Washington and Lee Journal of Civil Rights and Social Justice

Volume 21 | Issue 1 Article 11

9-2014

Putting the Brakes on Driver Privacy: Black Boxes, Data Collection, and the Fourth Amendment

Thayer Case
Washington and Lee University School of Law

Putting the Brakes on Driver Privacy: Black Boxes, Data Collection, and the Fourth Amendment

*Thayer Case**

Table of Contents

---

* Candidate for Juris Doctor, Washington and Lee University School of Law, 2015; B.A., cum laude, George Washington University, 2010. The author expresses her deepest thanks to Professor Lawrence Muir for sharing his wealth of knowledge and providing endless encouragement.

I. Introduction

In light of recent national dialogue concerning the National Security Administration's (NSA) use of spying, data collection, privacy, and civil liberties, it may come as no surprise that our vehicles are also tracking our movements and recording information that could be used against us in court. Regardless of whether this can (and perhaps should) be expected in the 21st century, it raises a disconcerting potential for infringement on privacy rights. Consumers and privacy advocates should be troubled by companies and the government having too much access to private information in the absence of clear guidelines about when and how this data can and will be used.

Most Americans are familiar with the "black box" in aircraft, which records data and sound continuously throughout a flight and can later be retrieved and played back in the event of an accident.[1] What most American car owners do not know is that approximately 96 percent of all new vehicles sold in the United States are also equipped with black boxes that record accident information.[2] Unlike black boxes in aircraft, drivers can rest

---

1. *See* Laurel Dalrymple, *What Would It Take To Destroy A Black Box?* NPR (Mar. 11, 2014), http://www.npr.org/blogs/thetwo-way/2014/03/11/289189214/what-would-it-take-to-destroy-a-black-box (explaining that aircraft have two black boxes; one which stores information on flight control and engine performance and another voice recorder, and that it is extremely rare for them to be destroyed).

2. *See* Martin Kaste, *Yes, Your New Car Has A 'Black Box.' Where's The Off Switch?* ALL TECH CONSIDERED: NPR (Mar. 20, 2013 4:46 PM), http://www.npr.org/blogs/alltechconsidered/2013/03/20/174827589/yes-your-new-car-has-a-black-box-wheres-the-off-switch (quoting Rep. Michael Capuano, D-Mass, stating "I don't think you'll find very many Americans who know these devices are in their cars"); *see also* Jaclyn Trop, *Black Boxes, in Most New Cars, Stir Privacy Concerns*, N. Y. TIMES, (July 22, 2013), http://www.bostonglobe.com/business/2013/07/21/black-boxes-cars-raise-privacy-concerns/VGaCyAgtTERx0D4njkPsFL/story.html (stating that approximately 96 percent of new vehicles sold in the United States have black boxes and that drivers who do not read the owner's manual thoroughly may not know their vehicle can capture and record their speed, brake position, seat belt use, and other data). *See also* Press Release, Nat'l Highway Traffic Safety Admin., U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety (Dec. 7, 2012) http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+

assured that the devices in their vehicles do not currently record audio or video,[3] although there is no guarantee that this will continue to be the case in the future. At minimum, automobile black boxes record brief events in the seconds before, during, and after a crash.[4] However, they also have the capacity to reveal information about drivers' habits, including where they go, how fast they travel, and even whether the driver and passengers have buckled up.[5] This information relates directly to finding fault in accident investigations.[6]

If a driver crashes his car into a tree and informs the police he was wearing a seat belt and driving within the speed limit, the police will help clear the scene and the driver will have to deal with his insurance company regarding the damages. If that vehicle is equipped with a black box, however, the speed of the car upon impact, the driver's acceleration or deceleration in the seconds before and just after impact, whether the air bag deployed on-time, and many other pieces of information relevant to an accident investigation may be recorded. The police can use this information to find fault and issue tickets.[7] Former lieutenant governor of Massachusetts, Timothy P. Murray, paid a $555 fine for driving more than 100 miles an hour and failing to wear a seat belt: the proof came from the silent witness in his own car.[8]

DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Saf ety [hereinafter NHTSA U.S. DOT Press Release] (stating that NHTSA estimates approximately 96 percent of model year 2013 passenger cars and light-duty vehicles are already equipped with EDR capability).

3. *See* NHTSA U.S. DOT Press Release, *supra* note 2 ("EDRs do not collect any personal identifying information or record conversations and do not run continuously.").

4. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *Welcome to the NHTSA Event Data Recorder Research Web Site*, http://www.nhtsa.gov/EDR (last visited Dec. 7, 2014) [hereinafter NHTSA Event Data Recorder] (discussing what EDRs record for NHTSA's purposes).

5. *See id.*; *see also* Phillip Swarts, *Is Your Car Spying on You? GPS Tracks 'Consumers,' Identity Theft at Risk*, THE WASHINGTON TIMES (Jan. 7, 2014), http://www.washington times.com/news/2014/jan/7/no-privacy-behind-the-wheel-your-car-might-be-spyi/?page=all (quoting an Electronic Privacy Information Center attorney, Alan Butler, who stated that "[EDR] data, if it was breached, could reveal a great deal of information about individual drivers . . . where they live, work and worship, among other things").

6. *See* Mary-Rose Abraham, *Is That a 'Black Box' in Your Car?* ABCNEWS (Feb. 22, 2010), http://abcnews.go.com/Technology/MellodyHobson/car-black-box-records-key-data/story?id=9814181 (noting the use of black box data is useful to law enforcement, insurance companies and accident reconstruction companies).

7. *See id.*

8. *See* Trop, *supra* note 2 (explaining that Murray had originally told the police he

The National Highway Traffic Safety Administration (NHTSA) recently proposed mandating black boxes in all new vehicles manufactured on or after September 2014.[9] NHTSA collects black box data after accidents and uses that information to develop more effective vehicle standards.[10] According to a NHTSA administrator, a broader black box requirement would "provide critical safety information that might not otherwise be available to NHTSA to evaluate what happened during a crash—and what future steps could be taken to save lives and prevent injuries."[11]

While automakers generally support NHTSA's efforts to make recording devices mandatory, consumer groups and privacy advocates are perpetually troubled by the prospect of the government gaining too much access to private information without limitation.[12] Auto manufacturers generally do not disclose to buyers information collected by black boxes, its uses or protections.[13] The result: most drivers are unaware that a silent witness in their car could, in the event of an accident, provide evidence in court to criminalize them.[14]

Americans have accepted the use of black boxes in aircraft but there remains a fundamental difference between boarding a commercial airline for a flight and stepping into one's own car to run some errands. Airplanes follow flight plans, are tracked by air traffic control, and flight manifests account for each person on board. Passengers choosing to fly commercial flights relinquish many privacy rights for the sake of safety, but are these

---

was wearing a seat belt and not speeding but according to the device in his car, he was driving more than 100 miles an hour and not wearing a seat belt).

9. *See* Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74,144 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571) (proposing a new safety standard mandating the installation of EDRs in most light vehicles manufactured on or after September 1, 2014); *see also* Request for Comment on Automotive Electronic Control Systems Safety and Security Notice, 79 Fed. Reg. 60574 n. 26 (noting that no final rule publication date has been established).

10. *See* NHTSA Event Data Recorder, *supra* note 4 (describing NHTSA's uses for black box information).

11. *See* NHTSA U.S. DOT Press Release, *supra* note 2 (quoting NHTSA Administrator David Strickland).

12. *See* Swarts, *supra* note 5 (quoting a Government Accountability Office representative discussing the concerns of privacy advocacy groups).

13. *See id.*

14. S*ee* Abraham, *supra* note 6 (noting that while automakers typically disclose the presence of an EDR in owner's manuals, some drivers still may not know they have an EDR in their vehicle).

same travelers equally willing to relinquish privacy rights in their own personal vehicles?

Complications ensue as data acquisition capabilities advance and converge with GPS data to remotely track drivers' locations.[15] Privacy concerns regarding the regulation of the information collected include: access, ownership, usage, accuracy, reliability, and post-accident security of the data. Without proper regulations, the conveyance of a driver's vehicle information can be sent to third parties without consent or used to commit identity theft, stalking, or surreptitious monitoring without their knowledge.[16] While citizens undoubtedly desire better-performing, safer vehicles, the quantity of data currently collected has the potential for abuse. The law needs to anticipate these technological issues before the data collection infringes on Americans' constitutional rights.

This Note examines the current legal framework governing the use of black boxes in automobiles. Part II distinguishes black boxes from other data capturing devices in automobiles and explains the capabilities of both, including storage of and access to the data—specifically who may access it and through what means. Part III sets forth the current federal and state provisions governing black boxes and discusses the legal consumer concerns regarding notice, ownership, consent, and privacy and how the federal guidelines fall short of necessary privacy safeguards. Part III also explores the potential Fourth Amendment implications of data collection from vehicles and its use by third parties as well as the use of black box data as evidence in civil and criminal trials. Part IV addresses pending federal legislation that will solve some, but not all, of the issues created by the recording and collection of vehicle data and anticipates what Americans might expect from the future as the prevalence of recording devices increases.

II. What is the Black Box?

Inconsistency plagues black box terminology; in the industry, it may be referred to as an event data recorder (EDR) or a sensing diagnostic module (SDM).[17] NHTSA uses the term, "event data recorder" and has

---

15. *See* Swarts, *supra* note 5 (noting that consumers' locations and other data are at risk of being leaked by companies running GPS and other automobile navigation systems).

16. *See id.*

17. *See* Gregg Laskoski, *NHTSA's Requirement: 'Black Box' Recorders in All U.S. Vehicles*, GASBUDDY (Sept. 13, 2014, 6:00 AM) https://blog.gasbuddy.com/posts/NHTSA-s-

defined it as "a device installed in a motor vehicle to record technical vehicle and occupant information for a brief period of time (seconds, not minutes) before, during and after a crash."[18] This Note will refer to "black boxes" or "EDRs" interchangeably, with the understanding that not all vehicles necessarily contain one physical box or device.

Black boxes in vehicles are not necessarily black or boxes. Rather, they comprise a network of separate components and the term "black box" refers to the function of recording certain data within a vehicle's system most often triggered by crash events.[19] In many advanced systems, dozens of interconnected electronic control units (ECUs) or electronic control modules (ECMs) can be found embedded in the body, doors, dash, roof, trunk, seats, wheels and many other parts of modern vehicles.[20] These individual components assist in vehicle management: sensing engine fuel levels, air bag system deployment, antilock brake system activation, roll stability, cruise control management, climate control management, pollution control, speed-controlled stereo volume, activating warning lights when necessary, and even sensing whether to pull seat belts tighter.[21]

General Motors pioneered EDR use in the mid-1970s in vehicles that were equipped with air bags, in order to better understand air bag responses during a crash.[22] By 1998, air bags were mandated in all new vehicles and

---

Requirement-Black-Box-Recorders-in-All-U-S-Vehicles/1715-583664-2635.aspx (noting the many names of Event Data Recorders, including "black boxes" and "sensing diagnostic modules").

18. *See* NHTSA Event Data Recorder *supra* note 4.

19. *See* John C. Glennon, *Event Data Recorders Explained*, CRASH FORENSICS.COM, http://www.crashforensics.com/automobiledatarecorders.cfm (last visited Jan. 2, 2014) (noting that "Black Box" is actually a descriptor of the recording function).

20. *Id*.

