accompanying text.

258. This itself might even be unnecessary. The court in *Mobley II* accurately described the trespassory test and *Katz* test as independently sufficient means of establishing that a search has occurred, suggesting that any current confusion may dissipate in short order as courts have time to digest the relevant statements in *Jones*. See 834 S.E.2d 785, 792 (Ga. 2019).

259. This suggestion builds upon an idea developed by Professor Orin Kerr as part of a larger proposal for how to implement the holding of *Carpenter*. See Orin S. Kerr, The Digital Fourth Amendment: Implementing *Carpenter* (forthcoming) (manuscript at 3), https://ssrn.com/abstract=3301257 (on file with the *Columbia Law Review*).

260. See Rafter, supra note 4.

an EDR is to browse deep into the vehicle's owner manual.[261] It does not seem that the owner should be penalized for not reading the depths of an owner's manual.

These solutions are not perfect, but they entail fewer drawbacks than those posed by the strict property test. The strict property test, as currently theorized, is not equipped to deal with complicated and fundamental problems regarding conflict of state and federal law[262] and affirmative access requirements in positive law.[263] In addition, entirely jettisoning the *Katz* test is a significant move that would undermine decades of doctrine.[264] This would create significant uncertainty as courts worked through the implications of previous Fourth Amendment holdings. Furthermore, premising Fourth Amendment protections entirely on the existence of property rights would likely result in fewer protections for the poor; the poor are less likely to hold property rights in areas subject to police intrusion and thus such intrusions would likely not be considered searches under the strict property test. For the moment, it therefore seems wiser to make adjustments within the current framework rather than abandoning the *Katz* test entirely in favor of the as-yet underdeveloped strict property test.

CONCLUSION

The data recorded by EDRs is commonly used by police to investigate car accidents.[265] Car accidents are a leading cause of death in America; more than 37,000 people died from car accidents in 2017 alone.[266] The investigation of these crashes is therefore a matter of significant import. Furthermore, the application of the Fourth Amendment to computers within cars is an area that is likely to become more important with the rise of autonomous vehicles and connected cars. As a computer embedded within the car's machinery, EDRs provide an early test of how Fourth Amendment doctrine can handle future investigations of computers in cars. Although the existing *Katz* approach is not without difficulties, the strict property test proposed by Justice Gorsuch as an alternative is, as of this moment, not developed enough to justify abandoning the *Katz* model.

---

261. Federal regulations require that owner's manuals include disclosures that EDRs are contained in a given vehicle, but do not require any other disclosures that might notify a buyer that their vehicle contains an EDR. See 49 C.F.R. § 563.11 (2017).

262. See supra notes 229–233 and accompanying text.

263. See supra notes 234–235 and accompanying text.

264. *Katz* was decided in 1967, meaning that more than fifty years of Fourth Amendment doctrine would be need to be reconsidered. United States v. Katz, 389 U.S. 347 (1967).

265. See State v. West, 548 S.W.3d 406, 410 (Mo. Ct. App. 2018).

266. See U.S. Nat'l Highway Traffic Safety Admin., supra note 35, at 1.