IN THE SUPREME COURT
STATE OF GEORGIA

VICTOR MOBLEY,	:	Petition No. S18G1546
Defendant–Appellant,	:	On Writ of Certiorari to the Court of Appeals of Georgia in A18A0500
v.	:	
THE STATE,	:	
Plaintiff–Appellee.	:	

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF GEORGIA, AND RIANA PFEFFERKORN IN SUPPORT OF APPELLANT SEEKING REVERSAL

Sean J. Young
Kosha S. Tucker
ACLU OF GEORGIA FOUNDATION
P.O. Box 77208
Atlanta, GA 30357
Email: syoung@acluga.org

Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Email: nwessler@aclu.org

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94114-4805
Email: jgranick@aclu.org

Counsel for Amici Curiae

Riana Pfefferkorn
559 Nathan Abbott Way
Stanford, CA 94305
Email: riana@law.stanford.edu

Pro Se

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU of Georgia is the Georgia affiliate of the national ACLU. The ACLU and ACLU of Georgia have long been at the forefront of efforts to protect and defend the Constitution, and the Fourth Amendment in particular. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts in numerous cases implicating Americans' right to privacy, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and as amicus in *United States v. Jones*, 565 U.S. 400 (2012), and *Riley v. California*, 573 U.S. 373 (2014). The ACLU of Georgia advocates on behalf of more than 20,000 members and supporters in Georgia.

Amica Riana Pfefferkorn is the Associate Director of Surveillance and Cybersecurity at the Center for Internet and Society ("CIS"), a public interest technology law and policy program at Stanford Law School. She appears in her personal capacity only and does not represent CIS, Stanford Law School, or Stanford University. A key part of Pfefferkorn's work at CIS involves researching novel forms of electronic data-gathering and surveillance by governments.

SUMMARY OF ARGUMENT

In *Riley v. California*, the United States Supreme Court held that the Fourth Amendment generally requires law enforcement to obtain a warrant before the digital data on a cell phone can be searched, even when the phone has been seized incident to a lawful arrest. The Court found that such digital data implicates substantial privacy interests, given that cell phones' "immense storage capacity" mean that the devices contain "a digital record of nearly every aspect of [the owners'] lives—from the mundane to the intimate," including "someone's specific movements down to the minute." 573 U.S. 373, 393 (2014). And the Court recognized that new technological realities are not automatically governed by decades-old Fourth Amendment frameworks, which could not possibly have accounted for the digital revolution. *See id.* at 386 (rationale behind older Fourth Amendment cases concerning "physical objects" does not have "much force with respect to digital content").

This case involves the question whether the reasoning of *Riley* as applied to digital data on cell phones also applies to the digital data stored in a vehicle's many computer systems, including event data recorders ("EDR"), that are now standard features in nearly every car. The answer is yes.

The massive amount of digital data contained in car computers implicates substantial privacy interests. Though many may not realize it, these computers can

and will contain unique digital records that track nearly every aspect of one's driving, including a car's specific movements, GPS location, steering input, speed, engine throttle and other detailed measurements down to the millisecond. Increasingly, such computers can even record the size and number of passengers, the music they are listening to, texts being exchanged, and private conversations. In sum, eyeballing a car wreck, which may be done without a warrant because it is public, does not implicate the same privacy interests as electronically excavating a car's extensive digital data. "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 573 U.S. at 393. Physically searching a vehicle after a car wreck may not work "substantial additional intrusion on privacy," but "any extension of that reasoning to digital data has to rest on its own bottom." *Id.*

Moreover, there is no basis for allowing blanket warrantless searches of a car's digital data in response to a car accident, when the car has been already impounded or otherwise poses no risk of being taken out of the jurisdiction. For these reasons and more, this Court should hold that law enforcement must obtain a warrant before downloading or searching data contained on a vehicle's EDR or other onboard computers, absent exigent circumstances. This Court should also reaffirm its longstanding decision not to adopt a good-faith exception to the

exclusionary rule, because such an exception would run counter to the Georgia legislature's express intent in creating a statutory suppression remedy, and would threaten to substantially inhibit the development of Fourth Amendment law.

ARGUMENT

I. Cars Increasingly Generate Sensitive and Private Information about Drivers and Passengers.

Gone are the days when people could tune up their cars in their driveways, using nothing more than a torque wrench and a keen ear. Today's vehicles rely on increasingly complex electronics that are monitored by powerful computers embedded into the vehicle itself, i.e., "onboard" computers. As one observer notes, "[t]oday's car has the computing power of 20 personal computers, features about 100 million lines of programming code, and processes up to 25 gigabytes of data an hour."[1] Digital data generated whenever a person operates their car can be automatically recorded and stored in these onboard computers.[2] These devices' data collection and storage will inevitably increase as technology evolves.

At issue in this case is one of the simpler onboard computers, sometimes called an airbag control module ("ACM"), or event data recorder ("EDR"). Also known colloquially as a vehicle "black box," EDRs are currently one of the most ubiquitous vehicle data recording devices. While EDRs generally store only

[1] *What's Driving the Connected Car*, McKinsey & Co., Sept. 2014, https://mck.co/2DTms8L.
[2] *A Brief Explanation of CAN Bus*, Sewell Dev. Corp. (2019), https://bit.ly/2vEiwo1.

information from around the time of a vehicle crash, other onboard computers store far more volume and variety of information for far longer periods of time, some of it permanently.[3] As the technology develops, computers in future cars will contain an immense amount of sensitive, private data.

The "event" to which the EDR's name refers is usually a car crash. Despite its name, however, an EDR does not exclusively record data at the moment of a collision. Using a "circular buffer" technique, these devices continually collect a fixed quantity of data, overwriting the oldest measurement on its record with the newest measurement, in perpetuity.[4] When the EDR detects a crash, it stops overwriting old measurements and retains the data it has recorded. The product is a multi-dimensional record of what the car—and its driver—were doing in the moments just before, during, and after a crash. In other words, EDRs are capable of telling a precise story about a car—and its driver and its passengers—by recording and storing a brief history of the car's operation and its various electronic and mechanical systems.

