DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
FOURTH DISTRICT

STATE OF FLORIDA,
Appellant,

v.

CHARLES WILEY WORSHAM, JR.,
Appellee.

No. 4D15-2733

[March 29, 2017]

CORRECTED OPINION

Appeal of a non-final order from the Circuit Court for the Fifteenth Judicial Circuit, Palm Beach County; Jack Schramm Cox, Judge; L.T. Case No. 2013CF012609AMB.

Pamela Jo Bondi, Attorney General, Tallahassee, and Mitchell A. Egber, Assistant Attorney General, West Palm Beach, for appellant.

Jack A. Fleischman of Fleischman & Fleischman, P.A., West Palm Beach, for appellee.

GROSS, J.

The state challenges an order granting appellee Charles Worsham's motion to suppress. Without a warrant, the police downloaded data from the "event data recorder" or "black box" located in Worsham's impounded vehicle. We affirm, concluding there is a reasonable expectation of privacy in the information retained by an event data recorder and downloading that information without a warrant from an impounded car in the absence of exigent circumstances violated the Fourth Amendment.

Worsham was the driver of a vehicle involved in a high speed accident that killed his passenger. The vehicle was impounded. Twelve days after the crash, on October 18, 2013, law enforcement downloaded the information retained on the vehicle's event data recorder. The police did not apply for a warrant until October 22, 2013. The warrant application was denied because the desired search had already occurred.

Worsham was later arrested and charged with DUI manslaughter and vehicular homicide. He moved to suppress the downloaded information, arguing the police could not access this data without first obtaining his consent or a search warrant. The state defended the search on the sole ground that Worsham had no privacy interest in the downloaded information, so that no Fourth Amendment search occurred.[1] The trial court granted Worsham's motion.

"A motion to suppress evidence generally involves a mixed question of fact and law. The trial court's factual determinations will not be disturbed if they are supported by competent substantial evidence, while the constitutional issues are reviewed de novo." *State v. K.C.*, 207 So. 3d 951, 953 (Fla. 4th DCA 2016) (internal citation omitted). An appellate court is bound by the trial court's findings of fact unless they are clearly erroneous. *Id.* The burden is on the defendant to show the search was invalid, "[h]owever, a warrantless search constitutes a prima facie showing which shifts to the State the burden of showing the search's legality." *Id.* (internal citation omitted).

In Florida, citizens are guaranteed the right to be free from unreasonable searches and seizures by the Fourth Amendment to the Unites States Constitution and section 12 of Florida's Declaration of Rights. *Smallwood v. State*, 113 So. 3d 724, 730 (Fla. 2013). "The most basic constitutional rule" in the area of Fourth Amendment searches

> is that "*searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.*" The exceptions are "jealously and carefully drawn," and there must be "a showing by those who seek exemption . . . that the exigencies of the situation made that course imperative." "*[T]he burden is on those seeking the exemption to show the need for it.*"

Id. at 729 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 454–55 (1971)).

"A Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."

---

[1] The state raises inevitable discovery and good faith in its brief. We do not reach these issues because they were not preserved in the circuit court. *Sunset Harbour Condo. Ass'n v. Robbins*, 914 So. 2d 925, 928 (Fla. 2005).

State v. Lampley, 817 So. 2d 989, 990 (Fla. 4th DCA 2002) (quoting *Kyllo v. United States*, 533 U.S. 27, 33 (2001)). This principle has been applied "to hold that a Fourth Amendment search does *not* occur . . . unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that expectation as reasonable.'" *Lampley*, 817 So. 2d at 990-91 (quoting *Kyllo*, 533 U.S. at 33)).

Katz v. United States explained "the Fourth Amendment protects people, not places," so "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." 389 U.S. 347, 351 (1967). One example is a car's exterior, which "is thrust into the public eye, and thus to examine it does not constitute a 'search.'" *New York v. Class*, 475 U.S. 106, 114 (1986); *see also Cardwell v. Lewis*, 417 U.S. 583, 592 (1974) (permitting warrantless search of an automobile's exterior).

Nevertheless, information someone seeks to "preserve as private," even where that information is accessible to the public, "may be constitutionally protected." *Katz*, 389 U.S. at 351. This is why "a car's interior as a whole is . . . subject to Fourth Amendment protection from unreasonable intrusions by the police." *Class*, 475 U.S. at 114–15; *see also United States v. Ortiz*, 422 U.S. 891, 896 (1975) ("A search, even of an automobile, is a substantial invasion of privacy.").