21. *See id.* (explaining how ECMs interact and the information they process); *see also* Nancy M. Erfle, *Learning to Live with Electronic Data Recorders*, 38 THE BRIEF 14 (2008) (describing the capabilities of some automobile models); *see also* Cheryl Balough & Richard Balough, *Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?*, 2013 A.B.A. BUS. L. TODAY 1 (2013) (describing the multiple points of entry into a car's computer system); *see also* Kaste, *supra* note 2 (noting how the car's safety system makes split-second decisions about various functions).

22. *See* Jim Travers, *Black Box 101: The Basics of Event Data Recorders*, CONSUMER REPORTS NEWS (Mar. 18, 2010, 1:50 PM), http://www.consumerreports.org/cro/news/2010/03/black-box-101-the-basics-of-event-data-recorders/index.htm (explaining that General Motors used a basic EDR on airbag-equipped models in the mid-1970s and downloaded the EDR data after the crash); *Black box 101: Understanding event data recorders* (Jan. 2014) http://consumerreports.org/cro/2012/10/black-box-101-understanding-event-data-recorders/index.htm; 84 AM. JUR. 3D 1 *Proof of Facts* § 10 (2005) (explaining that the impetus for the first EDR in automobiles was the development of the airbag).

as they became the norm, computer systems necessarily evolved to measure the acceleration forces involved in a crash and to electrically deploy the air bags.[23] Not surprisingly, vehicles became gradually more dependent on computers to run internal systems and manufacturers increasingly installed EDRs in their vehicles to perform a variety of operational and safety functions, including safety research.[24]

EDR systems have greatly advanced over the years and now have the capability to record many functions such as deceleration before and during a crash, engine throttle (how far the accelerator pedal was pressed), whether or not the brakes were applied, whether or not the driver was using a seat belt, frontal air bag deployment, and other data relevant to the moments immediately before, during, and after a crash.[25] Modern EDR systems are not limited to physical download and can transmit data over remote wireless networks, providing immediate safety information so that emergency personnel can respond directly to the scene of an accident.[26]

A. Use of EDR Data

NHTSA has been using information gathered from EDRs to support its crash investigation program for several years by collecting and analyzing EDR data from automobile accidents to determine causes and whether vehicles were operating properly just prior to an accident.[27] When NHTSA conducts crash investigations, the agency obtains permission from the

---

23. *See* Mark Joye, *Column: Big Brother or Big Savior? Here Comes the Black Box*, 16 S. CAROLINA LAWYER 38, 40 (Sept. 2004); *see also* Marjorie A. Shields, Annotation, *Admissibility of Evidence Taken from Vehicular Event Data Recorders (EDR), Sensing Diagnostic Modules (SDM) or "Black Boxes"*, 40 A.L.R. Fed. 595 (2013) (noting that every vehicle with an airbag has a control monitor which determines whether to deploy the airbags in a developing crash).

24. *See* Joye, *supra* note 23 (explaining the history of EDR devices).

25. *See* Jason Torchinsky, *Everything You Need To Know About The Black Boxes Coming To Your Next Car*, JALOPNIK.COM (Dec. 7, 2012, 2:45 PM), http://jalopnik.com/5966628/everything-you-need-to-know-about-the-black-boxes-coming-to-your-next-car (providing many examples of the capabilities of event data recorders).

26. *See* Event Data Recorders, 71 Fed. Reg. 50,998, 51,032 (Aug. 28, 2006) (to be codified at 49 C.F.R. pt. 563) (detailing how the data can expedite the dispatch of emergency services to the location of a crash, thus reducing morbidity and mortality of traffic crash victims); *see also* Balough & Balough, *supra* note 21 (adding that vehicle manufacturers are beginning to add Wi-Fi hot spots in vehicles).

27. *See* NHTSA Event Data Recorder, *supra* note 4 (stating that EDRs can provide valuable information to understanding crashes which can improve motor vehicle safety).

vehicle owner prior to downloading the EDR data.[28] According to NHTSA, personal identifying information about drivers is not collected.[29] NHTSA's findings are shared with manufacturers for designing safer vehicles, in line with NHTSA's mission to "[s]ave lives, prevent injuries and reduce economic costs due to road traffic crashes, through education, research, safety standards and enforcement activity."[30]

Only recently have EDRs come to the forefront of conversation due to NHTSA's proposed legislation mandating black boxes in every new vehicle by September 2014.[31] Industry experts believe that more vehicles equipped with EDRs will better help engineers and researchers understand how cars perform in the real world, outside test centers, and thus contribute to vehicle and passenger safety.[32] This information is allegedly only collected in the event of an accident but a deeper look into some manufacturer's privacy policies suggests that this may not be the case and that information sharing with third parties occurs for reasons other than promotion of safety research.[33]

Without on-board data recording, skid marks and any potential witness testimony comprise pre-crash information while post-crash information is centered on damage to the vehicles and the occupants' physical injuries. Vehicles equipped with EDR capabilities, however, can provide pre-crash information which includes, but is not limited to, seatbelt use, steering, speed, braking, ABS activation and environmental conditions.[34] During the

---

28. *See EDR Q&As*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. (Aug. 11, 2006), *available at* http://www.nhtsa.gov/DOT/NHTSA/Rulemaking/Rules/Associated%20Files/EDR_QAs_11Aug2006.pdf (recommending vehicle owners do not tamper or disable any vehicle safety system).

29. *Id*.

30. *NHTSA's Core Values*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *available at* http://www.nhtsa.gov/About+NHTSA/NH TSA's+Core+Values [hereinafter NHTSA's Core Values]. *See also* 77 Fed. Reg. 74,144 (Dec. 13, 2012) (giving an overview of EDR technology).

31. *See* Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74,144 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571) (proposing a new safety standard mandating the installation of EDRs in most light vehicles manufactured on or after September 1, 2014).

32. *See* Trop, *supra* note 2 (quoting Alliance of Automobile Manufacturers representative discussing the importance of EDRs in research and engineering).

33. *See infra* Part III.C.3 for a discussion of the likely possibility that more information is collected and used for a variety of purposes than what is expressed to consumers.

34. *See* AUGUSTUS CHIDESTER ET AL., RECORDING AUTOMOTIVE CRASH EVENT DATA,

crash, EDRs will record air bag activation time, change in speed, and location data.[35]

States are also beginning to test usage of EDR data for taxation: taxing drivers based on miles driven.[36] Federal and state-mandated gasoline taxes have existed for decades and are typically allocated for maintenance of road infrastructure.[37] As the fuel economy of modern vehicles improves[38] and, in some cases, when the car doesn't use any gasoline at all, the fair share that a new vehicle contributes toward the road infrastructure is reduced in comparison to an older vehicle with much higher fuel consumption. To circumvent this, a mileage fee is charged based on the number of miles driven and can be tracked using telematics.[39] The same systems insurance companies use to track drivers can be used to report mileage for taxation.[40]

NAT'L TRANSP. SAFETY BD. (May 5, 1999), http://www.nhtsa.gov/cars/problems/studies/record/chidester.htm (providing tables that show data which can be collected from vehicles equipped with enhanced on-board recording capability).

35. *Id.*

36. *See* Evan Halper, *A Black Box in Your Car? Some See a Source of Tax Revenue*, L.A. TIMES (Oct. 26, 2013), http://www.latimes.com/nation/la-na-roads-black-boxes-20131027,0,6090226.story#axzz2ixCo2VOR (explaining that since Americans are buying less gas because cars now get more miles to the gallon, politicians are looking to other ways to tax driving instead of continuing to raise gas prices). The concept for tracking and taxing commercial trucks, at least, has already been in use in Germany and New Zealand for many years. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-77, HIGHWAY TRUST FUND: PILOT PROGRAM COULD HELP DETERMINE THE VIABILITY OF MILEAGE FEES FOR CERTAIN VEHICLES, at 19 (Dec. 13, 2012), *available at* http://www.gao.gov/products/GAO-13-77 (explaining that the commercial truck user fee systems in Germany and New Zealand show considerable revenues and other benefits can be achieved but that enforcing compliance in a cost-effective manner presents trade-offs).

37. *See* Kelly Phillips Erb, *Federal Gas Tax Passes Another Milestone: What Is The Future?,* FORBES (June 6, 2013, 8:48 AM) (explaining the impetus in the 1950s of the highway trust fund to pay for roads and maintenance).

38. *See* Bill Vlasic & Jaclyn Trop, *Vehicle Fuel Efficiency Reaches a High, Nearing Goal for 2016*, N.Y. TIMES (Sept. 10, 2013) (pointing out the advancements in fuel-efficient vehicles and noting that consumers are interested in purchasing fuel-efficient vehicles).

39. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-77 *supra* note 36 (introducing a mileage-fee system called "True Mileage" and noting that people would be more open to the concept if the device did not track speed or location).

40. *See* John Pearley Huffman, *The Taxman Driveth: In the Future, Your Car May Rat You Out to the Tax Collector*, CAR AND DRIVER, Feb. 2014, at 22 (explaining how Progressive Insurance's "Snapshot" works by recording how the vehicle is operated, including miles driven during a 30-day period, and that this can be used to report mileage for taxation).

B. Other Data Capturing Devices

Black boxes are not the only means of collecting information about drivers. For the last two decades, vehicle manufacturers have been installing luxury systems and enhanced safety features in vehicles which coincidentally provide opportunities for remote-access to vehicle data and consumer information. Newer vehicles often have GPS device capability built in, providing customers with hands-free access to emergency services, vehicle diagnostics, navigation applications, turn-by-turn directions, and traffic information.[41] Some services even offer remote ignition block and remote deceleration in the event of vehicle theft.[42] When drivers use mobile phones to access GPS technology or use their in-car GPS systems, this information is often collected and shared with third-party marketers and the companies providing the luxury features.[43]

Insurance companies provide incentives for customers to use devices that track their driving habits—promising better drivers better rates.[44] Progressive Auto Insurance, for example, uses a device it calls "Snapshot" which tracks driver behavior and sends the data over a cellular signal to the insurer.[45] The Snapshot device even beeps when drivers make an unwise maneuver.[46]

---

41. *See id.* (explaining the rush for vehicle manufacturers to add new Wi-Fi functions as selling points); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-81, IN-CAR LOCATION-BASED SERVICES: COMPANIES ARE TAKING STEPS TO PROTECT PRIVACY, BUT SOME RISKS MAY NOT BE CLEAR TO CONSUMERS, at 11 (2013), [hereinafter GAO REPORT], *available at* http://www.gao.gov/assets/660/659509.pdf (discussing companies which collect location data from vehicles to provide turn-by-turn directions, traffic information, and other services to customers as well as third-party companies).

42. Balough & Balough, *supra* note 21.

43. GAO REPORT, *supra* note 41, at 2 (finding that a company review of the privacy of location data collected by mobile devices did not consistently follow industry-recommended privacy practices).

44. *See* Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U.L. REV. 1153, 1154 (Summer 2011) (describing how insurance companies use devices that record geographic location, minute-by-minute speeding violations, and seat belt usage); *see also* John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, N.Y. TIMES, Mar. 9, 2011, http://www.nytimes.com/2011/03/10/business/10hack.html?_r=0 (providing examples such as General Motors' OnStar, Toyota's SafetyConnect, Ford's Sync, BMW's Assist, and Mercedes Benz's Mbrace).

45. *See* Progressive Auto Insurance, *available at* http://www.progressive.com/auto/snapshot/ (last visited Nov. 27, 2013).

46. *Id*.

Transponders, like EZ-PASS, have been known to be used for data collection research and may allow law enforcement to gather information transmitted about vehicle locations.[47] All of these built-in "smart" technology features produce a trove of information that can easily be sold to third party marketers, companies, and agencies.