EDRs were first developed in the 1970s for a more limited purpose: so that car manufacturers could measure the effectiveness of airbags in collisions.[5] This is why they were initially called airbag control modules or ACMs, as they are

[3] Joel Eisenbaum**,** *What Information Is Being Stored on Vehicle Infotainment Systems?*, Click2Houston, July 26, 2017, https://bit.ly/2J3YR9H.
[4] Thomas Kowalick, Fatal Exit: The Automotive Black Box Debate 365 (IEEE Press 2005).
[5] *Black Box 101: Understanding Event Data Recorders: All New Cars Have Some Form of EDR*, Consumer Reports, Jan. 2014, https://bit.ly/2x24nV2.

referred to in this case. The recording devices did not gain broad popularity until the late 1990s, when manufacturers began to place the computers in cars so that they could evaluate vehicle performance in crashes by other metrics.[6] Today's EDRs connect with a controller area network bus ("CAN Bus")[7] or other vehicle network system, alongside up to 100 distinct electronic control units ("ECUs").[8] Many of these distributed mini-computers, which are responsible for the cars' functionality and safety, feed data to the EDR. In recent years, manufacturers have equipped most cars with EDRs; in 2017, for example, "99.6 percent of new light vehicles sold were equipped with EDRs."[9]

In contrast to EDRs' initial limited purpose in the 1970s, EDRs today track far more sensitive information. In 2011, the National Highway Traffic Safety Administration ("NHTSA"), which regulates the EDRs that are in use, mandated that EDRs collect data on fifteen distinct "data elements," or vehicle features. These metrics include vehicle speed, engine throttle, driver safety belt status, and

[6] Off. of Reg. Analysis and Evaluation, Nat'l Ctr. for Statistics and Analysis, Nat'l Highway Traffic Safety Admin., *Final Regulatory Evaluation: Event Data Recorders*, I-1–2 (July 2006), https://bit.ly/2J4KfGU.
[7] A "bus" is a communication system that transfers data between components inside a computer, or between computers. *See Bus (Computing)*, Wikipedia, https://bit.ly/2NBw3ac (last visited May 7, 2019).
[8] William Rosenbluth, *Collecting EDR Data for Crash Investigations*, Forensic Magazine, June 10, 2010, https://bit.ly/2Y3kytQ.
[9] Civil Disturbance Intervention and Disaster Assistance, Air Force Dep't, 84 FR 2804, 2805 (Feb. 8, 2019).

airbag deployment, among others. 49 C.F.R. § 563.7 (a) (2011).[10] EDRs may also record vehicle dynamics, driver inputs, seatbelt status, and post-crash information, "such as the activation of an automatic collision notification (ACN) system,"[11] as well as steering input, stability control, and the physical size and position of people in the car. 49 C.F.R. § 563.7(b).

There is also a plethora of personal tracking data outside the EDR that is available for collection. The most common way to access EDR data is by connecting a crash data retriever to the OBD-II port in the car.[12] But when a data retriever is plugged into the OBD-II, the port is able to return information on numerous vehicle diagnostics in addition to the data stored directly on the EDR computer. This means that the OBD-II connection can reveal information about a car's Vehicle Identification Number, how long a car has been running,[13] warranties, insurance coverage, and even logs of places the vehicle has traveled.[14]

The OBD-II can retrieve even more sensitive data from the powerful internal computer networks that control many modern cars, which also communicate with the OBD-II. In today's cars, the CAN Bus is one of the most common and important of these networks. The CAN Bus is the vehicle's centralized computer

[10] NHTSA has also set minimum standards for the amount of time, relative to the instant of the crash, for which the EDR should retain data on any given data element. *Id*.
[11] Nat'l Highway Traffic Safety Admin., *Event Data Recorder*, https://bit.ly/2PNVi88.
[12] Rosenbluth, *Collecting EDR Data for Crash Investigations*.
[13] CSS Electronics, *OBD2 Data Logger: Easily Record Your Car Data*, https://bit.ly/2H4dRCf.
[14] Dan Collins, *How to Access and Understand Your Vehicles OBD-II Codes*, Car Bibles, Feb. 25, 2019, https://www.carbibles.com/access-obd-ii-codes/.

that allows other internal computers and ECUs to communicate with one another. For example, a car's GPS system requires speed measurements in order to function. The CAN Bus facilitates communication between the GPS system and ECUs in the car that measure speed.[15] This means that it is possible to use the OBD-II to gather information about how most computers in a car communicate with one another, from advanced features like GPS to mechanical measurements like speed pulse frames (how fast the car was traveling at particular points in time).

In an age where cars are essentially roving computers, there is virtually no limit to the data—about drivers' and passengers' whereabouts, communications, activities, and biometrics—that cars can contain.[16] Vehicle manufacturers currently sell cars that record a range of car location and movement data, including "[p]hysical location recorded at regular intervals," "[p]revious destinations entered into navigation system," "[l]ast location parked," "[d]irection/heading of travel," and "[d]istances and times traveled."[17] "Connected cars" are cars that are connected to the internet through a range of technologies, including GPS navigation, infotainment systems, stolen-vehicle recovery technologies, and telematics (discussed below). These features not only allow cars to queue a driver's Spotify playlist with their voice, or get turn-by-turn instructions to a passenger's

[15] *Definition of CAN Bus*, PCMag Encyclopedia, https://bit.ly/2ZWCQPe.
[16] Jaclyn Trop, *The Next Data Privacy Battle May Be Waged Inside Your Car*, N.Y. Times, Jan. 10, 2014, https://nyti.ms/2WraoD9.
[17] Senator Edward Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk* 8 (Feb. 2015), https://bit.ly/2ztmX7S.

favorite coffee shop, but also store and communicate information about these activities to insurers, dealerships, manufacturers,[18] companies,[19] and even other cars.[20]

Technology in the category of "telematics," which broadly describes any system that "enables wireless data communication" in a vehicle, means privacy concerns in new fleets of connected vehicles are even greater than in older model cars.[21] Telematics, in essence, is communication of sensitive personal information about drivers, passengers, and their cars to a third party. These technologies are often sold with a car as "features" by a spate of private companies, telecom entities and car brands. GM, for example, has introduced real-time driver feedback, which emulates an EDR. The new "performance data recorder" makes use of GPS and camera information, as well as more traditional data like gear and brake diagnostics, to give both drivers and GM real-time feedback on their driving.[22]

---

[18] Arun Ganesan, *Data Security and Privacy in the Connected Car Age*, ECN Magazine, Aug. 15, 2018, https://bit.ly/2KWu9Mf ("First, there's automakers who collect data for many reasons, but mainly to provide services for vehicle owners. Then there's the manufacturers of infotainment centers who scrape customer data through apps like GPS, music, or contacts. Finally, there are third parties that collect data through dongles that connect to a port in a car.").

[19] Brett Berk, *The Unending Struggle to Make Your Car Feel Like Your Phone*, Wired, May 13, 2017, https://bit.ly/2pS3IwH ("For example, by connecting the vehicle infotainment system to real-time location data, and pegging it to your daily calendar and commute, your to-do lists, your learned behavior—and vendor partners like Amazon, Starbucks, and Open Table—car companies can provide a myriad of push marketing opportunities reminding you to buy yourself a latte or suggest a route that takes you by a new lunch spot you might like.").

[20] Nat'l Highway Traffic Safety Admin., *Vehicle-to-Vehicle Communication*, https://bit.ly/2nPPNrJ.

[21] Welcome to Telematics.com (2017), https://www.telematics.com/.

[22] Trop, *The Next Data Privacy Battle May Be Waged Inside Your Car*.

Verizon offers a service called "Hum," which allows automakers to connect cars with drivers' smartphones. By combining data from the car, smartphone, and manufacturer, Hum can keep track of car diagnostics, ensure roadside assistance, and provide vehicle tracking.[23]

Microphone- and video-enabled onboard computers can collect and store intimate communications among riders.[24] News that home assistant devices like the Amazon Alexa, Google Home, or Cortana are collecting snippets of private conversations which are sometimes reviewed by manufacturer employees are fueling public concern about the privacy risks of these devices.[25] These worries apply just as well to modern onboard vehicle computers.[26]

The trend of collecting ever-more-detailed personal and driving information by car computers will only accelerate as manufacturers slowly transform connected cars into autonomous vehicles. In order to function, autonomous vehicles ("AVs")

---

[23] Hum, Verizon, https://vz.to/2nGexRy.