A car's black box is analogous to other electronic storage devices for which courts have recognized a reasonable expectation of privacy. Modern technology facilitates the storage of large quantities of information on small, portable devices. The emerging trend is to require a warrant to search these devices. *See Riley v. California*, 134 S. Ct. 2473 (2014) (requiring warrant to search cell phone seized incident to arrest); *Smallwood*, 113 So. 3d 724 (requiring warrant to search cell phone in search incident to arrest); *State v. K.C.*, 207 So. 3d 951 (requiring warrant to search an "abandoned" but locked cell phone).

Noting that cell phones can access or contain "[t]he most private and secret personal information, *Smallwood*, 113 So. 3d at 732, the Florida Supreme Court has distinguished these computer-like electronic storage devices from other inanimate objects:

> [A]nalogizing computers to other physical objects when applying Fourth Amendment law is not an exact fit because computers hold so much personal and sensitive information touching on many private aspects of life. . . . [T]here is a far

> greater potential for the "inter-mingling" of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.

Id. (quoting *United States v. Lucas*, 640 F.3d 168, 178 (6th Cir. 2011)). Because of the "very personal and vast nature of the information" they contain, cell phones are "materially distinguishable from the static, limited-capacity cigarette packet in *Robinson*."[2] *Smallwood*, 113 So. 3d at 732. "[T]he search of a static, non-interactive container, cannot be deemed analogous to the search of a modern electronic device cell phone." *Id.* The *Smallwood* court made clear that the opinion was "narrowly limited to the legal question and facts with which [it] was presented." *Id.* at 741. Nonetheless, the court reiterated its desire to protect Fourth Amendment precedent "by ensuring that the exceptions to the warrant requirement remain 'jealously and carefully drawn.'" *Id.* at 740.

The United States Supreme Court drew a similar distinction between a cell phone and other tangible objects in *Riley v. California*. The Court held that the search incident to arrest exception did not apply because neither rationale–the interest in protecting officer safety or preventing destruction of evidence–justified the warrantless search of cell phone data. *Riley*, 134 S. Ct. at 2486-88. "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers . . . ." *Id.* at 2489.

Searches of these "minicomputers," with their "immense storage capacity," are far more intrusive than searches prior to the "digital age," which were "limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Id.* The capacity of these devices "allows even just one type of information to convey far more than previously possible." *Id.* The Court concluded, "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.* at 2495.

It is an issue of first impression in Florida whether a warrant is required to search an impounded vehicle's electronic data recorder or black box.[3]

---

[2] *United States v. Robinson*, 414 U.S. 218 (1973) (permitting the warrantless search of an arrestee's person incident to arrest if the officer had probable cause for the arrest).

[3] As of this writing, 17 states have laws addressing event data recorders, which provide under what circumstances the data may be downloaded. *Privacy of Data*

An event data recorder is a device installed in a vehicle to record "crash data" or technical vehicle and occupant information for a period of time before, during, and after a crash. NHTSA, Event Data Recorders, 49 C.F.R. § 563.5 (2015). Approximately 96% of cars manufactured since 2013 are equipped with event data recorders. *Black box 101: Understanding event data recorders*, CONSUMER REPORTS, http://www.consumerreports.org/cro/2012/10/black-box-101-understanding-event-data-recorders/index.htm, (published Jan. 2014).

Most of these devices are programmed either to activate during an event or record information in a continuous loop, writing over data again and again until the vehicle is in a collision. Michelle V. Rafter, *Decoding What's in Your Car's Black* Box, EDMUNDS, https://www.edmunds.com/car-technology/car-black-box-recorders-capture-crash-data.html (updated July 22, 2014). However, if triggered, the device can record multiple events. 49 C.F.R. § 563.9.

The National Highway Traffic Safety Administration has standardized the minimum requirements for electronic data recorders, mandating that the devices record 15 specific data inputs, including braking, stability control engagement, ignition cycle, engine rpm, steering, and the severity and duration of a crash. 49 C.F.R. § 563.7. Along with these required data inputs, the devices may record additional information like location or cruise control status and some devices can even perform diagnostic examinations to determine whether the vehicle's systems are operating properly. *See Decoding 'The Black Box' with Expert Advice*, AMERICAN BAR ASSOC. GP SOLO LAW TRENDS & NEWS, http://www.americanbar.org/content/newsletter/publications/law_trends_news_practice_area_e_newsletter_home/decodingblackbox.html (May 2005); *Vehicular Data Recorder Download, Collection, and Analysis*, COLLISION RESEARCH AND ANALYSIS INC., http://collisionresearch.com/services/event-data-recorder-0.