C. Access and Storage

Black boxes must capture and record data elements for events in accordance with federal regulations.[48] The data elements are stored within the vehicle and can only be accessed with vehicle-specific equipment.[49]

Each car manufacturer has its own mechanisms for collecting, storing, extracting, and using data from in-vehicle recording devices.[50] After all, manufacturers initially installed black boxes for safety reasons and the data was not initially intended for use either by consumers or third parties.[51] While it is likely more convenient for each manufacturer to have their own black box design and methods of access, the lack of standardization complicates accident investigations.[52] The data available depends on the year, make, and model of the vehicle and extraction of such data normally requires a technician with physical access to the vehicle.[53]

---

47. *See* Detroit News Washington Bureau, *Carmakers keep data on drivers' locations*, 2014 WLNR 462895 (Jan. 7, 2014) (explaining that EZ-PASS can be used by law enforcement as well as for research).

48. *See* Event Data Recorders, 49 C.F.R. § 563.9 (2014) (setting forth the requirements for data capture).

49. *See* Travers, *supra* note 22 (explaining that special tools are required to access captured EDR data); *see also* Abraham, *supra* note 6 (pointing out that retrieval of data requires special software to collect speed, engine rpm, brake and throttle data, and more).

50. *See* GAO REPORT, *supra* note 41, at 25 (reporting that there is no consensus among major automakers, each of whom has differing policies about how much data they collect and how long they keep it); *see also* Susan Kuchinskas, *Making the Most of the App Opportunity, Part II*, TELEMATICS UPDATE (June 17, 2013), http://analysis.telematics update.com/infotainment/making-most-app-opportunity-part-ii. (stating that according to the head of consumer applications for ALK Technologies, an American company and global leader in GeoLogistics and navigation software, "[a]uto vendors like to keep control over the customer and the customer experience").

51. *See* Kaste, *supra* note 2 (quoting accident reconstruction specialist Dave Wells saying "[blackbox] was never designed for investigative purposes . . . [i]t was designed for . . . motor vehicle safety and keeping people less injured and alive").

52. *See id.*

53. *See* Dorothy J. Glancy, *Column: Retrieving Black Box Evidence from Vehicles: Uses and Abuses of Vehicle Data Recorder Evidence in Criminal Trials*, 33 CHAMPION 12,

Some domestic and import manufacturers allow third party suppliers to make tools available to investigators to access the data but others make the data harder to obtain.[54] Toyota, for example, has garnered criticism for restricting access to their vehicles' black box data; the company has only one laptop in the United States capable of downloading data from its black boxes.[55] In a case discussed later in this Note, local police authorities were initially unable to download data from a security vehicle involved in a motor accident and, in order to complete the investigation, had to wait several days for a private crash reconstructionist who had the appropriate tools for downloading the module's data.[56]

Manufacturers ensure that EDR data can be retained, even when disconnected from a power source or after a significant crash, or fire, rendering the ignition non-operational.[57] If air bags have deployed, the EDR data is frozen and can be removed from the vehicle so that the data can be downloaded.[58] Many EDRs also record *potential* crash situations where the air bags do not deploy.[59] Storage of potential or pre-crash data occurs in

---

13–14 (May 2009) (describing what information is recorded by automobile black boxes and that access can be obtained through a port in the vehicle).

54. *See* Travers, *supra* note 22. General Motors and Ford Motor Co., for instance, allow outsiders to access EDR data by purchasing a $25,000 reader. *See id.* Toyota has been criticized for how difficult it is to access their black box data; the company releases crash data only under a court order or at the request of NHTSA. *Id*. Furthering that, Toyota said the company only had one laptop in the United States that was capable of downloading data from its black boxes but that Toyota "pledged to make more available to officials soon." *Id.* It seems ironic that Toyota has been singled out after the well-known 2009–2011 Toyota vehicle recalls due to brake problems. *See* Hiroko Tabuchi, *1.5 Million Toyotas Recalled for Brake and Fuel Pump Problems*, N.Y. TIMES (Oct. 21, 2010), http://www.nytimes.com/2010/10/22/business/global/22toyota.html?_r=0 (reporting on the Toyota Motor Company announcement of a global recall of 1.53 million vehicles due to brake and fuel pump problems).

55. *See* Travers, *supra* note 22 (furthering that the company releases crash data only under a court order or at the request of NHTSA but that Toyota "pledged to make more available to officials soon."); *see also* Tabuchi, *supra* note 54.

56. *See* Kirsch v. State, 276 S.W.3d 579, 588 (Tex. Crim. App. 2008) (quoting the relevant findings from the trial court); *see also infra* Part III.C.3.

57. *See* Joye, *supra* note 23 (noting that non-volatile electrically erasable programmable read-only memory (EEPROM) technology was first used in electric odometers that saved the vehicle's cumulative mileage even when the battery was disconnected).

58. *Id*. (explaining how EDR data is retrieved from a vehicle).

59. *See* Glancy *supra* note 53, at 14 (noting that "[a]lmost no one, outside the vehicle manufacturer and regulation communities, is aware that *pre-crash* data is recorded") (emphasis added).

situations such as making sudden stops or bounces, rapid speed changes, or sharp turns to avoid obstacles in the road.[60] Thus, many erratic movements that may very well be necessary to avoid collisions are recorded. Storage of pre-crash data is limited to a set time period (perhaps one or two months or a number of ignition cycles) but could potentially be available as evidence in court before being automatically overwritten.[61]

III. Current Legal Framework

Vehicle black boxes are primarily regulated and studied by NHTSA, which has neither imposed caps on the amount of data that can be collected nor directly addressed consumer privacy concerns.

Fourteen states have crafted various standards of ownership and rights but no federal law exists to clarify the rights of a vehicle owner with respect to this recorded data.[62] Ultimately, if drivers are even aware of the possibility that their actions could be recorded, they are denied a clear understanding, based on any federal law, of exactly what is stored and for how long that information could potentially be used against them.

A. Federal Regulations

In 2006, NHTSA finalized a rule specifying uniform, national requirements for vehicles equipped with EDRs "concerning the collection, storage, and retrievability of onboard motor vehicle crash event data" for vehicles manufactured after September 1, 2012.[63] This regulation, codified in the Code of Federal Regulations, Title 49, §§ 563.1 through 563.12, does not *require* EDRs in vehicles; it only applies to vehicles that the manufacturer has already equipped with this technology.[64] The purpose is to

---

60. *See id.*

61. *See id*.

62. *See* Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74,144 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571) (acknowledging that consumer privacy concerns persist regarding EDR data but that the NHTSA, as an agency, does not have the statutory authority to address many privacy issues because they are generally matters of State and Federal law). Approximately 12 states have enacted laws addressing these issues. *Id.*

63. 49 C.F.R. §§ 563.1–563.12 (2014). This requirement applies to light vehicles manufactured on or after September 1, 2012 that are equipped with EDRs. *Id.*

64. *Id.*

help ensure "that EDRs record, in a readily usable manner, data valuable for effective crash investigations and for analysis of safety equipment performance . . . These data will help provide a better understanding of the circumstances in which crashes and injuries occur and will lead to safer vehicle designs."[65]

The current regulations set forth exactly which data elements EDRs, if they are installed, *must* capture and record in certain circumstances; these include: changes in speed leading up to and during a crash, percentage of engine throttle, how far the accelerator pedal was pressed, whether or not the brake was applied, the number of power cycles applied to the EDR at the time of crash and number of power cycles applied to the EDR when the data was downloaded, whether or not the driver was using a safety belt, whether or not the frontal air bag warning lamp was on, driver frontal air bag deployment, right front passenger frontal air bag deployment, number of crash events, time between first two crash events if applicable, whether or not the EDR completed recording.[66]

The rule addresses the issue of access by requiring "vehicle manufacturers to make data retrieval tools and/or methods commercially available so that crash investigators and researchers are able to retrieve data from EDRs."[67] This means data must be both physically survivable and retrievable after a crash, even in the event of major damage or a fire, and the data must be readily usable—otherwise the devices are rendered useless.[68] The data must also be recorded in a format specified and with a certain degree of accuracy.[69] Without this caveat, manufacturing companies might be the sole entities capable of retrieving and reading the data in their

---

65. *Id*. at § 563.2.

66. *See id*. at § 563.7 (listing the required data elements for vehicles equipped with an EDR); *Event Data Recorders*, INS. INST. FOR HIGHWAY SAFETY (Mar. 2014), http://www.iihs.org/iihs/topics/t/event-data-recorders/qanda#cite-text-0-1 (citing Final Rule on Event Data Recorders, 71 Fed. Reg. 50,998–51,048 (Aug. 28, 2006) (to be codified at 49 C.F.R pt. 563) (listing what EDRs must record for layman understanding rather than reading the C.F.R which uses more technical language).

67. *See* 49 C.F.R. § 563.1 (providing the scope of part 563).

68. *See infra* Part IV.A.1 for a discussion of NHTSA's proposed regulations; Crash Test Performance and Survivability, 49 C.F.R. § 563.10 (2014); Event Data Recorders, 77 Fed. Reg. 74,144 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571) (explaining the purpose for standard requirements for EDRs).

69. See 49 C.F.R. § 563.8 (2014), for a table of data elements that must be reported in accordance with a specific degree of accuracy; *See* 49 C.F.R. § 563.10 (outlining crash test performance and survivability); 49 C.F.R. § 563.9 (specifying that air bag deployment-event data must not be overwritten by current event data).

vehicles. That could be troublesome because it would add additional burdens for all parties if the data were subpoenaed to be used in court.

Clearly, the primary purpose of the current federal regulations is to emulate NHTSA's goals of targeting driver safety, understanding accident causation, and developing safer vehicle designs[70] with little regard to consumer protection and personal data privacy concerns. Neither the Code of Federal Regulations, nor NHTSA specifically, explains the type of data it collects and uses. In fact, NHTSA has even acknowledged that "*consumer privacy concerns persist* regarding EDR data: Who owns it, who has access to it and under what circumstances, and what purposes for which it may be used."[71]

B. Consumer Concerns

1. Notice

The current federal regulations do not sufficiently address the issue of notice for consumers. Code of Federal Regulations Section 563.11 does set forth a specific statement that must be in the owner's manual, alerting the owner to the presence of an EDR and its function.[72] This blanket statement, however, will be buried somewhere in the text with no consumer disclosure requirement prior to purchase.[73] A buyer is unlikely to read through the

---

70. *See* 49 C.F.R. § 563.2 (noting the purpose of 49 C.F.R. 563); *see also* NHTSA's Core Values, *supra* note 30 (providing NHTSA's core values and purpose).

71. *See* Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74,144, 74,146 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571) (emphasis added).

72. *See* 49 C.F.R. § 563.11(a) (2014). The owner's manual in each vehicle must state that the vehicle is equipped with an EDR and that its main purpose is to record, in certain crash or near crash situations, information such as an air bag deployment or hitting a road obstacle, how various systems in the vehicle were operating, whether or not safety belts were buckled, how far the driver was depressing the accelerator and/or brake pedal, and how fast the vehicle was traveling. *Id.*

73. For an example of notice of the presence of an event data recorder in a modern car, see 2012 HONDA CIVIC SEDAN ONLINE REFERENCE OWNER'S MANUAL, AMERICAN HONDA MOTOR CO. 1 (2011), *available at* http://techinfo.honda.com/rjanisis/pubs/OM/R01212/R01212OM.pdf. In this online manual, which is presumably identical to the print version, neither the "Quick Reference Guide" nor the extensive Index mention "event data recorder," "EDR," or anything about recording devices in the vehicle. One would have to "control F" to find the notice of "Event Data Recorders" which states that the vehicle is equipped with an EDR and explains the "main purpose of an EDR is to record, in certain crash or near crash-like situations, such as an air bag deployment or hitting a road obstacle, data that will

manual *prior* to purchasing a vehicle, if ever. Thus, many vehicle owners are oblivious as to the presence of an EDR in their vehicle and many more are not aware that this data can be used against them in civil or criminal proceedings, or by their insurance company to increase their rates.[74] Additionally, drivers purchasing luxury vehicles may not understand that in-car GPS technology also has the potential to collect both personal and current location data.