[24] *In the Matter of the Application of the United States For An Order Authorizing The Roving Interception Of Oral Communications*, 349 F.3d 1132 (9th Cir. 2003) (officers monitored conversation via onboard microphone, order ultimately struck down on appeal); *State v. Wilson*, No. 07CA56 (Ohio Ct. App. 2008) (officers monitored conversation through OnStar system); Jeff Plungis, *Who Owns the Data Your Car Collects?*, Consumer Reports, May 2, 2018, https://bit.ly/2UmgO5u ("But to make future self-driving cars safe and reliable, automakers need data—about the road, about driving habits, and about how drivers interact with each other. Companies such as Mobileye, which provides computer vision systems to BMW, Nissan, and Volkswagen, are helping carmakers to collect that data through the cameras embedded in cars that drivers own today.").

[25] Adam Clark Estes, *The Terrible Truth About Alexa*, Gizmodo, Apr. 27, 2019, https://bit.ly/2La6flO.

[26] Thomas Brewster, *Cartapping: How Feds Have Spied On Connected Cars for 15 Years*, Forbes, Jan. 15, 2017, https://bit.ly/2V3qNMp; Alex Davies, *How Amazon Taught the Echo Auto to Hear You in a Noisy Car*, Wired, Mar. 4, 2019, https://bit.ly/2EuwSeG.

rely on massive production and collection of data. That is because the computers that control AVs need that data to safely navigate the vehicle, and also to improve their autonomy through machine-learning techniques. As with EDRs, data that AVs collect will be expansive. Unlike EDRs, however, AVs will not restrict data recording to driving habits, nor to crash scenarios. At a minimum, AVs must use an extensive system of sensors to collect GPS coordinates, 360-degree video surrounding the car, and granular telemetry revealing speed, direction, and vehicle system functioning.[27] AVs are also likely to have the ability to record not only whether people enter and leave a car, but who those people are.[28]

Teslas, for example, which are starting to implement AV technology, have been revealed to store unencrypted personal data from paired devices and the cars' own cameras, sensors, and navigation services. One investigation revealed that, after a car crash, information from the crashed car leaked not just details about the

[27] *Self-Driving Cars Explained*, Union of Concerned Scientists, Feb. 21, 2018, https://bit.ly/2CI1wmo; Adrienne Lafrance, *How Self-Driving Cars Will Threaten Privacy*, Atlantic, Mar. 21, 2016, https://bit.ly/2V1DnM1 ("This level of data collection is a natural extension of a driverless car's functionality. For self-driving cars to work, technologically speaking, an ocean of data has to flow into a lattice of sophisticated sensors. The car has to know where it is, where it's going, and be able to keep track of every other thing and creature on the road. Self-driving cars will rely on high-tech cameras and ultra-precise GPS data.").

[28] John R. Quain, *Eyes on the Road! (Your Car Is Watching)*, N.Y. Times, Mar. 28, 2019, https://nyti.ms/2FP2Mo4 ("When fully autonomous vehicles begin circulating on public roads, designers note, they will have to be able to detect when people enter or exit a vehicle, [and] who the person is.").

crash, but also the driver's phone calls, text messages, and countless other personal pieces of information extraneous to the crash.[29]

AV manufacturers are moving to even more invasive technologies that scan peoples' eyes to measure engagement with surroundings on the road.[30] Cadillac's assisted driving technology, Super Cruise, will only work if the "driver attention system detects that the driver appears attentive."[31] AVs could also record the car occupant's private messages for the purpose of detecting their "emotional tone," which can supposedly determine the occupant's inebriation, injury, or even food preferences.[32]

Even when drivers become obsolete, as policy and industry experts alike expect will happen,[33] cars will still collect "reams of information" about passengers

[29] Kate Fazzini & Lora Kolodny, *Tesla Cars Keep More Data Than You Think, Including This Video of a Crash That Totaled a Model 3*, CNBC, Mar. 29, 2019, https://cnb.cx/2U5U2mi.
[30] Quain, *Eyes on the Road! (Your Car Is Watching)* (describing cameras that track the driver's eyes and head position as part of both the Super Cruise system in General Motors' 2018 Cadillac CT6 vehicle and the Extended Traffic Jam Assistant system in BMW's 2019 X5 sport utility vehicle).
[31] *Super Cruise Cadillac: Designed to Take Your Hands and Breath Away*, Cadillac, https://bit.ly/2Tg24V1.
[32] Quain, *Eyes on the Road! (Your Car Is Watching)* ("When fully autonomous vehicles begin circulating on public roads, designers note, they will have to be able to detect … if a person has become disabled (because of intoxication or a medical emergency)."); Lafrance, *How Self-Driving Cars Will Threaten Privacy* ("As for the lunch special, that really *is* a favorite restaurant of yours—but the car has never driven you there before. It knows your preferences because the vehicle has combed through your emails, identified key words, and assessed related messages for emotional tone.").
[33] Alex Davies, *The Wired Guide to Self-Driving Cars*, Wired, Mar. 13, 2018, https://bit.ly/2Ew1rQN.

using cameras and GPS in concert with more advanced technologies.[34] Cars' onboard computers, like the computers in modern smartphones, will increasingly contain information revealing an individual's private relationships, physical condition, location, and preferences. *See Riley*, 573 U.S. 373 (warrant required to search modern cell phones incident to arrest due to sensitive data stored on them).

II. Law Enforcement Access to Vehicle EDR Data is a Search for Which a Warrant is Required.

A. Downloading EDR Data is a Search.

Government agents conduct a search under the Fourth Amendment when they either (a) intrude on private property for the purpose of obtaining information, or (b) violate a person's reasonable expectation of privacy. *Florida v. Jardines*, 569 U.S. 1, 5 (2013); *United States v. Jones*, 565 U.S. 400, 404, 411 (2012). Either rubric provides an independent basis for concluding that downloading data from the EDR in a person's car is a search.

First, downloading data from an EDR intrudes on private property—both the vehicle and the data—for the purpose of obtaining information. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." As the United States Supreme Court has explained, "[i]t is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment." *Jones*, 565 U.S. at 404. When a

[34] Lafrance, *How Self-Driving Cars Will Threaten Privacy*.

police officer physically connects a device to a person's vehicle and uses that device to download data off of one or more of the vehicle's computer systems, the government has "physically occupied private property for the purpose of obtaining information." *Id.* Because "such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted," it continues to be a search today. *Id.* at 404–05; *accord Silverman v. United States*, 365 U.S. 505, 509–12 (1961) (intruding into a home by "even a fraction of an inch" by touching a "spike mike" to edge of a home heating duct in order to eavesdrop on conversations within the home constitutes a search).