The information contained in a vehicle's black box is fairly difficult to obtain. The data retrieval kit necessary to extract the information is expensive and each manufacturer's data recorder requires a different type of cable to connect with the diagnostic port. Rafter, *supra*. The downloaded data must then be interpreted by a specialist with extensive

---

From Event Data Recorders: State Statutes, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx (Jan. 4, 2016). Florida does not have similar legislation.

training. *Id.*; *see also* Melissa Massheder Torres, *The Automotive Black Box*, 55 REV. DER. P.R. 191, 192 (2015).

The record reflects that the black box in Worsham's vehicle recorded speed and braking data, the car's change in velocity, steering input, yaw rate, angular rate, safety belt status, system voltage, and airbag warning lamp information.

Extracting and interpreting the information from a car's black box is not like putting a car on a lift and examining the brakes or tires. Because the recorded data is not exposed to the public, and because the stored data is so difficult to extract and interpret, we hold there is a reasonable expectation of privacy in that information, protected by the Fourth Amendment, which required law enforcement in the absence of exigent circumstances to obtain a warrant before extracting the information from an impounded vehicle.

Although electronic data recorders do not yet store the same quantity of information as a cell phone, nor is it of the same personal nature, the rationale for requiring a warrant to search a cell phone is informative in determining whether a warrant is necessary to search an immobilized vehicle's data recorder. These recorders document more than what is voluntarily conveyed to the public and the information is inherently different from the tangible "mechanical" parts of a vehicle. Just as cell phones evolved to contain more and more personal information, as the electronic systems in cars have gotten more complex, the data recorders are able to record more information.[4] The difficulty in extracting such information buttresses an expectation of privacy.

Recently enacted federal legislation enhances the notion that there is an expectation of privacy in information contained in an automobile data recorder. The Driver Privacy Act of 2015 states that "[a]ny data retained by an event data recorder . . . is the property of the owner . . . of the motor vehicle in which the event data recorder is installed." § 24302(a), 49 U.S.C. § 30101 note (2015). The general rule of the statute is that "[d]ata recorded or transmitted by an event data recorder . . . *may not be accessed by a person other than an owner . . . of the motor vehicle in which the event data*

---

[4] *See* U.S. GOV'T ACCOUNTABILITY OFF., REPORT TO CHAIRMAN, SUBCOMM. ON PRIVACY, TECH. AND THE LAW, COMM. ON THE JUDICIARY, U.S. SENATE, (Dec. 2013), http://www.gao.gov/assets/660/659509.pdf; Peter Gareffa, *Senate Committee Approves Black Box Privacy Bill*, EDMUNDS, (Apr. 18, 2014), https://www.edmunds.com/car-news/senate-committee-approves-black-box-privacy-bill.html.

recorder is installed." § 24302(b) (emphasis added). There are only five exceptions to this rule, which include authorization from a court or administrative authority or consent of the owner. § 24302(b)(1)-(5).

A state court in California has addressed the Fourth Amendment's application to a vehicle's data recorder. That authority is not persuasive or controlling and was decided prior to the passing of the Driver Privacy Act of 2015.

People v. Diaz, held that the defendant lacked a privacy interest in his vehicle's speed and braking data, obtained from the "sensing diagnostic module" after a fatal accident, 153 Cal. Rptr. 3d 90 (Cal. Ct. App. 2013). It was undisputed the search was conducted without a warrant, over a year after the accident. *Id.* at 96. There was testimony about the defendant's speed at the time of the accident, but the officer conceded this was based on the information downloaded from the vehicle's sensing diagnostic module. *Id.* at 94.

The court concluded that the defendant failed to demonstrate "a subjective expectation of privacy in the SDM's recorded data because she was driving on the public roadway, and others could observe her vehicle's movements, braking, and speed, either directly or through the use of technology such as radar guns or automated cameras." *Id.* at 102. Since the diagnostic module "merely captured information defendant knowingly exposed to the public," downloading that information without a warrant was not a violation of the Fourth Amendment. *Id.* (citing *Smith v. Maryland* 442 U.S. 735, 741–45 (1979) (holding installation of a pen register did not violate the Fourth Amendment because it only recorded information "voluntarily conveyed . . . in the ordinary course of business.")).

