Chicago-Kent Law Review

Volume 90
Issue 3 *Juries and Lay Participation: American Perspectives and Global Trends*
Article 13

6-23-2015

Coming to a Car Dealership Near You: Standardizing Event Data Recorder Technology Use in Automobiles

Kara Ryan
IIT Chicago-Kent College of Law

COMING TO A CAR DEALERSHIP NEAR YOU: STANDARDIZING EVENT DATA RECORDER TECHNOLOGY USE IN AUTOMOBILES

KARA RYAN*

INTRODUCTION

When Timothy Murray, the former lieutenant governor of Massachusetts, crashed his Ford automobile in 2011, he told the police that he was wearing a seat belt and that he was driving within the speed limit.[1] He would have never been caught in these lies or misrepresentations but for the "black box"[2] in his vehicle that revealed a different set of facts.[3] The "black box" disclosed that Mr. Murray was driving over 100 miles an hour and he was not wearing a seat belt.[4]

Event Data Recorders (EDRs) are small metal boxes, approximately four inches by four inches that are installed in automobiles.[5] EDRs are generally installed under the front passenger seat or, in some cases, on the center console or behind the dashboard.[6] Automobile manufacturers can download the EDR data through retrieval tools such as Vetronix's Crash Data Retrieval system.[7] The information that can be downloaded depends on the year, make, and model of the automobile.[8]

* J.D., May 2015, Chicago-Kent College of Law, Illinois Institute of Technology. The author would like to thank Professor Richard Warner for his exceptional mentorship.

1. Jaclyn Trop, *A Black Box for Car Crashes*, N.Y. TIMES, July 21, 2013, http://www.nytimes.com/2013/07/22/business/black-boxes-in-cars-a-question-of-privacy.html?pagewanted=all&_r=0privacy html?pagewanted. =all&_r=0.

2. Dorothy J. Glancy, *Retrieving Black Box Evidence from Vehicles: Uses and Abuses of Vehicle Data Recorder Evidence in Criminal Trials*, 33 CHAMPION 12, 12 (May 2009) ("EDRs borrow their 'black box' nickname from flight data recorders in aircraft.").

3. *Id.*

4. *Mass. Politician Driving 108 MPH at Time of Car Crash*, NBC News (Jan. 4, 2012), http://usnews.nbcnews.com/_news/2012/01/04/9948515-mass-politician-driving-108-mph-at-time-of-car-crash?lite.

5. Glancy, *supra* note 2, at 13.

6. *Id.*

7. *Id.* at 12.

8. *Id.* at 13 (stating that, "Beginning around 1974, General Motors began including event data recorders made by Delphi in a few GM vehicles equipped with air bags. Since the beginning of this century, nearly all cars sold in the United States by General Motors, Ford, Isuzu, Mazda, Mitsubishi, Subaru, and Suzuki have Vetronix EDRs built into them.").

EDRs collect information used for a number of purposes, including improving highway safety by capturing data in the few moments before and after a motor vehicle accident.[9] According to the National Highway Traffic Safety Administration (NHTSA), EDRs record technical information for a brief period regarding the status and operation of a vehicle's systems for the purpose of post-crash assessment of the vehicle's safety performance.[10]

In 2006, NHTSA proposed that EDRs be voluntarily installed by manufacturers in automobiles for safety research purposes,[11] and in 2012, NHTSA proposed stricter requirements, suggesting that EDRs should be mandated in all lightweight cars beginning September 1, 2014.[12] NHTSA estimates that 96% of automobiles manufactured in 2013 are already equipped with these devices.[13] Why were automobile manufacturers so eager to comply with NHTSA's voluntary proposal back in 2006? Automobile manufacturers were eager to comply because the type of information that EDRs collect, such as driving and crash data, is extraordinarily useful to manufacturers in the defense of product liability lawsuits.

There are no prohibitions or limitations on using the data collected by EDRs to create detailed and comprehensive consumer profiles, or to build a specific profile for one individual.[14] The EDRs can track the drivers' movements and destinations. The identity of stores, shops, and other establishments at these locations are ascertained, and, combined with other databases, possess information about the age, gender, and additional characteristics of drivers, to develop consumer profiles. The collection of all this data can also lead to the disclosure of sensitive information. For example, the EDR data can disclose the age and gen-

9. 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), *available at* http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Safety.

10. *Id.*

11. *Id.*

12. *Id.* (discussing that the devices intended for automobiles differ from the "black boxes" on airplanes in that EDRs installed in automobiles presently record information for only a small period of time and do not record any audio sounds or communications between passengers).