Moreover, the EDR data itself is a "paper" or "effect" within the meaning of the Fourth Amendment. *See Carpenter v. United States*, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting) (explaining that digital data can constitute a person's "modern-day papers and effects"); *Riley*, 573 U.S. 373 (requiring warrant for searches of data stored on cell phones); *cf. United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (explaining that "Email is the technological scion of tangible mail," and therefore protected under the Fourth Amendment). Quite clearly, EDR data belongs to the person in possession of the car. *See, e.g.*, 49 U.S.C. § 30101 note (Driver Privacy Act of 2015) ("Any data retained by an event data recorder . . . is the property of the owner, or . . . lessee of the motor vehicle in

which the event data recorder is installed."). Therefore, government acquisition of the data is a search of that person's "papers" and "effects."

Second, accessing data in a car's onboard computer system is also a search because it impinges on the driver's reasonable expectation of privacy. "One who owns and possesses a car, like one who owns and possesses a house, almost always has a reasonable expectation of privacy in it." *Byrd v. United States*, 138 S. Ct. 1518, 1527 (2018). Therefore, the "privacy interests in an automobile are constitutionally protected." *California v. Carney*, 471 U.S. 386, 390 (1985). Moreover, people have a reasonable expectation of privacy in the contents of their computers and other digital storage media, both because of their possessory interest in those items, and because of the wide array of sensitive data electronic devices can contain. *See, e.g.*, *Riley*, 573 U.S. at 393–97 (reasonable expectation of privacy in contents of cell phone); *Henson v. State*, 314 Ga. App. 152, 157, 723 S.E.2d 456, 460 (2012) (explaining Fourth Amendment privacy interests implicated by searches of computers); *People v. Michael E.*, 230 Cal. App. 4th 261, 276, 278–79 (Cal. Ct. App. 2014) (reasonable expectation of privacy in data stored on a flash drive).

Contrary to these longstanding principles, the Court of Appeals below concluded that the Defendant lacked a reasonable expectation of privacy in the data from his vehicle's ACM because "there are outward manifestations of the

functioning of some of the vehicle's systems when a vehicle is operated on public roads. For example, a member of the public can observe a vehicle's approximate speed [and] observe whether a vehicle's brakes are being employed." *Mobley v. State*, 346 Ga. App. 641, 646, 816 S.E. 2d 769, 774 (Ga. Ct. App. 2018). In the court's view, "because an individual knowingly exposes such information to the public," he or she lacks a reasonable expectation of privacy in it. *Id.*

As a factual matter, the Court of Appeals was mistaken. "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." *State v. Worsham*, 227 So. 3d 602, 606 (Fla. Dist. Ct. App. 2017). No outside observer could reliably observe with computer-like precision "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," let alone all of that data ensemble. *Id.*; *see also* Mot. to Suppress Tr. at 56–58 (detailing data contained on Defendant's EDR); State's Trial Exh. 9 (attached to Bench Trial Tr.) (report of data extracted from Defendant's EDR).

And even if humans had the ability to know all of this detailed information simply by eyeballing a vehicle, which they do not, the United States Supreme Court has firmly rejected the proposition that mere exposure of a vehicle's or person's movements or activities to the public, by itself, vitiates a person's

reasonable expectation of privacy in equivalent information when gathered by a search of digital data. *Carpenter*, 138 S. Ct. at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere."); *see also Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in the judgment).

The constitutionality of a government search must be judged by whether the *method* by which the government actually obtained the information was lawful, not whether it could have obtained the same information legally from a different source or by different, lawful means. Police might, for example, "learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful." *Kyllo v. United States*, 533 U.S. 27, 35 n.2 (2001). The Supreme Court's decision in *Riley v. California*, which required a warrant for searches of cell phones incident to arrest, illustrates the point. The government argued in that case that police should at least be permitted to access call logs on a cell phone without a warrant, citing the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979). *Smith* "held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller" because people have no reasonable expectation of privacy in information (dialed phone numbers) voluntarily shared with a third party (the phone company). *Riley*, 573 U.S. at 400

(citing *Smith*, 442 U.S. at 745–46). The Court rejected the government's argument, holding that when police obtain call records through a search of the suspect's own cell phone, the Fourth Amendment requires a warrant, even if the same information properly could have been lawfully obtained without a warrant from another source. *Id*.

Likewise, in *Kyllo v. United States*, the Court held that law enforcement agents must obtain a warrant before using a thermal imaging device to learn facts about the interior of a home, even if the same information could be obtained in other permissible ways that do not require a warrant, "for example, by observing snowmelt on the roof." 533 U.S. at 35 n.2. The Court explained that "[t]he fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." *Id*. The D.C. Circuit similarly concluded in *United States v. Maynard* that "when it comes to the Fourth Amendment, means do matter." 615 F.3d 544, 566 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 565 U.S. 400. *Maynard* involved the prolonged GPS tracking of a suspect's car without a valid warrant. The court rejected the government's argument that because law enforcement agents could in theory have conducted uninterrupted visual surveillance of the suspect for 28 days, surreptitious GPS monitoring over that period did not implicate the Fourth Amendment. *Id.* at 565–66. The court applied the protections of the Fourth Amendment to the investigative means the

government actually used, and concluded that the prolonged GPS tracking violated the Constitution. *Id*. at 566–67. Numerous other courts have applied similar logic in a variety of circumstances. *See, e.g.*, *Commonwealth v. Almonor*, 2019 WL 1769556, at *5 n.11 (Mass. Apr. 23, 2019) (holding that real-time cell phone tracking is a search, and explaining that "the nature of the challenged governmental conduct -- i.e., what the government does -- has always been relevant to whether such conduct implicates reasonable expectations of privacy"); *United States v. Dzwonczyk*, 2016 WL 7428390, at *10 (D. Neb. 2016) (holding that remotely accessing a computer to obtain its internet protocol address is a search, and noting that "the Fourth Amendment inquiry requires an analysis not only of the information obtained, but more fundamentally, the means of obtaining it").

Had police learned Defendant's speed and other general facts by canvassing witnesses or analyzing skid mark data, he indeed would have lacked a reasonable expectation of privacy in the information revealed through those investigative techniques. But that is not what took place. As in *Riley*, the search here was of Defendant's own property—his car's onboard computer system and the data stored on it—in which he had both a property interest and a reasonable expectation of privacy. Under either or both these grounds, the police here conducted a search. The fact that police might properly have been able to obtain similar information by

some other lawful means does not vitiate the Fourth Amendment's protections applied to a search of Defendant's vehicle computer system itself.

B. The Vehicle-Search Exception to the Warrant Requirement Does Not Apply to Data Generated, Collected, or Recorded by ACMs, EDRs, or other Onboard Computers.

Where, as here, "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, [Fourth Amendment] reasonableness generally requires the obtaining of a judicial warrant. . . . In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley*, 573 U.S. at 382 (citations and quotation marks omitted). One of these exceptions is the so-called vehicle exception. That exception should not apply here. Though EDR data is generated by the operation of an automobile, digital data can be comprehensive, and searches of it are highly intrusive. Downloading or analyzing EDR data after a car crash is untethered from the purpose of the vehicle exception to the warrant requirement.[35]

1. Warrantless Car Searches Generally Require Probable Cause but Not Necessarily a Warrant Due to the Mobility and Extensive Regulation of Vehicles.