Diaz is unpersuasive. It relied on *Smith v. Maryland*, which found no expectation of privacy in information "voluntarily conveyed" to a third party. 422 U.S. at 745. However, when addressing digital devices, the Supreme Court has moved away from the *Smith* rationale. In *United States v. Jones*, the Court could have relied on *Smith* when considering the constitutionality of placing a GPS tracking device on a vehicle without a warrant, since the vehicle's position "had been voluntarily conveyed to the public." 132 S. Ct. 945, 951 (2012). Instead, the Court relied on a trespass theory to find that while "mere visual observation does not constitute a search," attaching a device to the vehicle or reaching into a vehicle's interior constitutes "encroach[ment] on a protected area." *Id.* at 952-53.

Additionally, the *Diaz* court's reliance on *Smith v. Maryland* seems misplaced because, as the opinion acknowledged, sensory diagnostic

modules can record much more information than what is observable to the public, including "the throttle, steering, suspension, brakes, tires, and wheels." 213 Cal. App. 4th at 748. We disagree with *Diaz* that all black box data is "exposed to the public."

Although the issue was not before the Court, the majority in *Jones* acknowledged that acquiring data "through electronic means, without an accompanying trespass," could still be "an unconstitutional invasion of privacy." *Id.* at 953.

In his concurring opinion, Justice Alito expressed a preference for analyzing the case by "asking whether [Jones's] reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." 132 S. Ct. at 958. Justice Alito observed that the *Katz* expectation-of-privacy test,

> rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the trade off worthwhile.

Id. at 962. Under Justice Alito's approach, the constant, unrelenting black box surveillance of driving conditions could contribute to a reasonable expectation of privacy in the recorded data. Considering 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, and we agree with the trial court that a warrant was required before police could search the black box.

Affirmed.

KLINGENSMITH, J., concurs.
FORST, J., dissents with opinion.

FORST, J., dissenting.

I respectfully dissent. There are not many court opinions addressing a warrantless search of the "black box" event data recorder ("EDR") attached

to an individual's motor vehicle.[5] An opinion by a "Justice Court" in New York (similar to a circuit court in Florida)[6] and an appellate court in California[7] appear to be the only published precedent addressing the instant matter. 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, and the United States Constitution's right to privacy sheds no light on the subject (particularly since there is no provision actually describing such a right to privacy).[8]

Thus, there is no definitive answer to the question posed in this case—whether the warrantless search of Appellee's car's EDR constituted a violation of his Fourth Amendment protection against unreasonable searches. Nonetheless, contrary to the well-reasoned majority opinion, I conclude that the "search" of the EDR attached to Appellee's vehicle was not a search or seizure protected by the Fourth Amendment, as Appellee did not have a reasonable expectation of privacy with respect to the data in this particular EDR.

Background

The relevant facts are set forth in the majority opinion.

Analysis

---

[5] In General Motors vehicles, the EDR is also referred to as the "Sensing Diagnostic Module (SDM)." *People v. Diaz*, 153 Cal. Reptr. 3d 90, 92 n.2 (Ct. App. 2013); *People v. Christmann*, 776 N.Y.S.2d 437, 438 (Just. Ct. 2004). "The SDM . . . has multiple functions: (1) it determines if a severe enough impact has occurred to warrant deployment of the air bag; (2) it monitors the air bag's components; and (3) it permanently records information." *Bachman v. Gen. Motors Corp.*, 776 N.E.2d 262, 271-72 (Ill. App. Ct. 2002).

[6] *Christmann*, 776 N.Y.S.2d 437.

[7] *Diaz*, 153 Cal. Reptr. 3d 90. *Diaz* is discussed in this opinion. Another California appellate court decision, *People v. Xinos*, 121 Cal. Rptr. 3d 496 (Ct. App. 2011), which held that the downloading of data from the vehicle's EDR following an accident violated the driver's Fourth Amendment rights, is not discussed as it predates *Diaz* and was ordered not to be officially published. *Id.* at 507-12.

[8] Appellee does not rely upon the Florida Constitution's Right of Privacy, Article I, Section 23. Further, that provision yields to Article I, Section 12 with respect to "searches and seizures," with the Florida Constitutional right "construed in conformity with the 4th Amendment to the United States Constitution, as interpreted by the United States Supreme Court."