2. Ownership and Consent

The presence of EDR systems is generally nonconsensual; they are present in most new vehicles unbeknownst to the purchaser, who cannot refuse to be monitored.[75] "[Y]ou can't shut it off, and you can't manipulate it," said a General Motors safety engineering spokesman.[76] In fact, because EDRs are an integral part of a vehicle's operating system, if a vehicle owner tampers with or disables an EDR, it may render inoperative important vehicle safety devices such as the air bag system.[77]

Even if vehicle owners have consented to the presence of recording devices in their cars, ownership remains a common concern of consumer

---

assist in understanding how a vehicle's systems performed. *Id* at 21. The EDR is designed to record data related to vehicle dynamics and safety systems for a short period of time, typically 30 seconds or less. *Id.* The EDR in this vehicle is designed to record such data as: "How various systems in your vehicle were operating; whether or not the driver and passenger safety belts were buckled/fastened; how far (if at all) the driver was depressing the accelerator and/or brake pedal; and, how fast the vehicle was traveling . . ." *Id* The section also sets forth how the data is used and includes a notice that, while no data is recorded under "normal driving conditions" and no personal data are recorded, other parties, such as law enforcement, could combine the EDR data with the type of personally identifying data routinely acquired during a crash investigation. *Id.*

74. *See* Mike Capuano, *Congressman Capuano's E-Update*, *Privacy and Your Vehicle*, U.S. HOUSE OF REPS. (June 24, 2013), *available at* http://www.house.gov/capuano/e-updates/eu2013-06-24.shtml (writing to his constituents about his recent filing of the "Black Box Privacy Protection Act").

75. *See* Bob Gritzinger, *Big Brother is Riding Shotgun*, AUTOMOTIVE NEWS (Nov. 15, 2004, 12:01 AM), http://www.autonews.com/article/20041115/SUB/411150735#axzz2mGobpoFp (noting that the system cannot be manipulated or shut off and thus purchasers of a new vehicle containing an EDR cannot refuse to have the EDR used in that vehicle).

76. *See id.* (quoting GM safety engineering spokesman, Jim Schell).

77. *See EDR Q&As*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. (Aug. 11, 2006), http://www.nhtsa.gov/DOT/NHTSA/Rulemaking/Rules/Associated%20Files/EDR_QAs_11Aug2006.pdf (recommending vehicle owners do not tamper or disable any vehicle safety system).

and privacy advocates—who owns EDRs and the data obtained from them?[78] NHTSA considers the owner of the vehicle to be the owner of its EDR data but this, ultimately, is a matter of state law.[79]

Generally, the fourteen states that have EDR laws have also concluded that the vehicle, as well as the data, have a common owner and the EDR data may not be downloaded by anyone other than the registered owner, except with the owner's consent or if ordered by a court.[80] Even in those fourteen states, regardless of who *owns* the EDR data, it has generally been allowed as evidence in criminal cases if necessary.[81] Because there is no similar EDR legislation in the other thirty-six states, there is no guarantee that accident investigators won't download the data with or without the owner's consent.

In *Kirsch v. State*,[82] the Texas Court of Appeals addressed an exception in the Texas Transportation Code which allows information contained on a black box to be retrieved by someone other than the owner *if the owner consents*.[83] Brian Thomas Kirsch, a deputy sheriff, was convicted

---

78. *See* 84 AM. JUR. 3D *Proof of Facts* § 15 (2005) (discussing EDR admissibility in civil trials).

79. *See* Memorandum from Raymond P. Owings, Assoc. Admin. for Research and Development, Nat'l Highway Traffic Safety Administration to The Docket (Sept. 30, 2011) (on file with author) (noting NHTSA's position about who owns EDR data and assuring that the owner's personal identifiable information is held to be confidential pursuant to the Privacy Act 5 U.S.C. § 522a).

80. *See* ARK. CODE ANN. § 23-112-107 (2013); CAL. VEH. CODE § 9951 (2014); COLO. REV. STAT. § 12-6-402 (2014); CONN. GEN. STAT. § 14-164aa (Supp. 2014); ME. REV. STAT. ANN. tit. 29-A, §§ 1972-1973 (2011); NEV. REV. STAT. ANN. § 484D.485 (LEXIS 2013); N.H. REV. STAT. ANN. § 357-G:1 (LEXIS 2014); N.Y. VEH. § TRAF. LAW § 416-b (Consol. Supp. 2014); N.D. Cent. Code § 51-07-28 (2013); OR. REV. STAT. §§ 105.928, .932, .935, .942, .945 (2014); TEX. TRANSP. CODE ANN. § 547.615 (West 2013); UT CODE §§ 41-1a-1501-04 (2014); VA. CODE ANN. § 46.2-1088.6 (West Supp. 2014); WASH. REV. CODE ANN. §§ 46.35.020, 0.30 (Supp. 2014).

81. *See* 84 AM. JUR. 3D *Proof of Facts* § 15 (2005) (noting that despite laws regarding EDR ownership, data is easily admissible in court); *see infra* Part III.E discussing EDR evidence in court.

82. Kirsch v. State, 276 S.W.3d 579 (Tex. Crim. App. 2008)), *aff'd*, 306 S.W.3d 738 (Tex. Crim. App. 2010).

83. TEX. TRANSP. CODE ANN. § 547.615 (West 2013) (emphasis added). Consent may also be obtained from anyone with authority over the property. *See* United States v. Matlock, 415 U.S. 164, 171 (1974) ("[W]hen the prosecution seeks to justify a warrantless search by proof of voluntary consent, it . . . may show that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship . . . ."). The State has the burden of establishing common authority, *see* Welch v. State, 93 S.W.3d, 50, 53 (Tex. Crim. App. 2002) (Sep. 18, 2002), but in *Kirsch* the true owner was present and gave authority.

for driving while intoxicated, after crashing into a tractor trailer when he was driving a borrowed patrol car.[84] After the accident, the unconscious Kirsch was transferred to a hospital for a blood-alcohol test which revealed a blood-alcohol level of 0.10 approximately 80 minutes after the accident occurred.[85] In the meantime, investigators attempted to retrieve data from the vehicle's black box. The black box data showed that Kirsch delayed applying his brake until less than one second before impact.[86]

Kirsch appealed his jury conviction for driving while intoxicated, challenging the admission of the evidence obtained from the black box and asserting that the evidence was seized in violation of his Fourth Amendment protection against unreasonable search and seizure.[87] Even though Kirsch was driving the vehicle, he was not the registered owner.[88] The true owner of the vehicle, however, consented to the removal of the black box,[89] rendering the search valid under the Fourth Amendment and *United States v. Matlock*.[90]

3. Privacy

In addition to notice, ownership, and consent, individuals' privacy rights with regard to various uses for the data is a common concern. No comprehensive federal privacy laws govern the collection, use, and sale of personal information by private-sector companies.[91] While members of

---

84. *See* Kirsch v. State, 276 S.W.3d at 581–82, 591 (explaining that Kirsch was working an extra job on patrol in a borrowed patrol car).

85. *Id.* at 583–84 (finding that Kirsch's blood-alcohol results were probative evidence that he had consumed alcohol on the night of the accident).

86. *Id.* at 582–83 (explaining that the black box stored data concerning the vehicle's actions for five seconds prior to air bag deployment).

87. *See id* at 587–88 (asserting that he had a legitimate expectation of privacy in the black box data).

88. *See* Kirsch v. State, 276 S.W.3d 579, 588–89 (Tex. Crim. App. 2008)), *aff'd*, 306 S.W.3d 738 (Tex. Crim. App. 2010).

89. *Id.* at 582 (explaining that the owner retrieved his personal items from the vehicle and told the officers who were attempting to download the black box data to "do what you need to do" to complete the investigation).

90. *See id.* at 588 (stating that the evidence shows the removal of the black box from the true owner's vehicle constituted a valid search); *see also* United States v. Matlock, 415 U.S. 164, 171 (1974); *see also* Welch v. State, 93 S.W.3d 50, 52 (Tex. Crim. App. 2002) (holding that a recognized exception to searches conducted without a warrant includes when voluntary consent to search has been given).

91. *See* GAO REPORT, *supra* note 41, at 7 (furthering that, rather, the privacy of

Congress have proposed legislation aimed at protecting the privacy of location data by mobile devices and navigation systems, none of the proposals have been enacted.[92]

Congress's concerns have to do with both black boxes and GPS-type devices.[93] While serving different purposes, both have the capacity to provide third parties with data that can be used to personally identify drivers, their private information, and their driving habits.[94] Data collected from these devices can be sold to third parties for marketing or monitoring and, disturbingly, it also has the potential to be used for stealing individuals' identity or stalking them.[95] NHTSA believes that privacy concerns are mitigated because it uses only a brief snapshot of EDR data surrounding a crash.[96] NHTSA also limits the amount of time after a crash that EDR data can be retrieved to 10 days, and limits storage of the information to 30 days.[97] But as evidenced by the fairly minimal federal regulations in place, while NHTSA has its own opinion on the matter, it does not control the market or what auto manufacturers choose to do with the EDRs placed in their vehicles.

A recent Government Accountability Office (GAO) report examining ten companies involved in the automobile industry, including manufacturers: Ford, General Motors, Chrysler, Toyota, Honda, and Nissan; GPS producers: Garmin and TomTom; and navigation developers: Google Maps and Tele-nav, found a wide variety of policies regarding

---

consumers' data is addressed in various federal laws).

92. *See, e.g.*, Geolocational Privacy and Surveillance Act, H.R. 1312, 113th Cong. (2013); Geolocational Privacy and Surveillance Act, S. 639, 113th Cong. (2013). Additionally, a bill was introduced in the 112th Congress that addressed the privacy of location data. *See* Location Privacy Protection Act of 2012, S. 1223, 112th Cong. (2011).

93. *See* GAO REPORT, *supra* note 41, at 1–22 (including a letter responding to Sen. Al-Franken's request to review issues related to the privacy of location data collected by in-car location-based services, including GPS).

94. *See* Swarts, *supra* note 5.

95. *See* GAO REPORT, *supra* note 41, at 1–3 (expressing common concerns of privacy groups and policy makers).

96. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., EVENT DATA RECORDERS, FINAL RULE, at 39, 115 (Aug. 2006) (stating that NHTSA's use of the data collected would not raise privacy concerns and that a broader use of EDR data would not be necessary for NHTSA's purposes).

97. *Id.* (modifying the prior rule based upon information from manufacturers about how much time it takes to complete crash test data analysis and validation).

tracking drivers' data.[98] The report did not identify specific policies employed by the investigated companies.[99]

The GAO report noted that recommended practices state that "companies should safeguard location data, in part, by de-identifying them; that companies should not keep location data longer than needed; and that such data should be deleted after a specific amount of time."[100] "De-identified" location data is data that has had personally identifiable information, such as a consumer's name or home address, removed or masked.[101] The report concluded that while the companies studied did safeguard location data, they used a variety of de-identification methods with no consistent levels of protection for consumers.[102] The fact that de-identified data can be reconstituted in certain circumstances and re-identified was not specifically addressed by the companies.[103]

While the report noted that the ten companies had each taken some steps consistent with the industry-recommended privacy practices, not all practices were followed and, in certain instances, companies' privacy practices were "unclear, which could make it difficult for consumers to understand the privacy risks that may exist."[104] For instance, companies used a variety of methods to disclose their privacy practices to consumers and the information about the use and sharing of location data was sometimes unclear.[105]

C. State Laws on EDRs

Some states have attempted to address consumers' EDR concerns but because vehicles commonly travel across state lines, federal regulations are better equipped to address the various issues.