The United States Supreme Court has held that the search of an automobile can be reasonable without a warrant. *Carroll v. United States*, 267 U.S. 132 (1925). The Court explained that there is a difference between searching a building and

[35] Because the Court of Appeals found that there was no reasonable expectation of privacy in the EDR data, it did not address whether any exception to the warrant requirement applies. *Mobley*, 346 Ga. App. at 646.

searching an automobile because a "vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought." *Id.* at 153. So long as there was probable cause, the warrantless search could be constitutional. *South Dakota v. Opperman*, 428 U.S. 364, 387 (1976); *see also Carney*, 471 U.S. at 390; *Cooper v. California*, 386 U.S. 58, 59 (1967); *Chambers v. Maroney*, 399 U.S. 42, 51–52 (1970). Subsequent cases justified the automobile exception with the additional rationale that there is "pervasive regulation of vehicles capable of traveling on the public highways," resulting in "reduced expectations of privacy." *Carney*, 471 U.S. at 392.

However, under the Fourth Amendment, searches carried out pursuant to an exception to the warrant requirement "must be limited in scope to that which is justified by the particular purposes served by the exception." *Florida v. Royer*, 460 U.S. 491, 500 (1983). In *Collins v. Virginia*, for example, the United States Supreme Court refused to "[e]xpand[] the scope of the automobile exception" to permit warrantless entry onto the curtilage of a home in order to search a vehicle, because doing so "would both undervalue the core Fourth Amendment protection afforded to the home and its curtilage and untether the automobile exception from the justifications underlying it." 138 S. Ct. 1663, 1671 (2018) (citation and quotation marks omitted); *see also Arizona v. Gant*, 556 U.S. 332, 343 (2009)

(limiting application of the search-incident-to-arrest exception to automobiles in order not to "untether the rule from the justifications underlying" it).

Here, the State has argued that the automobile exception to the warrant requirement should be newly extended to searches of digital data in a vehicle's EDR. *See* Br. of Appellee (Ct. App.) at 10–12. It should not. *See Worsham*, 227 So. 3d at 606 (holding that warrant required for law enforcement access to vehicle's EDR). In *Riley v. California*, the United States Supreme Court made clear that traditional exceptions to the Fourth Amendment's warrant requirement do not automatically extend to searches of digital data, and that "any extension of [pre-digital] reasoning to digital data has to rest on its own bottom." 573 U.S. at 393. In determining whether a warrant exception applies to digital-age searches, the Constitution requires a balancing of individual privacy interests against legitimate governmental interests. *Id*. at 385–86. After conducting this balancing, the Court held in *Riley* that the search-incident-to-arrest exception does not apply to cell phones for two reasons: first, individuals have unique privacy interests in the contents of cell phones; and second, warrantless searches of cell phones are not sufficiently "tethered" to the underlying rationales for the search-incident-to-arrest exception because they are not necessary to ensure officer safety or preserve evidence. *Id.* at 386.

Applying this balancing test to searches of vehicle EDRs likewise leads to the conclusion that a warrant is required. As discussed below, the privacy interests in the digital data stored in vehicle EDRs and other onboard computers are enormous. Such privacy interests far outweigh the police's interest in immediately downloading EDR data, without a warrant, at the scene of an accident, where the vehicle will be impounded and thus poses no risk of being driven out of town.

2. The Privacy Interests in Vehicle EDRs are Unique.

Drivers' privacy interests in the contents of their vehicles' onboard computers, including EDRs, are high. The devices record granular data reflecting moment-to-moment details about the driving of the car including, at a minimum, vehicle speed, engine speed, brake status, throttle position, engine RPMs, status of driver's seatbelt, status of brake switch, rate of deceleration, and other data. Mot. to Suppress Tr. at 56–57. Given the range and precision of the data, "[t]hese recorders document more than what is voluntarily conveyed to the public." *Worsham*, 227 So. 3d at 606. "Because the recorded data is not exposed to the public, and because the stored data is so difficult to extract and interpret, . . . there is a reasonable expectation of privacy in that information." *Id.* [36]

[36] "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. The downloaded data must then be interpreted by a specialist with extensive training." *Worsham*, 227 So. 3d at 606.

"Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements [and activities] were limited by a dearth of records and the frailties of recollection." *Carpenter*, 138 S. Ct. at 2218. With access to EDR data, however, "the Government can now travel back in time" to recreate facts that were not otherwise observed. *Id.* Because virtually every car sold today contains an EDR, "this newfound tracking capacity runs against everyone," *id.*, magnifying the Fourth Amendment concerns.

EDR data has little in common with the things police might previously have found during a traditional search of a car. In *Riley*, the Court explained that "[b]efore cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. . . . But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones" because of the incredible volume and variety of information they contain. 573 U.S. at 393–94. Thus, allowing warrantless searches of cell phones fails to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 138 S. Ct. at 2271 (alteration in original).

The same is true of the data generated and stored by EDRs. Car searches have traditionally involved inspecting the passenger and storage compartments of

the vehicle and any containers found therein. *United States v. Ross*, 456 U.S. 798, 817–22 (1982). By necessity, this exercise was "limited by physical realities," *Riley*, 573 U.S. at 393. Prior to the digital age, cars could carry only as many persons, papers, and effects as could fit in the trunk, glovebox, and seats. Today, however, cars can contain data that would never have been found during a physical search of these areas, both because digital storage space is capacious and cheap, and because the types of information found on EDRs—millisecond-to-millisecond data about the functioning and activities of the car itself, *see* State's Trial Exh. 9 (attached to Bench Trial Tr.) at 8, 9, 12–14 (report of data extracted from Defendant's EDR)—simply could not have been recorded and stored with anything close to the granularity and volume that computerized storage allows. Any attempt to approximate this automated data recordation would quickly fill a car with paper, should this be possible at all.

EDRs are one subset of the extensive computer systems contained in virtually every car sold today. Like cell phones, vehicle computers now and in the future "differ in both a quantitative and a qualitative sense from other objects that might be kept" in a person's car. *Riley*, 573 U.S. at 393. For one, these computers have an "immense storage capacity." *Id*. They "collect[] in one place many distinct types of information . . . that reveal much more in combination than any isolated record. [And vehicle computers'] capacity allows even just one type of information

to convey far more than previously possible." *Id.* at 394. The data stored in vehicle computers is manifold, ranging from location and travel history, to cell phone contact lists and call history. *See supra* Part I. Each of these types of data merits the Fourth Amendment's full protection against warrantless search. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2220 (warrant required for historical cell phone location data, even when it is held by a service provider rather than on a person's own phone); *Riley*, 573 U.S. at 400, 403 (warrant required to search contents of cell phone, including location history, call logs, and contact lists); *Jones*, 565 U.S. at 428–31 (Alito, J., concurring in the judgment) (applying Fourth Amendment protections to GPS location data for a car, and expressing concern with the privacy implications of "cars that are equipped with devices that permit a central station to ascertain the car's location at any time").