As noted in the majority opinion, "[a] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *State v. Lampley*, 817 So. 2d 989, 990 (Fla. 4th DCA 2002) (quoting *Kyllo v. United States*, 533 U.S. 27, 33 (2001)). The reverse is also true: "a Fourth Amendment search does *not* occur . . . unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that expectation as reasonable.'" *Id.* at 991 (alterations in original) (quoting *Kyllo*, 533 U.S. at 33).

In contrast to a cellular phone, an EDR does not contain "a broad array of private information" such as photos, passwords, and other "sensitive records previously found in the home." *Riley v. California*, 134 S. Ct. 2473, 2491 (2014). Significantly, the EDR in the instant case did not contain GPS information relative to the vehicle's travels, which may be subject to privacy protection. *See United States v. Jones*, 565 U.S. 400, 415-17 (2012) (Sotomayor, J., concurring) (expressing concern with GPS information which "reflects a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations"). As noted in the majority opinion, the EDR in this case was only recording speed and braking data, the car's change in velocity, steering input, yaw rate,[9] angular rate, safety belt status, system voltage, and airbag warning lamp information. Moreover, this data had not been knowingly inputted by Appellee; in fact, it is likely that Appellee did not even know that the vehicle he was driving had an EDR. Therefore, it would be quite a stretch to conclude that Appellee sought to preserve this information as "private."

The majority opinion references the United States Supreme Court's *Riley* decision as well as this Court's recent opinion in *State v. K.C.*, 207 So. 3d 951 (Fla. 4th DCA 2016). Both cases involved cell phones. As distinguished from an EDR attached to an undercarriage of a motor vehicle, cell phones are usually carried close to an individual's body, generally in a pants or shirt pocket or in a purse or belt case. The database of the EDR in this case carries extremely non-private, non-confidential information, such as the vehicle's yaw rate; a cell phone, on the other hand, "collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal

---

[9] "A yaw rotation is a movement around the yaw axis of a rigid body that changes the direction it is pointing, to the left or right of its direction of motion. The yaw rate or yaw velocity of a car, aircraft, projectile or other rigid body is the angular velocity of this rotation . . . ." *Yaw (rotation)*, WIKIPEDIA (Mar. 13, 2017, 2:37 PM), https://en.wikipedia.org/wiki/Yaw_(rotation) (emphasis omitted). Yes, I also didn't know what this was.

much more in combination than any isolated record." *Riley*, 134 S. Ct. at 2489. A reasonably prudent seller of his/her used cellphone or personal computer would clear the hard drive of all personal information; the seller of a used vehicle would be unlikely to take similar action with respect to the vehicle's EDR.

In our *K.C.* opinion, we emphasized that, though abandoned by the phone's owner, "[the] contents [of the cell phone] were still protected by a password, clearly indicating an intention to protect the privacy of all of the digital material on the cell phone or able to be accessed by it." *K.C.*, 207 So. 3d at 955. The private data in a cell phone is, for the most part, created by the owner and is password protected by the owner for his/her own benefit and privacy. The data on the EDR, however, was not created by the owner and was not protected by a password by or for the benefit of the owner (even though there apparently was a password-like encryption on the data). This data is collected and stored in the interest of public safety, including the safety of the vehicle's driver.

In the aforementioned New York *Christmann* decision which involved a prosecution for speeding and failing to exercise due care, the court held that the motorist had only a diminished expectation of privacy following an accident with respect to the vehicle's mechanical areas, and therefore retrieval by law enforcement of data stored in the vehicle's SDM did not constitute an unreasonable search and seizure. *Christmann*, 776 N.Y.S.2d at 441-42; *see also People v. Quackenbush*, 670 N.E.2d 434, 439-40 (N.Y. 1996) (similar, and specifically referring to the diminished expectation of privacy yielding to the overwhelming state interest in investigating fatal accidents).

The California case of *Diaz* involved a situation similar to the instant case. *Diaz*, 153 Cal. Rptr. 3d 90. There was a motor vehicle accident and, as part of their investigation, law enforcement personnel, without a warrant, downloaded the SDM. *Id.* at 96. The California Court of Appeal affirmed the trial court's ruling that there was no reasonable expectation of privacy with respect to the data in the SDM, finding the defendant failed to demonstrate "a subjective expectation of privacy in the SDM's recorded data because she was driving on the public roadway, and others could observe her vehicle's movements, braking, and speed, either directly or through the use of technology such as radar guns or automated cameras." *Id.* at 102. "[T]echnology merely captured information defendant knowingly exposed to the public—the speed at which she was travelling and whether she applied her brakes before the impact." *Id.*