California, in 2004, was the first state to enact legislation concerning EDRs.[106] Since then, thirteen additional states have followed suit.[107] The

---

98. *See* GAO REPORT, *supra* note 41.

99. *Id*.

100. *Id.* at 16.

101. *Id*. at 10 n.13.

102. *See id.* at 16.

103. *See id.* at 10 n.13 (explaining that when "data are de-identified," a consumer's personally identifiable information could be reconstituted in certain circumstances).

104. GAO REPORT, *supra* note 41, at 2.

105. *See id.* at 12.

106. Nancy M. Erfle, *Learning to Live with Electronic Data Recorders*, 38 THE BRIEF

crux in all fourteen states surrounds ownership—whether the owner of the vehicle also owns the EDR and whether a lessee of a vehicle also leases or owns the EDR during the lease period.[108]

While the individual state provisions vary considerably, all fourteen states prohibit data downloading without the owner's consent, with various exceptions.[109] The exceptions include data that has been subpoenaed by a court order, data used for emergency medical care or for vehicle safety research, and where there is probable cause of an offense.[110] In other words, states that specify the exception that the data may be used for vehicle safety research without the owner's consent are allowing government, NHTSA, or auto manufacturers to download the data for safety research purposes.

Another critical distinction between states is notice and disclosure; states have various levels of disclosure concerning the presence of data recording technology. In Arkansas, a written notice at the time of vehicle purchase from the dealership is required.[111] By contrast, Connecticut does not require any disclosure except "in agreements with subscription services."[112] Subscription services might include insurance companies' driving programs, such as Progressive's Snapshot, which not every consumer opts in to.[113] Without thoroughly addressing the notice/disclosure issue, Connecticut ignores the fact that many of consumers' privacy concerns might be mitigated were they at least aware of the fact that their driving habits might be recorded.

While Arkansas appears to account for the notice concern, the state's regulations neglect the fact that not every driver purchases a new vehicle

---

14, 16 (2008).

107. *See Privacy of Data from Event Data Recorders: State Statutes*, NAT'L CONF. OF STATE LEGISLATURES (June 23, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx (listing selected provisions in the fourteen states with laws on sensing diagnostic modules).

108. *Id.*

109. *Id*. (demonstrating the degree of differences among states); *See* Lou Stanley, *Decoding Data: EDRs in Auto Claims Investigations*, CLAIMS MAG., Mar. 2014, at 34, (noting that ownership of the EDR and its data is a matter of state law and such provisions vary considerably).

110. See *Privacy of Data from Event Data Recorders: State Statutes*, *supra* note 107 (listing exceptions where data can be downloaded without the owner's consent).

111. ARK. CODE ANN. § 23-112-107 (2014). Note that the statute specifies purchase from dealerships but many consumers purchase vehicles from other venues or third parties.

112. CONN. GEN. STAT. § 14-164aa (Supp. 2014).

113. See *supra* Part II.B, for a brief discussion of insurance companies' use of tracking devices.

from a dealership. In Arkansas, if someone purchases a used vehicle other than from a dealership, there may be no disclosure.

The states that have passed laws regarding EDR data collection have made a progressive step in the right direction, but the laws are lacking in depth and, in general, state laws regarding EDRs disregard an important fact about cars: they cross state lines. When a driver leaves a state with EDR legislation and travels to a state without it, the driver's data may no longer be protected. This is why a comprehensive federal law is necessary to cover all vehicles' EDRs and their owners or lessees.

D. The Fourth Amendment and Automobiles

Regardless of whether drivers have consented to—or are even aware of—the presence of recording devices, do individuals have a reasonable expectation of privacy in their vehicles from the ominous, ostensibly objective witness within?

The question remains whether the government, NHTSA, automobile manufacturers, or private companies may collect data from Americans' vehicles and use it for their respective purposes. Significant government regulation exists for automobiles operating on public roads, but regulation and Fourth Amendment jurisprudence with regard to protections *inside* of a vehicle is far from clear.[114]

1. Governmental Activity

The Fourth Amendment provides safeguards for the public to be secure in their "persons, houses, papers, and effects, against unreasonable searches and seizures."[115] The threshold question to consider is whether there is governmental activity. The Fourth Amendment does not apply to searches and seizures by private parties, reasonable or otherwise, if the party is not acting as an agent of the government or with the participation or knowledge of any governmental official.[116]

---

114. *See* Phyllis T. Bookspan, *Reworking the Warrant Requirement: Resuscitating the Fourth Amendment*, 44 VAND. L. REV. 473, 474–75 (1991) ("Current search and seizure doctrine is inconsistent and incoherent. No one, including the police who are to abide by it, judges who apply it, or the people who are protected by it, has any meaningful sense of what the law is.").

115. U.S. CONST. amend. IV.

116. *See* Marjorie A. Shields, Annotation, *Fourth Amendment Protections, and*

NHTSA, a government agency, does not currently require black boxes in automobiles—although they would like to.[117] Private parties (automobile manufacturers) already install black boxes on their own initiative.[118] NHTSA, supposedly, only uses the data from a crash for its research after consent from vehicle owners.[119] It might be difficult to assert that NHTSA's current involvement with this data constitutes a sufficient government connection.

An alternative point of view might consider automobile manufacturers as agents of the government by participating in the data collection NHTSA uses. General Motors Company's U.S. Consumer Privacy Statement explains that GM receives information "from your vehicle's Event Data Recorder [] as described in your owner's manual (i.e., how various systems in your vehicle operate)."[120] The privacy statement further notes instances in which "GM may share the information it collects about you and your vehicle . . ." including "with third parties for research and development purposes (such as university research institutes for improving highway safety)."[121] A careful reading of GM's entire privacy statement makes clear that GM has a broad range of options regarding individuals' personally identifying information and vehicle data, including providing it to the government—provided it is "for improving highway safety."[122]

If NHTSA's proposed legislation to mandate black boxes in all new vehicles passes, there would be a stronger argument for government activity. The Fourth Amendment analysis does not end there, however.

Equivalent State Constitutional Protections, as Applied to the Use of GPS Technology, Transponder, or the Like, to Monitor Location and Movement of Motor Vehicle, Aircraft, or Watercraft, 5 A.L.R. FED. 385 (2005).

117. *See infra* Part IV.1 (providing NHTSA's proposal to mandate EDRs in all new vehicles); *see also* Request for Comment on Automotive Electronic Control Systems Safety and Security Notice, 79 Fed. Reg. 60574 n. 26 (noting that no final rule publication date has been established).

118. *See supra* Part II (explaining that as vehicles became gradually more dependent on computers to run internal systems, manufacturers increasingly installed EDRs into their vehicles to perform a variety of operating and safety functions).

119. *See* Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74,143 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571) (stating that the agency strives to minimize impacts on privacy and obtains a vehicle owner's consent prior to obtaining EDR data in a crash investigation).

120. *See Privacy Statement*, GEN. MOTORS (last modified Dec. 19, 2013), http://www.gm.com/privacy/ (describing, minimally, the information General Motors collects from its vehicles equipped with EDRs).

121. *Id*.

122. *Id.*

2. Is Data Collection a Search?

If there is government activity, the collection of individuals' data without consent may be considered a Fourth Amendment search. NHTSA and vehicle manufacturers claim they are not actually monitoring vehicles; EDRs simply record information about crash situations.[123] But the collection of this data, even if its purpose is solely to improve vehicle safety, may still be considered a "search" under the Fourth Amendment.

The Supreme Court asserts that the Fourth Amendment protection from unreasonable government intrusion does not constitute a constitutional "right to privacy"[124] but depends on the *expectation* of privacy in the place searched and whether that expectation is recognized by society as *reasonable*.[125] Fourth Amendment jurisprudence has traditionally been governed by the "reasonable expectation of privacy" test introduced by Justice Harlan in his famous concurring opinion in *United States v. Katz*.[126] Specifically, Justice Harlan held that a "search" requires two conditions to be met: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[127]

The reasonable expectation of privacy standard depends, in large part, "upon whether that expectation relates to information that has been exposed

---

123. *See supra* Part II.A (explaining the functions of EDRs).

124. *See* Katz v. United States, 389 U.S. 347, 349 (1967) (holding that the Fourth Amendment cannot be generalized as a constitutional right to privacy and that the protections of the Fourth Amendment often have nothing to do with privacy issues).

125. *Id.* at 360 (Harlan, J., concurring) (summarizing his reading of the majority's holding that "a person has a constitutionally protected *reasonable* expectation of privacy" and the reasonableness is measured by that which society is prepared to recognize as "reasonable") (emphasis added).

126. *See id.*; *see also* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 316 (2012) (asserting that from the 1960s until *Jones*, the search inquiry was governed by the reasonable expectation of privacy test). In United States v. Jones, 132 S. Ct. 945, 945 (2012), the court held that the Government's attachment of a GPS device to Jones's vehicle to monitor the vehicle's movements constituted a Fourth Amendment "search." Additionally, the court noted that the defendant possessed the vehicle at the time the Government trespassorily inserted the information-gathering device and therefore the Government physically occupied private property under the common law trespass test. Such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.

127. *See Katz* 389 U.S. at 361 (Harlan, J., concurring) (explaining his understanding of the rule from prior decisions and continuing to explain that "a man's home is, for most purposes, a place where he expects privacy").

to the public."[128] Accordingly, no invasion of privacy occurs if the invasion or intrusion is something that the general public would be free to view.[129] This makes the privacy issue with regard to vehicles a little vague.

The Fourth Amendment covers an *individual's* privacy within their vehicle but does *not* extend to the vehicle itself when driving on a public road.[130] By traveling on public roads, drivers cannot expect privacy with regard to information they are voluntarily conveying to anyone within view, such as the route they are traveling, the approximate speed of the car, and the nature of their driving.[131] These are all movements that any witness to a car accident might be able to testify to.

This is the theory behind police using GPS tracking devices on vehicles—GPS devices record only information that could be picked up by the *naked eye*.[132] While there is no reasonable expectation of privacy in the *outside* of a vehicle, monitoring driver activity *within* a vehicle that is not visible to the public is arguably different.[133] The inside of a vehicle is subject to Fourth Amendment protection.[134]

Accident reconstruction experts are able to hypothesize about the speed of a car and braking times based on skid marks and other physical

---

128. United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010) (citation omitted) (internal quotation marks omitted). The D.C. Circuit posits that a single journey or trip is not subject to a reasonable expectation of privacy because roadways are public and open to plain view but "the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil." *Id.*

129. *See* United States v. Vazquez, 31 F. Supp. 2d 85, 90 (D. Conn. 1998) (holding that in order for an invasion of privacy to occur, in a vehicle or otherwise, that "invasion or intrusion must be of something which the general public would not be free to view").

130. *See* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). This theory derives from the open fields doctrine. *See* Hester v. United States, 265 U.S. 57, 59 (1924) (stating that the distinction between an open field and one's home is "as old as the common law").

131. *See Knotts*, 460 U.S. at 281–82 (furthering that by traveling on public streets, the party "voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, . . . whatever stops he made, and . . . his final destination when he exited from public roads onto private property").