Today's advanced connected cars can collect nearly a *gigabyte* of data per second.[37] While estimates vary, that is approximately equivalent to more than 500,000 pages of text per second.[38] Some of this data will be transmitted to remote "cloud" servers, but much of it will also be stored locally by onboard computers in the car.[39] And the coming proliferation of cars operated in full or in part by artificial intelligence systems, including automated vehicles, will rely on the

[37] Martin Booth, *What's Driving Automotive Storage?*, Elec. Eng'g Times, May 30, 2017, https://ubm.io/2JsfM5l.
[38] Doug Austin, *eDiscovery Best Practices: the Number of Pages in Each Gigabyte Can Vary Widely*, CloudNine, July 31, 2012, https://bit.ly/2Y5HDfu.
[39] Tom Coughlin, *The Memory of Cars*, Forbes, July 20, 2016, https://bit.ly/2Y6Tie7.

collection and processing of extraordinary quantities of sensitive data, including location data, recorded video feeds, and occupants' biometric data. Experts estimate that autonomous vehicles will generate and consume roughly 40 terabytes of data for every eight hours of driving.[40] One terabyte of data constitutes approximately 130,000 digital photos.[41] And because vehicle computer systems are interconnected and the data on them is constantly intermingling, access to an EDR risks obtaining data far beyond the more limited set of information that the EDR is supposed to contain. *See supra* Part I. This volume of sensitive data should not be left vulnerable to warrantless search.

Even if the court views the data obtained from the EDR in this case as not particularly sensitive, it should still hold that a warrant is required. Police cannot know, in advance, how extensive, granular, and revealing the data downloaded from a vehicle will be. Therefore, the rule this court adopts "'must take account of more sophisticated systems that are already in use or in development.'" *Carpenter*, 138 S. Ct. at 2218–19 (quoting *Kyllo*, 533 U.S. at 36). A bright-line rule requiring a warrant is the only cohesive way to comply with the United States Supreme Court's "preference to provide clear guidance to law enforcement through categorical rules." *Riley*, 573 U.S. at 398. Any other outcome would "launch courts

[40] Patrick Nelson, *Just One Autonomous Car Will Use 4,000 GB of Data/Day*, Network World, Dec. 7, 2016, https://bit.ly/2H6XJA4.
[41] Tim Fisher, *Terabytes, Gigabytes, & Petabytes: How Big Are They?*, Lifewire, Jan. 7, 2019, https://bit.ly/2RZqkKd.

on a difficult line-drawing expedition," necessitating case-by-case evaluation based on the particular data obtained from each make, model, and year of car. *Id.* at 401. The Supreme Court drew such a bright line in *Riley*, where it was presented with warrantless searches of two defendants' phones: a modern smartphone, on which police viewed a range of data including videos and text files; and an older model "flip phone," on which police merely "pressed one button on the phone to access its call log, then another button to determine the phone number associated with the 'my house' label." *Id.* at 380. The Court rejected the government's fallback argument to require a warrant for the former search but not for the latter, rejecting the lack of clarity that such case-by-case evaluation would entail. *Id.* at 401. Instead, the Court provided a "simple" rule: "get a warrant." *Id.* at 403. The same rule is appropriate here.[42]

3. Warrantless Searches of Vehicle EDRs are Not Tethered to the Relevant Government Interests Underlying the Vehicle-Search Exception.

The second prong of the Fourth Amendment balancing test evaluates the governmental interests by considering whether warrantless searches of the category of property at issue are "tethered" to the narrow rationales justifying the warrant

[42] At a minimum, if this Court concludes that the warrantless search of the EDR in this case was reasonable under the Fourth Amendment, it should make clear that its ruling is a narrow one. As vehicle technology continues to advance, ever-more-sensitive and voluminous data is likely to be available to police with the push of a button. The Court should be alert to the danger of sanctioning warrantless searches of other kinds of data based on the particular facts of this case. *See Mobley*, 346 Ga. App. at 646–47.

exception. *Riley*, 573 U.S. at 386. Here, warrantless searches of EDRs and other vehicle computers are not justified by the limited purposes of the automobile exception. The exception is meant to account for the "'ready mobility' of vehicles," and for the "the pervasive regulation of vehicles capable of traveling on the public highways." *Collins*, 138 S. Ct. at 1669–70 (citations omitted).

The facts of this case ably demonstrate that warrantless searches of EDR data are not necessary to serve either purpose of the automobile exception. Where, as here, law enforcement is investigating a car crash to establish whether a driver was criminally culpable, there is no danger of the car under investigation driving away. Having secured the scene of the crash, police can apply for a warrant from the scene, or can tow the car to an impound lot and hold it there until the warrant is sought and issued. Thus, the "ready mobility of automobiles" is not an impediment to investigating a crash.

Nor does the "pervasive regulation of vehicles" justify warrantless searches of EDRs. For the reasons discussed above and set forth in *Riley*, the voluminous, sensitive, and private digital data in a car's EDR implicates the same strong privacy interests one has in a smartphone's digital data, regardless of the diminished expectation of privacy stemming from the regulation of vehicles. *See, e.g.*, *Riley*, 573 U.S. at 392 ("The fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture

entirely. . . . Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of . . . physical items"). Were it otherwise, police could search a vehicle's EDR during virtually any traffic stop, to obtain data revealing the car's speed, its braking pattern, whether it was driving straight or weaving, and much more that might serve as potential evidence of a traffic violation. Permitting the warrantless search of EDRs would threaten to turn every routine traffic stop into a digital dragnet. It would, after all, "be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any [traffic] crime could be found on" an EDR. *Riley*, 573 U.S. at 399.

The State may also argue that the automobile exception permits "the warrantless search of containers within an automobile." *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999) (emphasis omitted). But because EDRs reflect a constantly updating moment-to-moment account of the functioning of the car, treating an EDR as a mere static container subject to routine warrantless search would extend the logic of the automobile exception beyond its breaking point. *Cf. Riley*, 573 U.S at 397 ("Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained . . . .").

Finally, the process of getting a warrant is not unduly burdensome and will not impede the efficient investigation of a vehicle crash. If police have probable

cause to search an EDR, they may secure the vehicle while they prepare an application for a search warrant. Indeed, following the initial warrantless search, police did exactly that in this case, impounding the car and then securing a warrant for a search of the EDR. *See* State's Suppression Exh. 1 (attached to Mot. to Suppress Tr.) (Search and Seizure Warrant). Further, as the Supreme Court explained in *Riley*, "[r]ecent technological advances … have … made the process of obtaining a warrant itself more efficient." 573 U.S. at 401. Because warrants can be sought electronically and even by video conference, OCGA § 17-5-21.1, in cases like this one where the probable-cause showing is straightforward, the warrant can be sought and obtained quickly. *Riley*, 573 U.S. at 401; *Missouri v. McNeely*, 569 U.S. 141, 155 (2013). And in instances where there is truly no time to go to a judge, the exigent-circumstances exception may apply on a case-by-case basis. *See Riley*, 573 U.S. at 388.