The majority opinion discounts the reasoning in *Diaz*, finding it neither "persuasive [n]or controlling." Certainly, it is not controlling. However, it is persuasive, as the trial court's decision denying the defendant's motion to suppress, quoted in the District Court's opinion, is particularly logical:

> "Assuming the defendant had such knowledge [that there was an SDM in the car] and also had an expectation of privacy, it does not seem that such expectation would be reasonable. These computer modules were placed in cars as safety devices to gather information such as braking and speed, so as to be able to deploy the air bag at an appropriate time. They were not designed to gather any personal information nor designed or developed by the government to gather incrimination evidence from a driver. One cannot record communication of any kind on them. Indeed, they are not under the control of the individual driver at all."
>
> The trial court further held: "[Defendant] had no reasonable expectation of privacy in her speed on a public roadway or when and if she applied her brakes shortly before the crash. If a witness observed those actions and testified to them, the evidence would be admitted. If an expert in accident reconstruction testified to them, that evidence would be admitted. There is no difference in an electronic witness whose memory is much more accurately preserved, both to exonerate and implicate defendants."

Id. at 97.

The majority opinion maintains that *Diaz* inappropriately relied on *Smith v. Maryland*, 442 U.S. 735 (1979), and implies that *Jones* is the operative Supreme Court precedent for this issue. Actually, the *Diaz* opinion discusses *Jones* at some length, noting that the Supreme Court decision was based "on the common law theory of trespass in placing the GPS on the defendant's personal property, combined with the police attempt to obtain information," and the "trespass theory underlying *Jones* has no relevance [in this SDM search case] and, as the trial court aptly pointed out, the purpose of the SDM was not to obtain information for the police." *Diaz*, 153 Cal. Rptr. 3d at 101. The majority in the instant case suggests that the *Jones* opinion's reliance on this trespass theory when it could have relied on the *Smith* theory means that *Smith* is no longer binding precedent. But the fact that the Supreme Court chose to resolve *Jones* on the narrower trespass grounds rather than to wade into the waters of voluntary conveyance of information from *Smith* means only that

trespass is *a* viable Fourth Amendment consideration, not that trespass is the *only* consideration remaining.

Furthermore, in *Jones*, the government placed a GPS tracking device on the defendant's car to monitor the vehicle's movement *and location*. *Jones*, 565 U.S. at 403. By contrast, an EDR is installed on vehicles before they are sold/leased to a driver and the purpose is not to track the vehicle's location or route. Moreover, although the EDR is placed under the vehicle and most vehicle owners and drivers are unaware that there is such a black box attached to the vehicle, there is no attempt on the part of the government to secretively attach the EDR and have it record this information. Unlike the situation in *Jones*, the attachment of the EDR is not directed at any individual; as noted in the majority opinion, "[a]pproximately 96% of cars manufactured since 2013 are equipped with event data recorders" and they are installed prior to the conveyance of the vehicle to any individual.

Finally, I take issue with the majority opinion's holding that the Driver Privacy Act of 2015 "enhances the notion that there is an expectation of privacy in information contained in an automobile data recorder." What actually happened is that Congress took note that most vehicles were being sold with EDRs installed by the manufacturer; it determined that the data collected may be sensitive and/or private but not to the extent that extraction of this data by the government would be limited by the Constitution; and it thus chose to fill the void, just as seventeen state legislatures had previously done. Filling the void, where authorized by the Constitution, is a power properly delegated to the legislature, not the judiciary.

Conclusion

The data that the government extracted from the vehicle that was owned and driven by Appellee in this case was not information for which Appellee or any other owner/driver had a reasonable expectation of privacy. The data was not personal to Appellee, was not password protected by Appellee, and was not being collected and maintained solely for the benefit of Appellee. The EDR was installed by the vehicle's manufacturer at the behest of the National Highway Traffic Safety Administration and, as distinct from *Jones*, the purpose of the data collection is highway and driver safety. *See New York v. Class*, 475 U.S. 106, 113 (1986) ("[A]utomobiles are justifiably the subject of pervasive regulation by the State [and e]very operator of a motor vehicle must expect the State, in enforcing its regulations, will intrude to some extent upon that operator's privacy.").

Accordingly, as the extraction of data from the vehicle's EDR in the instant case was not a search or seizure protected by the Fourth Amendment, I would reverse the trial court's suppression of this evidence. Thus, I respectfully dissent.

* * *

Not final until disposition of timely filed motion for rehearing.