132. *See* Shields, *supra* note 116 (noting that electronic tracking devices have been recognized to be governed by the law of search and seizure, and not by the laws of electronic surveillance); *GPS Overview*, GPS.GOV, http://www.gps.gov/systems/gps/ (last visited Nov. 1, 2013) (noting that GPS provides users with positioning, navigation, and timing services).

133. *See* New York v. Class, 475 U.S. 106, 112–14 (1986) (noting that the interior of the vehicle, in contrast to the exterior, is subject to Fourth Amendment protection).

134. *Id.*

evidence at the scene or on the vehicle.[135] Bystanders, including law enforcement officers, might witness an accident, speeding, driving under the influence, driving without a seatbelt; but only the EDR may know exactly what happened *inside* the vehicle—e.g. the exact moment that the driver hit the brake or the precise rate of deceleration.[136]

While it has been held to be reasonable for an officer's head or torso to be inside an open car window during a stop, no law enforcement officer would even be capable of performing a "search" of EDR data within a vehicle simply by viewing it.[137] If the EDR simply recorded information which the public could view or even record with their personal phones and video recorders, perhaps the black box is not protected. But it seems clear that manufacturers are sharing with third parties personal driver information that cannot be publicly surmised, constituting an invasion of privacy.[138] If no one is around to witness an accident, there is still a silent witness in our car.

At the other end of the spectrum, drivers may find EDR data can be used to their advantage in automobile product liability cases.[139] The EDR becomes a reliable "witness" for proving there was a mechanical problem inside the vehicle,[140] proving that a seatbelt was worn but injuries still resulted, or proving that the driver depressed the brake pedal but nothing happened.[141]

---

135. *See generally* AMERICAN PROSECUTORS RESEARCH INSTITUTE, CRASH RECONSTRUCTION BASICS FOR PROSECUTORS 11 (2003), *available at* http://www.ndaa.org/pdf/crash_reconstruction_basics.pdf (describing the elements of common crashes and the formula for determining speed from friction marks made by tires).

136. *See* Torchinsky, *supra* note 25 (providing examples of the capabilities of event data recorders, including brake depression and rate of deceleration).

137. *See* United States v. Ryles, 988 F.2d 13, 15 (5th Cir. 1993) (noting that a state trooper would not have been unreasonable either in placing his head inside the interior of the vehicle through an open window or in opening the driver's door and placing his torso inside, even assuming he did not smell marijuana before the intrusion).

138. *See* Swarts, *supra* note 16.

139. See *infra* III.E.1, for a discussion of Bachman v. Gen. Motors Corp., 776 N.E.2d 262, 289 (Ill. App. Ct. 2002), in which the plaintiff won based on evidence from an EDR that her airbag had inadvertently deployed, causing the accident.

140. *See id.* Individuals may have little bargaining power when it comes to lawsuits against automobile manufacturers. But if a mechanical problem *caused* the accident, this could be to the consumer's advantage.

141. Recall the Toyota unintended acceleration crisis in 2011. *See* Csaba Csere, *It's All Your Fault: The DOT Renders Its Verdict on Toyota's Unintended-Acceleration Scare*, CAR AND DRIVER (June 2011), http://www.caranddriver.com/features/its-all-your-fault-the-dot-renders-its-verdict-on-toyotas-unintended-acceleration-scare-feature (reporting that an

3. Is Data Collection a Seizure?

The next inquiry: whether data collection constitutes a seizure. Even if one considers data collection to be a Fourth Amendment search, private companies may still be able to collect and use the data, particularly if companies argue that vehicle owners provided consent, or even implied consent, by purchasing the vehicle already equipped with EDR technology.[142]

A seizure of property, for purposes of the Fourth Amendment, occurs when "there is some meaningful interference with an individual's possessory interests in that property."[143] The owner of property has a right to exclude it from "all the world," and government use "infringes that exclusionary right."[144] Additionally, seizures of property must be based on probable cause or reasonable, articulable suspicion.[145]

EDRs are a functional component of an automobile, rather than a distinct piece of personal property.[146] Thus, even if the owner of the vehicle is considered to own the EDR, a seizure of the EDR's data does not actually deprive the owner of any possessory interest in the EDR.[147] One might complain that the time it took for a law enforcement officer to download the EDR data after an accident was a meaningful interference with their possessory interest and infringed on their exclusionary right to it. However,

---

examination of the problem Toyota vehicles' EDRs demonstrated that none of them showed pre-impact braking or substantial acceleration, suggesting that drivers were unaware of impending crashes).

142. *See Privacy Statement*, *supra* note 120 (describing instances where GM shares information it collects about drivers and their vehicles with third parties).

143. United States v. Karo, 468 U.S. 705, 712 (1984) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

144. *Id.* at 729 (Stevens, J., dissenting).

145. *See* United States v. Place, 462 U.S. 696, 700 (1983); *see also* Texas v. Brown, 460 U.S. 730, 749 (1983) (Stevens, J., with Brennan & Marshall, JJ., concurring); *see also* Payton v. New York, 445 U.S. 573, 587 (1980). When there is probable cause to believe that a container holds contraband or evidence of a crime, the Court has held that the Fourth Amendment permits law enforcement officers to seize the property pending issuance of a warrant if justified by exigent circumstances or another exception to the warrant requirement. *See Place*, 462 U.S. at 701.

146. *See* Glennon, *supra* note 19 (explaining the interconnectivity of EDRs in vehicles).

147. *See Karo*, 468 U.S. at 712 (describing a seizure of property as occurring when there is some meaningful interference with an individual's possessory interests in that property).

if there is a court order to download the data, probable cause has already been established and seizure would be warranted.[148]

Law enforcement may also be able to seize EDR data under the theory of exigent circumstances.[149] Any data not downloaded soon after an accident could be destroyed; there might be another crash that results in a fire and destroys the EDR or the driver might even attempt to tamper with the device to avoid potential liability.[150] When such exigent circumstances exist, particularly with regard to vehicles in which the owner already has a diminished expectation of privacy, seizure of potential evidence has been found to be constitutional.[151]

E. EDR Data as Evidence in Civil and Criminal Trials

EDRs were not designed to provide evidence for criminal prosecutions, but evidence obtained from EDRs has been increasingly used in certain types of criminal trials such as motor vehicle homicide, operating under the influence, and driving to endanger.[152] Police and investigators use the data to reconstruct what happened in a crash to help apportion blame.[153] In civil cases, "[c]ourts . . . have manifested a willingness to accept data collected by these [EDR] systems . . . as long as it complies with the applicable evidentiary standard of 'general acceptance' as a legitimate technology."[154]

---

148. *See* U.S. CONST. amend. IV. The Fourth Amendment allows for search warrants only if there is a finding of probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized. *Id.*

149. *See* Carroll v. United States, 267 U.S. 132, 162 (1925) (holding a warrantless search of an automobile is constitutional based upon exigency); *see also* People v. Christmann, 776 N.Y.S.2d 437, 441 (2004) (citing Cardwell v. Lewis, 417 U.S. 583, 590 (1974)) (noting that the *Carroll* exigency exception now has been mostly replaced by findings that there is a diminished expectation of privacy in vehicles).

150. *See Black Box Data*, DYSART LAW FIRM, http://www.dysart-law.com/cases-we-accept/winning-your-case/the-importance-of-preserving-evidence/black-box-data/ (pointing out that insurance companies and defendants "can be expected to work hard to avoid liability").

151. *See* People v. Christmann, 776 N.Y.S.2d at 441 (explaining the concept of exigency with regard to warrantless searches of automobiles).

152. *See* Glancy, *supra* note 53, at 14; *see also* Shields, *supra* note 23, at 595 (giving examples of the routine uses of black box data in prosecutions).

153. *See* Travers, *supra* note 22 (explaining common uses of EDR data).

154. Frank Douma & Jordan Deckenbach, *The Challenge of ITS for the Law of Privacy*, 2009 U. ILL. J.L. TECH. & POL'Y 295, 314 (2009).

Recall that Kirsch argued that his delayed brake timing did not indicate impairment because the tractor-trailer that he crashed into made an unexpected right-hand turn.[155] Viewed in a light most favorable to the jury's verdict, the appellate court found that the brake timing evidence from the black box data supported the inference that the delayed response was caused by alcohol.[156] Finding the evidence legally sufficient to support the verdict, the appellate court did not even reach the alternative means by which the State could prove intoxication—based on proof that Kirsch's blood alcohol concentration was above 0.08.[157]

This may seem like an unsupported inference, but it illustrates a privacy concern implicated by the collection of EDR data. For instance, a law enforcement officer who pulls over a car for speeding may have probable cause to conduct a field sobriety test, or even a Breathalyzer test, to determine whether the driver was intoxicated beyond the legal limit.[158] The driver may then be transported to a hospital where blood work will also conclusively show the driver's level of intoxication.[159] But Brian Kirsch was convicted based on third-party data and an expert witness testifying about reaction times.[160] Of course, in this case his blood-alcohol level was over the legal limit anyway.[161] That does not diminish the fact that the data from the black box assumed the role of the police and became an objective witness to the accident.[162] Kirsch may not have even known that was a possibility.

In *Kirsch*, there appeared to be sufficient extrinsic and technical evidence to support the finding that the driver was liable for the accident.[163]

---

155. *See* Kirsch v. State, 276 S.W.3d 579, 584 (Tex. Crim. App. 2008) (summarizing appellant's argument for the legal sufficiency analysis of evidence of driving while intoxicated).

156. *See id.*

157. *See id.*

158. *See* State v. Marks, 644 N.W.2d 35, 38 (Iowa Ct. App. 2002) (finding that field sobriety tests did not violate motorist's Fourth Amendment rights when a valid speeding stop was made and motorist exhibited visual signs of intoxication, thus giving the officer probable cause to arrest).

159. *See* Schmerber v. California, 384 U.S. 757, 771–72 (1966) (finding that the Fourth Amendment does not protect an individual against actions by private individuals, thus a seizure of a blood sample by a hospital for treatment purposes is not within the ambit of the Fourth Amendment).

160. *See Kirsch*, 276 S.W.3d at 748.

161. *See id.*

162. *See id.* at 740.

163. *See id.*

But in cases where courts must rely almost entirely on technical evidence and data, the potential for technical error, misuse, and incorrect convictions or incorrect exonerations looms.[164] Due to the technology involved, EDR data may not always be reliable and/or accurate enough to be used in court and the reliability "likely will continue to be—fodder for *Daubert* challenges."[165]

Prosecutors of motor vehicle offenses attempting to use EDR data must overcome two critical evidentiary issues; the data must be admissible under the relevant standard for testimony by expert crash reconstructionists (almost all jurisdictions apply either the federal *Daubert*[166] test or the older test under *Frye*)[167] and the prosecutor must show the probative value of the data in establishing the driver's conduct.[168] "In civil cases, the latter hurdle has proven the more difficult to overcome, but the passage of time and an accompanying rise in use of automotive black boxes may bring greater judicial endorsement of the data's probative value."[169]

1. Admissibility of Evidence

Admissibility of EDR data might be essential in ensuring the achievement of justice in accident investigations. Courts have been inconsistent regarding the admissibility of EDR data.[170] In one of the

---

164. *See* John G. Browning, *Emerging Technology and its Impact on Automotive Litigation*, 81 DEF. COUNS. J. 83, 88 (Jan. 2014) (introducing a brief summary of courts struggling with admissibility of this new technology).