A rule that permits warrantless searches of the data that happens to be saved on EDRs today risks enabling even more egregious warrantless privacy invasions in the future, as cars record ever more types and volumes of data. Should this Court decide otherwise, it should carefully limit its holding to the particular facts of this case, as the appellate court did. *Mobley*, 346 Ga. App. at 646–47. To do otherwise would put constitutionally protected sensitive and personal information at risk as onboard computers evolve.

III. *Gary v. State* Rightfully Declined to Adopt a Good-Faith Exception to the Exclusionary Rule.

The General Assembly's decision not to create a good-faith exception to the exclusionary rule ensures that egregious conduct will be remedied and encourages the development and clarification of Fourth Amendment law. This Court rightly decided *Gary v. State*, 262 Ga. 572, 658 S.E.2d 577 (1992), and there is no basis to overturn it.

A. This Court Rightfully Declined to Adopt the Good-Faith Exception to the Exclusionary Rule in *Gary v. State*, Because It Would Constitute Judicial Legislation.

When it decided *Gary*, this Court declined to adopt the good-faith exception to the exclusionary rule created by the United States Supreme Court in *United States v. Leon*, 468 U.S. 897 (1984), because Georgia already had a legislatively-mandated exclusionary rule found in OCGA § 17-5-30 that did not recognize such an exception. In other words, this Court correctly rejected the good-faith exception on statutory grounds, finding that the Georgia Legislature had elected to do as states are "free as a matter of [their] own law" to do: impose "greater requirements upon [the state's] law enforcement officers than that required by the U.S. Constitution, as interpreted by the U.S. Supreme Court." *Gary*, 262 Ga. at 574, 658 S.E.2d at 428 (citing *Oregon v. Hass*, 420 U.S. 714, 718 (1975)).

This Court found dispositive subsection (2) of OCGA § 17-5-30, which provides:

> A defendant aggrieved by an unlawful search and seizure may move the court . . . to suppress as evidence anything so obtained on the grounds that: . . . (2) The search and seizure with a warrant was illegal because the warrant is insufficient on its face, there was not probable cause for the issuance of the warrant, or the warrant was illegally executed.

OCGA § 17-5-30(a)(2). This Court interpreted that portion of the statute as "the legislature's unequivocal expression of its desire that evidence seized by means of a warrant that is not supported by probable cause be suppressed." *Gary*, 262 Ga. at 575, 658 S.E.2d at 428. The legislative intent behind this statutory exclusionary rule was clear, according to this Court:

> The legislature enacted this statute to protect against governmental disregard for constitutionally-protected rights by requiring the integral actors in the warrant-issuing process—the law enforcement officers who seek warrants and the members of the judiciary who issue warrants—to respect the probable cause requirements of the Georgia Constitution, and to carefully prepare and scrutinize applications for warrants.

Id. at 575 (internal citations omitted). Georgia, thanks to its legislature, holds true to what the "Framers of the Bill of Rights sought to accomplish through the express requirements of the Fourth Amendment": to "define precisely the conditions under which government agents could search private property so that citizens would not have to depend solely upon the discretion and restraint of those agents for the protection of their privacy." *Leon*, 468 U.S. at 948 (Brennan, J. and Marshall, J., dissenting).

Since *Gary*, this Court has reaffirmed its holding that Georgia law prohibits the application of the good-faith exception to the exclusionary rule, because to do

otherwise "would be tantamount to judicial legislation." *Gary*, 262 Ga. at 575, 658 S.E.2d at 429. *E.g.*, *Beck v. State*, 283 Ga. 352, 353, 658 S.E.2d 577, 579 (2008) ("Georgia does not recognize the good faith exception to its statutory exclusionary rule because our legislature has not provided one."); *Miley v. State*, 279 Ga. 420, 422, 614 S.E.2d 744, 745 (2005) ("Because Georgia law has no good faith exception regarding search warrant requirements, the lack of probable cause necessary for the warrant's issuance requires the suppression of the evidence."); *Harvey v. State*, 266 Ga. 671, 671–72, 469 S.E.2d 176, 177–78 (1996) (affirming the Court of Appeals' opinion, which found that "there is no 'good faith' exception in Georgia unless and until the legislature sees fit to adopt one," *Harvey v. State*, 217 Ga. App. 776, 778, 459 S.E.2d 433, 434 (1995)).

Likewise, the Georgia legislature has demonstrated its acceptance of this Court's interpretation of the law and the legislative intent behind the law, declining to amend or repeal its statutory exclusionary rule in OCGA § 17-5-30 in the more than 26 years since *Gary* was decided. This Court should therefore continue to regard Georgia's statutory exclusionary rule as a "legislative overruling of the judicially created good faith exception," *Brent v. State*, 270 Ga. 160, 162, 510 S.E.2d 14, 17 (1998), stay out of the "realm of the legislature," *Gary*, 262 Ga. at 576, and maintain this state's strict standards for protecting its residents against unlawful searches and seizures as is intended by Fourth Amendment.

B. A Good-Faith Exception Would Allow Egregious Conduct to Go Unremedied, Eroding the Boundaries of the Fourth Amendment and Stifling Potential Development of the Law.

Creating a good-faith exception not only invades the province of the legislature, it would allow egregious conduct to go unremedied and stifle the development or clarification of Fourth Amendment law. The exclusionary rule of the Fourth Amendment is intended to serve as a sanction, making evidence obtained through an illegal search inadmissible at trial. When law enforcement officers know that such a sanction awaits if they engage in an illegal search, they have an incentive to abide by the Constitution. However, a good-faith exception undermines this incentive, giving law enforcement officers a safe harbor for their errors and misconduct and leaving those who have suffered from unconstitutional police action without relief. A good-faith exception dilutes the exclusionary rule, emboldening officers to disregard constitutionally protected rights and discouraging people from even challenging illegal searches.

Since its inception, courts that apply the good-faith exception to the exclusionary rule have routinely failed to even reach the question of whether the Fourth Amendment was violated. *See*, *e.g.*, *United States v. Cherna*, 184 F.3d 403, 407 (5th Cir. 1999) ("If the good-faith exception applies, we need not reach the question of probable cause."); *United States v. Webb*, 255 F.3d 890, 905 (D.C. Cir. 2001) (holding that the good-faith exception applied no matter "what[ ] may be

said of the search warrant affidavit in this case"); *United States v. Koch*, 625 F.3d 470, 476–77 (8th Cir. 2010) ("We need not address [whether there was a Fourth Amendment violation] … because we conclude that the agents had an objective, good faith belief . . . that their search was legal.").

Inhibiting the development of Fourth Amendment law is particularly harmful in cases, like this one, involving law enforcement's exploitation of digital-age technologies to conduct searches. As the Sixth Circuit put it, "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." *Warshak*, 631 F.3d at 285. Such legal development is greatly slowed when the good-faith exception is allowed to preempt consideration of the Fourth Amendment's substantive protections in case after case.