165. *See id.* After *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), Federal Rule of Evidence 702 was amended to reflect the decision. *Daubert* set forth a non-exclusive checklist for trial courts to use in assessing the reliability of scientific expert testimony: (1) whether the expert's technique or theory can be or has been tested; (2) whether the technique or theory has been subject to peer review and publication; (3) the known or potential rate of error of the technique or theory when applied; (4) the existence and maintenance of standards and controls; and (5) whether the technique or theory has been generally accepted in the scientific community. *See* FED. R. EVID. 702.

166. *See* FED. R. EVID. 702 (explaining the *Daubert* test).

167. Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923). The "general acceptance" test of Frye was superseded by the Federal Rules of Evidence.

168. *See* Shields, *supra* note 23, at 595 (adding that this prong is necessary for the data to be of any practical use).

169. Kevin J. Powers, *David Hasselhoff No Longer Owns the Only Talking Car: Automotive Black Boxes in Criminal Law*, 39 SUFFOLK U. L. REV. 289, 291 (2005).

170. *See* Browning, *supra* note 164 (explaining that courts have gone both ways in determining the admissibility of EDR data).

earliest decisions involving EDR data in 2000, the Sixth Circuit reversed a summary judgment for General Motors in a products liability case, holding that the General Motors expert's affidavit relying on the EDR data was insufficient in and of itself to justify rejecting the plaintiff's claims outright that the air bag deployed *after* the accident.[171] Conversely, in another leading case, *Bachman v. General Motors Corp.*, application of the *Frye* test supported admissibility of EDR data.[172] Debra Bachman brought an action against her automobile manufacturer and others for injuries she and her daughter suffered, claiming her air bag sensing and diagnostic module (SDM) was "hypersensitive" to road surfaces and inadvertently deployed, causing the accident.[173] Over the plaintiff's objections, the trial court admitted the EDR data as well as the General Motors expert's interpretation of that data.[174] An expert for the defendants testified that the downloaded data "showed that the delta-v for [Bachman's] Cavalier during the collision was 16.2 miles per hour, which was above the air-bag deployment threshold of 14 miles per hour."[175]

Affirming the jury's verdict against the plaintiff, the Illinois Appellate Court stated that, "the process of recording and downloading SDM data does not appear to constitute a novel technique or method," thus satisfying the *Frye* admissibility standard, and the trial court did not abuse its discretion in finding that the use of this kind of data had "gained general acceptance in the relevant scientific community."[176] Application of the Frye test in *Bachman* supports the admissibility of EDR data.[177] The *Frye* standard, also known as the general acceptance test, dictates that scientific evidence can only be admitted at trial if the methodology or scientific principle upon which the opinion is based is "sufficiently established to

---

171. *See* Harris v. Gen. Motors Corp., 201 F.3d 800, 802–04 (6th Cir. 2000) (summarizing General Motors' argument that the air bag could not have deployed "belatedly" in the manner described by the plaintiff because the data suggested that the system functioned as designed by deploying during plaintiff's accident). Harris, the Plaintiff, claimed that after the accident, as she reached to turn off the ignition, the air bag deployed and broke her arm. *Id.*

172. *See* Bachman v. General Motors Corp., 776 N.E.2d 262, 283 (Ill. App. Ct. 2002) (holding SDM data admissible under the *Frye* test).

173. *See id.* at 271 (explaining that the SDM is an air bag crash sensor).

174. *See id.*

175. *Id.* at 279–80 (adding that if, as plaintiffs alleged, the air bag inadvertently deployed prior to the collision, "'there would be two records present in the SDM': (1) the inadvertent deployment; and (2) the 16.2 mile per hour delta-v").

176. *Id.* at 281–83.

177. *Id.*

have gained general acceptance in the particular field in which it belongs."[178]

2. Discovery

Discovery can be an issue simply because of the varying technologies and state rules surrounding the retrieval of EDR data, but generally, there must be either consent or a court order to retrieve such data.[179] Many professional accident investigators have devices which allow a laptop to communicate with an EDR to download the information, but there remain many vehicles whose data can only be retrieved by the manufacturer.[180]

Additional issues of spoliation of evidence are likely to plague courts confronted with EDR evidence.[181] Steps must be taken to preserve crash data since there have been cases involving post-accident events that triggered the loss of data.[182] These cases indicate the need for a more comprehensive bright-line rule that law enforcement officers download EDR data whenever possible at the scene of an accident.

IV. The Future of EDRs

EDRs are here to stay and if NHTSA has its way, at some point all vehicles on the road will have recording capabilities.[183] This technology is constantly advancing and becoming more prevalent in vehicles.[184]

---

178. Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923).

179. The following are state laws governing retrieval of EDR data: ARK. CODE ANN. § 23-112-107 (2013); CAL. VEH. CODE § 9951 (2014); COLO. REV. STAT. § 12-6-402 (2014); CONN. GEN. STAT. § 14-164aa (Supp. 2014); ME. REV. STAT. ANN. tit. 29-A, §§ 1972-1973 (2011); NEV. REV. STAT. ANN. § 484D.485 (LexisNexis 2013); N.H. REV. STAT. ANN. § 357-G:1 (LexisNexis 2014); N.Y. VEH. & TRAF. LAW § 416-b (Consol. Supp. 2014); N.D. Cent. Code § 51-07-28 (2013); OR. REV. STAT. §§ 105.928, .932, .935, .942, .945 (2014); TEX. TRANSP. CODE ANN. § 547.615 (West 2013); UT CODE §§ 41-1a-1501-04 (2014); VA. CODE ANN. § 46.2-1088.6 (West Supp. 2014); WASH. REV. CODE ANN. §§ 46.35.020, 0.30 (Supp. 2014).

180. *See* Leonard Bucklin, *There's a Black Box in Your Client's Car – EDR*, LAWYER TRIAL FORMS 1, 4–5, *available at* http://lawyertrialforms.com/catalog/power-articles/MVA-EDR-article.pdf (last visited Dec. 10, 2014) (describing recoverability and usability of EDR data).

181. *See* Browning, *supra* note 164 (discussing issues of spoliation of evidence).

182. *See id.*

183. *See* Editorial*, Black Boxes Are in 96% of New Cars*, USA TODAY (Jan. 6, 2013, 6:37 PM), http://www.usatoday.com/story/opinion/2013/01/06/black-boxes-cars-edr/1566098/

A. Proposed Legislation

The following proposals reflect an attempt to create consistent standards regarding EDR data and to address various ownership and notice concerns.

1. NHTSA's Proposal

Currently, the federal government does not require manufacturers to install EDRs, but in December, 2012, NHTSA formally proposed regulations to establish a new safety standard mandating the installation of EDRs in all light vehicles that are required to have frontal air bags (essentially all light vehicles).[185] The purpose of this proposed regulation is to "expand and, therefore, potentially enhance the utilization of the recorded information and lead to further improvements in the safety of current and future motor vehicles."[186] The EDRs would still need to meet the standards of the existing 2006 regulations.[187]

NHTSA believes that the information available, if all new vehicles were equipped with EDR functions, would be "vital to an agency

---

(concluding that black boxes are not going anywhere).

184. *See* GAO REPORT, *supra* note 41 (writing that the prevalence of these systems has brought consumers significant benefits and features as well as raised privacy concerns).

185. Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74,144 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571). The EDRs in those vehicles would be required by the new standard to meet the data elements, data capture and format, data retrieval, and data crash survivability requirements contained in 49 C.F.R. pt. 563. *See also* Memorandum from William Shakely, Attorney Advisor, Nat'l Highway Traffic Safety Admin. to Docket No. NHTSA-2012-0177 (Aug. 27, 2013), *available at* http://www.regulations.gov/#!documentDetail;D=NHTSA-2012-0177-1038 (setting forth substantive changes to the Dec. 13, 2012 NPRM after the review by the Office of Information and Regulatory Affairs (OIRA)). Walk-in van-type trucks or vehicles designed to be sold exclusively to the United States Postal Service are excluded from air bag and EDR requirements. *See* Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. at 74,144 .

186. Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. at 74,152 (explaining that NHTSA believes requiring EDRs in all light vehicles could potentially enhance the utilization of the recorded information and lead to further improvements in the safety of current and future motor vehicles).

187. *Id.* at 74,146. The 2012 proposal would not modify any of the requirements or specifications already existing for EDRs voluntarily installed between September 1, 2012 and September 1, 2014; *See supra* Part III.A for a discussion of the current regulations on existing EDRs.

investigation seeking to determine whether there is a safety defect in vehicles that are being driven by consumers on the road and to agency efforts to assess the performance of advanced safety technologies for possible future regulatory action."[188]

This proposal is two-fold; it may truly increase drivers' safety but it will also eliminate consumers' individual rights to make choices about the types of vehicles they drive—whether they want to drive a vehicle that has the capacity to record their driving or not.

2. Black Box Privacy Protection Act

In response to NHTSA's 2012 proposal, Representative Michael Capuano (D-MA) introduced the Black Box Privacy Protection Act, H.R. 2414, which amends the Automobile Information Disclosure Act to require automobile manufacturers to disclose the presence of EDRs on new automobiles and to require manufacturers to provide the consumer with the option to enable or disable such devices on future automobiles.[189] Capuano believes that "[c]onsumers should have control over the information collected by event data recorders in vehicles that they own and they should have the option of disabling the device if they choose to do so. This is a basic issue of privacy."[190]

The bill requires the following information on the window of the automobile: (1) the presence and location[191] of an event data recorder, (2) the type of information recorded and how such information is recorded, and (3) that the recording may be used in a law enforcement proceeding.[192]

---

188. *Id.* at 74,150.

189. *See* Black Box Privacy Protection Act, H.R. 2414, 113th Cong. § 4 (2013). This bill was assigned to a congressional committee on June 18, 2013 which will consider it before possibly sending it on to the House or Senate as a whole. Rep. Capuano has been filing this bill since 2006. *See* Mike Capuano, *Congressman Capuano's E-Update*, *Privacy*, U.S. HOUSE OF REPS. (July 19, 2013), *available at* http://capuano.house.gov/e-updates/eu2013-07-19.shtml (explaining H.R. 2414 as giving consumers control over EDR data).

190. Press Release, Rep. Michael E. Capuano, Congressman Capuano Introduces Legislation Giving Consumers More Control Over Their Car's "Black Boxes" (June 29, 2011), *available at* http://www.house.gov/capuano/news/2011/pr062911.shtml. This bill is co-sponsored by Rep. Jim Sensenbrenner (R-WI).

191. The wording of this bill demonstrates the lack of understanding about EDR systems since it is not a box sitting in one location of the vehicle but instead a complex, interconnected system.

192. *See* H.R. 2414, § 3.

Additionally, it requires the EDR, and any data recorded, to be considered the property of the owner of the automobile or motorcycle.[193]

If this bill passes, it would seem to eliminate almost all notice issues as well as some privacy concerns.

3. Driver Privacy Act

Another recent bill, introduced January 14, 2014 by Senator Amy Klobucher, (D-MN) and Senator John Hoeven, (R-ND), covers the same ownership issue as the Black Box Privacy Protection Act[194] and adds a measure for protecting driver privacy.[195] The Act provides that EDR data cannot be extracted from individual's cars or taken by another party without the owner's consent except under specific circumstances: under authorization by a court of law, when the data is necessary in an emergency medical situation, or for the purpose of traffic safety research.[196] In other words, NHTSA may retrieve information from drivers' vehicles *without* owners' consent in some circumstances. The data retrieved for traffic safety research, however, must not disclose any personally identifiable information about the owner or lessee of the vehicle, including the vehicle identification number.[197]

The Act covers another issue—the lessee of a leased vehicle is also considered the owner during the lease period for purposes of the EDR and its data. [198] Many consumers choose to lease vehicles and deserve the same ownership rights over the data produced by their driving of the leased vehicle.

This bill would provide the initial safeguards necessary to ensure that personally identifiable information remains undisclosed.[199] Regardless of the passage of the Black Box Privacy Protection Act or the Driver Privacy

---

193. *See id.* at § 5.

194. *See* Driver Privacy Act, S. 1925, 113th Cong. § 2 (2014). The Driver Privacy Act makes any information in a vehicle's EDR the property of the vehicle's owner or lessee.

195. *See id.*

196. *See id.*

197. *See id.*

198. Of the 14 states that have passed EDR legislation, only a few mention leasing of a vehicle in addition to ownership. For a list of these states, see *supra* note 80.

199. *See* S. 1925, § 2.

Act, EDRs are not going anywhere.[200] Their presence and use will inevitably become commonplace in our society.[201]

B. Potential Misuses of EDRs

The current proposals fail to sufficiently address the potential issues of reliability and security.[202] It is important to understand the potential misuses of this data by criminals, courts, and terrorists. "As vehicles become more integrated with wireless technology, there are more avenues through which a hacker could introduce malicious code, and more avenues through which a driver's basic right to privacy could be compromised."[203]

1. Reliability

As EDR technology continues to improve, the data retrieved is considered to be accurate in many cases and reliable for its intended purposes.[204] But critics have questioned the data's reliability.[205]

Reliability has multiple components: whether the system will work under a variety of conditions, the accuracy of the information generally, and finally, the integrity and encryption of the data which can be subject to corruption.[206] Black boxes in aircraft are specially engineered to withstand extreme conditions—submersion in water, fire, and major crashes. This engineering may not be as applicable to automobiles, but major road accidents do happen and if the data is to be relied upon, it must be

---

200. *See* Trop, *supra* note 2 (stating that approximately 96 percent of new vehicles sold in the United States have black boxes).

201. *Id.*

202. *See* Browning, *supra* note 164 (noting that the pending universality of EDR use contributes to the ongoing challenges of reliability).

203. Jim Finkle, *U.S. Senator Seeks Information on Carmaker Efforts to Thwart Hackers*, REUTERS (Dec. 3, 2013), http://uk.reuters.com/article/2013/12/03/us-hacking-cars-markeyidUKBRE9B213620131203.

204. *See* Lawrence S. Nordoff, *Accuracy of Various Measuring Tasks for Reconstructionists—Accuracy of EDR Data*, 2 LITIGATING MAJOR AUTOMOBILE INJURY AND DEATH CASES § 30:38 (Oct. 2013).

205. *See* Trop, *supra* note 2.

206. *See* Aditi Mukherji, *Black Boxes in Cars Raise Legal Concerns*, FINDLAW (July 22, 2013, 9:54 AM), http://blogs.findlaw.com/law_and_life/2013/07/black-boxes-in-cars-raise-legal-concerns.html (discussing reliability concerns of black box car crash data).

retrievable under a variety of circumstances. Additionally, anyone today can purchase software to overwrite and erase EDR data.[207]

According to a NHTSA study, "[c]urrent EDR technology can provide very useful information to crash reconstructionists and vehicle safety researchers by objectively reporting real-world crash data . . . ."[208] That same study, however, notes that "[EDR data] should always be used in conjunction with other data sources . . . ."[209] And according to a Toyota spokesman in 2010, Toyota's devices are "experimental and unreliable for reporting crash data."[210]

It seems as though society should care about justice and ensuring that negligent drivers are punished when their driving causes bodily harm. But what about a situation in which an insurance company seeks to admit EDR data because it tends to show that you, the owner and driver, were more at fault even though you are sure that there was a defect in the car because the brake pedal was not responding?

Inaccurate or incomplete EDR data can be detrimental to a plaintiff trying to prove a vehicle defect or a vehicular manslaughter defendant trying to prove innocence. This data has not been used in court enough to establish clear and consistent use and there is still something chilling about the presence of a silent witness in your car that can "testify" against you in court.

2. Cyber Security Concerns

In 2011, researchers hacked into two vehicles as an experiment to prove potential vulnerabilities.[211] The researchers did not have direct

---

207. *See Event Data Recorders: Problems with Ownership, Privacy, and Evidence*, NEWSOMEBLOG (Nov. 2, 2012), http://www.newsomeblog.com/2012/11/02/event-data-recorders-problems-with-ownership-privacy-and-evidence/ (last visited Jan. 5, 2014) (discussing the issue of data integrity).

208. MARCO P. DASILVA, ANALYSIS OF EVENT DATA RECORDER DATA FOR VEHICLE SAFETY IMPROVEMENT, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. 77 (Apr. 2008) *available at http://www.nhtsa.gov/Research/Event+Data+Recorder+(EDR)/Event+Data+Recorder+(EDR)+Research+Applications+of+Articles,+Products+and+Research*. This study analyzed 2,541 EDR files downloaded from databases supplied by NHTSA to assess the accuracy and usefulness of EDR data in crash reconstruction and improvement of vehicle safety systems.

209. *Id.* at 78.

210. Travers, *supra* note 22.

211. *See* Markoff, *supra* note 44.

physical access to the cars but were able to gain remote access and override vehicle controls by undermining the security of the cellular phone inside the vehicle, which subsequently allowed them to send commands to the car's electronic control unit.[212] Although an actual vehicle hacking has yet to be reported, the researchers' experiment demonstrates the capacity of a hacker to remotely control vehicles containing EDRs, cellular connections, and Bluetooth wireless technology.[213]

The auto industry claims to be making cybersecurity a top priority.[214] Senator Ed Markey (D-MA), a member of the Commerce Committee that oversees automobiles, said that "[t]hese threats demonstrate the need for robust vehicle security policies to ensure the safety and privacy of our nation's drivers."[215] But the auto industry may not be the best equipped to protect vehicle owners from hackers. Modern cars with expensive infotainment systems are essentially rolling computers, but according to a security expert, "the average auto maker is about 20 years behind software companies in understanding how to prevent cyberattacks."[216] Until standards for protection are addressed across the industry, car owners and passengers remain vulnerable to attack.

If a hacker did gain access to a vehicle's computer system, a consumer might have a cause of action under consumer protection laws; a court would need to find that the auto maker knew or should have known about its cars' vulnerability to hacking and should have disclosed that vulnerability.[217] A car's computer system may also be a "protected computer" under the Computer Fraud and Abuse Act (CFAA)—the primary federal statute aimed at combating computer crime.[218] The CFAA defines a "computer" as

---

212. *See id.* (noting that the computer hackers did not require any more than a modest amount of expertise to gain control).

213. *Id.*

214. *See* John K. Sutherland, *Automakers Making Vehicle Cyber Security a Top Priority*, THE CHRONICLE HERALD (Jan. 10, 2014), http://thechronicleherald.ca/wheelsnews/1178810-automakers-making-vehicle-cyber-security-a-top-priority (explaining that the auto industry is aware of the potential cybersecurity issues).

215. Press Release, Sen. Ed Markey, As Wireless Technology Becomes Standard, Markey Queries Car Companies About Security, Privacy, (Dec. 2, 2013), *available at* http://www.markey.senate.gov/news/press-releases/as-wireless-technology-becomes-standard-markey-queries-car-companies-about-security-privacy.

216. Balough & Balough, *supra* note 21.

217. *See id.* (comparing a consumer's potential cause of action in the above example to a class action where plaintiffs alleged defendants reasonably should have known about a faulty part in a car and should have disclosed the defect to consumers).

218. 18 U.S.C. § 1030 (2012).

an "electronic . . . high speed data processing device . . ."[219] In modern vehicles, ECMs connect to one another, akin to computers on a network, thus ECUs, EDRs, and other vehicle systems meet this definition of "computer."[220] But in order to fall under the CFAA, these systems must be "protected" computers.

The car or ECUs must be considered a computer "which is used in or affecting interstate or foreign commerce . . . ."[221] Computers probably fit this definition if they are connected to the Internet which is inherently interstate commerce.[222] While cars do travel across state lines, is a car's system really affecting interstate commerce as defined by the CFAA?

Even if a car cannot be considered a protected computer, the path a hacker uses to infect a car's ECU with malware might involve a protected computer. For instance, any time an owner takes a car to a dealership for maintenance, the risk exists that a hacker has introduced malware into the dealer's computer which could then be transferred to the vehicle's computer system. The dealership's computer connects to the Internet and would be a protected computer under the CFAA. Similarly, insurance companies that monitor drivers to reduce premiums, such as Progressive, use computers that are subject to malware which could potentially be transferred to vehicles in violation of the CFAA.[223]

It is unclear whether existing laws provide a viable way to address malicious hacking into automotive computer systems, either as a civil cause of action or criminal offense. Regardless of the CFAA's application, car dealerships and insurance companies must understand the extent to which their systems can affect vehicles which consumers rely on to operate and function normally.

---

219. *Id.* at § 1030(e)(1).

220. *See* Glennon, *supra* note 19 (positing that a vehicle's internal network operates much like any other computer network).

221. 18 U.S.C. § 1030(e)(2)(B).

222. *See* United States v. MacEwan, 445 F3d 237, 245 (3d. Cir. Mar. 9, 2006) (holding that the Internet is a channel and instrumentality of interstate commerce which Congress can regulate because the Internet and interstate commerce are inexorably intertwined).

223. *See supra* Part II.B for a discussion of Progressive Auto Insurance driver monitoring programs.

V. Conclusion

Eventually, most vehicles on the road will be equipped with some type of black box or recording device.[224] One would expect most consumers to be in favor of black box technology because it contributes to safer vehicles and regulations, provides options for lower insurance rates, and assists in developing accurate evidence following an accident. A beneficial side effect of the presence of black boxes in vehicles is that it could actually lead to safer drivers not just safer vehicles. Studies have shown that the presence of recording devices increases driver safety by helping to modify driver behavior.[225] This hinges on the basic fact that drivers must be *aware* of the presence of black boxes in order to be influenced to drive more safely.

This is a key moment in which to anticipate issues surrounding the juncture of consumer privacy and EDRs. The proposed Black Box Privacy Protection Act provides the transparency necessary for consumers to understand the presence of EDRs and their capabilities. But as the law stands today, most consumers are oblivious to the fact that their driving might be recorded. Consumers, at the very least, have a right to know that information regarding their driving may be collected and their actions might be recorded. Everyone wants to reap the benefits of data collection, but when vast storehouses of data are unregulated and personal information is at risk, consumers should be able to opt-in or opt-out.

Consumers appreciate options, transparency, and the knowledge that their privacy is protected. The Fourth Amendment offers a minimum protection of privacy, but the government can do more by legislatively restricting governmental access to records, even if the black box itself is constitutional. As more recording devices are installed in vehicles, and particularly if they are soon mandated in all new vehicles, legislators must take steps to ensure that the privacy rights and interests of citizens are protected.

---

224. *See* Travers, *supra* note 22 (noting the NHTSA proposed rule requiring EDRs in all light-passenger vehicles starting September 1, 2014).

225. *See* Travers, *supra* note 22 (citing NHTSA studies which show crash reductions of as much as 30 percent in vehicles equipped with EDRs); *see also* Harry Stoffer, *Promise and Pitfalls Seen in Black Box*, AUTOMOTIVE NEWS (Sept. 17, 2001), *available at* http://www.autonews.com/article/20010917/SEO/109170720/promise-and-pitfalls-seen-in-black-box (explaining a finding from a panel of industry experts that driver awareness of the presence of black boxes "tends to reduce the number and severity of crashes").