Thankfully, this problem does not present itself in Georgia. Because the General Assembly has rejected the good-faith exception, Georgia courts still engage in meaningful judicial review of police conduct. For instance, in *State v. Burgess*, 2019 WL 1198613 (Ga. Ct. App. 2019), the Georgia Court of Appeals reversed the trial court's order denying the defendant's motion to suppress evidence obtained in a warrantless search of defendant's home, finding that the exclusionary rule applied to the search, despite the officers' reliance on a temporary protective order ("TPO") they believed gave them entry into the home.

The Court of Appeals reached the question of whether the Fourth Amendment was violated, dismissing the government's attempt to argue the good-faith exception, and making meaningful findings in the process about the multiple reasons why the police conduct was unconstitutional: absence of consent to the search, expansion of the search even beyond the very thing officers illegally relied upon (a TPO) as an invalid substitute for a search warrant, and the officers' failure to apply for a warrant. *Burgess*, 2019 WL 1198613, at *3–8.

Instead of skipping directly to good faith, Georgia courts reach the Fourth Amendment question because they must, and as a result, the Fourth Amendment still has the bite it is meant to have. In *Brown v. State*, 330 Ga. App. 488, 767 S.E.2d 299, 303 (2014), for example, the Georgia Court of Appeals reversed the trial court's decision denying the defendant's motion to suppress cell phone evidence obtained by a warrantless search, finding the search incident to arrest exception inapplicable under *Riley*, 573 U.S. 373, and finding the government's argument that officers "reasonably relied on existing caselaw" irrelevant under *Gary*. On the latter point, the Court of Appeals explained that "even if Georgia recognized the good faith exception, allowing this evidence to be admitted . . . would be inconsistent with fairness and the even-handed administration of justice." *Brown*, 330 Ga. App. at 493, 767 S.E.2d at 303. In arriving at that conclusion, the Court of Appeals in *Brown* seemed to recognize how the developments of Fourth

Amendment law under *Riley* would have been stunted under an application of the good-faith exception. *See id.* at 490–94, 300–04 (refusing to end its analysis at the government's good-faith argument and instead following the recent *Riley* decision, because to do otherwise "would treat similarly situated defendants differently.").

Similarly, this Court has rightly applied the protections of the Fourth Amendment in numerous cases and imposed the suppression remedy when it found a violation of the Amendment's requirements. *E.g.*, *Harper v. State*, 283 Ga. 102, 107, 657 S.E.2d 213, 217 (2008) (finding a Fourth Amendment violation "[b]ecause a warrant was required for the search . . . , because the warrant authorizing the search was issued without a showing of probable cause, because no exception to the warrant requirement has been shown, and because Georgia does not have a good faith exception to the search warrant requirement"); *Register v. State*, 281 Ga. App. 822, 824–25, 637 S.E.2d 761, 762–63 (2006) (finding a Fourth Amendment violation where officers, relying on an invalid arrest warrant, illegally searched defendant's car and obtained inadmissible evidence); *Boatright v. State*, 225 Ga. App. 181, 183–85, 483 S.E.2d 659, 662–64 (1997) (reaching the Fourth Amendment question, despite officers' good faith claim, and finding that the search and evidence obtained from it should be suppressed).

While some courts outside of Georgia continue to "expand[] the good faith exception to the point of eviscerating the exclusionary rule altogether," *United*

States v. Katzin, 769 F.3d 163, 187 (3d Cir. 2014) (en banc) (Greenaway, J., dissenting), this Court should continue to uphold its 26-year-old safeguard against unconstitutional police conduct: *Gary v. State*. In doing so, Georgia will be in good company, remaining aligned with the dozen state supreme courts that also have expressly rejected the good-faith exception.[43] As Georgia's and these states' experience shows, robust application of the exclusionary rule provides a clear and administrable rule for police and the public, and simultaneously honors the Fourth Amendment's critical purpose "to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214.

CONCLUSION

For the foregoing reasons, this Court should hold that in the absence of exigent circumstances, law enforcement must obtain a warrant before downloading or searching data contained on a vehicle's EDR or other onboard computers. Further, this Court should not create a good-faith exception to the warrant requirement under Georgia law.

[43] *State v. Marsala*, 579 A.2d 58, 59 (Conn. 1990); *Dorsey v. State*, 761 A.2d 807, 814 (Del. 2000); *State v. Guzman*, 842 P.2d 660, 677 (Idaho 1992); *State v. Cline*, 617 N.W.2d 277, 283 (Iowa 2000), abrogated on other grounds by *State v. Turner*, 630 N.W.2d 601 (Iowa 2001); *Commonwealth v. Upton*, 476 N.E.2d 548, 554 n.5 (Mass. 1985); *State v. Canelo*, 653 A.2d 1097, 1102 (N.H. 1995); *State v. Johnson*, 775 A.2d 1273, 1282 (N.J. 2001); *State v. Gutierrez*, 863 P.2d 1052, 1053 (N.M. 1993); *People v. Bigelow*, 488 N.E.2d 451, 458 (N.Y. 1985); *State v. Carter*, 370 S.E.2d 553, 562 (N.C. 1988); *Commonwealth v. Edmunds*, 586 A.2d 887, 888 (Pa. 1991); *State v. Oakes*, 598 A.2d 119, 121 (Vt. 1991). Illinois law precludes any good-faith exception when police lack a warrant. *People v. Krueger*, 675 N.E.2d 604, 606 (Ill. 1996). The Supreme Courts of two states have indicated, without expressly holding, that their constitutions preclude any good-faith exception. *State v. Lopez*, 896 P.2d 889, 902 (Haw. 1995); *Garza v. State*, 632 N.W.2d 633, 640 (Minn. 2001).

Respectfully submitted this 7th day of May, 2019,

/s/ Sean J. Young
Sean J. Young
Kosha S. Tucker
ACLU OF GEORGIA FOUNDATION
P.O. Box 77208
Atlanta, GA 30357
Email: syoung@acluga.org

Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Email: nwessler@aclu.org

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94103
Email: jgranick@aclu.org

Counsel for Amici Curiae

Riana Pfefferkorn
559 Nathan Abbott Way
Stanford, CA 94305
Email: riana@law.stanford.edu

Pro Se

CERTIFICATE OF SERVICE

This is to certify that I have this day served a true and correct copy of BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF GEORGIA, AND RIANA PFEFFERKORN IN SUPPORT OF APPELLANT SEEKING REVERSAL upon the parties by depositing same in the United States mail with proper postage affixed to ensure delivery and addressed as follows:

Sharon Lee Hopkins, Esq.
Assistant District Attorney
Flint Judicial Circuit
Second Floor, West Tower
One Courthouse Square
McDonough, GA 30253

Brandon A. Bullard
Appellate Division
Georgia Public Defender Council
104 Marietta Street, NW
Suite 600
Atlanta, GA 30303

This 7th Day of May, 2019.

/s/ Sean J. Young
Sean J. Young
ACLU OF GEORGIA FOUNDATION
P.O. Box 77208
Atlanta, GA 30357
Email: syoung@acluga.org

Counsel for Amici Curiae