13. Press Release, NHTSA Proposes Mandatory Use of Event Data Recorders in Light-Duty Passenger Vehicles. (Dec. 12, 2012), *available at* http://www.automotive-fleet.com/news/story/2012/12/nhtsa-proposes-mandatory-use-of-event-data-recorders-in-light-duty-passenger-vehicles.aspx.

14. FED. TRADE COMM., PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.

der of a driver that visited an identifiable medical facility specializing in a specific area of treatment on specified dates.

With nearly all cars possessing EDRs or cars having the capability for the devices to be installed, Congress must enact legislation to standardize the collection of EDR data because many consumers are not aware of their existence or that EDRs pose a threat to the privacy of the automobile driver.[15] Legislation must address: (1) who owns the information collected from the EDRs, (2) what type of information will be collected, (3) under what circumstances the information can be disclosed to other parties, and (4) how the existence of EDRs shall be disclosed to the automobile owner.

Part I of this paper assesses current state and federal laws enacted to regulate EDRs and the benefits of EDRs, such as how these devices can enhance safety procedures. Part II of this paper addresses what type of information EDRs preserve and the potential risks arising out of the collection of this data. Specifically, this section addresses NHTSA's proposal regarding the type of data that the EDRs will collect and the repercussions of misusing this data. Part III of this paper attempts to balance the benefits of EDRs with the concerns over the loss of privacy associated with EDRs. Part IV of this paper addresses the need for legislation to preempt the area of EDR data in order to establish under what circumstances the data can be collected; who owns the data; and how the existence of EDRs within automobiles will be disclosed to vehicle owners. Additionally, Part IV explores proposed legislation in Congress.

I. EVENT DATA RECORDERS AND THE LAW

EDRs can prevent future crashes and save lives if the collected data assesses and enhances vehicle safety measures. Increasing the amount of information gathered and analyzed will likely enhance vehicle and highway safety. NHTSA states that "EDR data [is] used to improve crash and defect investigation and crash data collection quality to assist safety researchers, vehicle manufacturers, and the agency to understand vehicle crashes better and more precisely."[16] NHTSA anticipates that collecting crash information will lead to further improve-

15. 84 AM. JUR. 3D *Proof of Facts* § 3 (2005).

16. Federal Motor Vehicle Safety Standards; Event Data Recorders, 70 Fed. Reg. 74,144, 74,145 (Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571).

ments in the safety of current vehicles as well as future ones.[17] Using EDRs to assess automobile accidents, NHTSA, prosecutors, and insurance companies can use reliable statistical information retrieved from the EDRs instead of relying on witness accounts. The data provides automobile manufacturers with information to identify and address safety concerns associated with possible defects in the design or performance of their vehicles.[18] The collected information also benefits Automatic Collision Notification (ACN), its successor Advanced Automatic Collision Notification (AACN), and Emergency Medical Services (EMS). AACN informs emergency responders, prior to their arrival at a vehicular accident, as to the potential severity of the crash and the likelihood of individuals sustaining severe injuries.[19] By NHTSA working together with AACN to collect and share data, EMS personnel may obtain enormous benefits in terms of more rapid assessment of injury severity, patient field triage, care, and transport.[20] EDRs have the potential to vastly increase automobile manufacturers', NHTSA's, and AACN's knowledge of automotive collisions and improve vehicle safety for society as a whole.[21] The installation of EDRs will aid in the future development of safer vehicles and reduce crash-related injuries and deaths.

A recent study conducted by the BMW Group clearly illustrates the benefits derived from collecting and sharing the EDR data. The BMW Group researched the implications of collecting vehicular data with EDRs and sharing the information with ACN. According to the BMW Group, ACN is notified if a motor vehicular accident occurs. ACN then notifies emergency responders of the need to render assistance to the individuals in the accident.[22] The information provided by ACN, through EDRs, includes the exact Global Positioning System (GPS) location of the accident and the Vehicle Identification Numbers of the vehi-

17. *Welcome to the NHTSA Event Data Recorder Research Web Site*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., http://www.nhtsa.gov/Research/Event+Data+Recorder+%28EDR%29/Welcome+to+the+NHTSA+Event+Data+Recorder+Research+Web+site (last visited May 10, 2015) ("[EDRs] can make a major impact on highway safety, assisting in real-world data collection to better define the auto safety problem, aiding in law enforcement, and understanding the specific aspects of a crash.").

18. Federal Motor Vehicle Safety Standards; Event Data Recorders, 70 Fed. Reg. at 74,145.

19. *Id.* at 74,152.

20. Elizabeth Garthe & Nicolas Mango, *Scene Triage Criteria Associated with Fatal Crashes and Potential Use of Event Data Recorder (EDR) Data* (Health and Safety Research, Inc., ESV Paper No. 05-0445), *available at* http://www-nrd.nhtsa.dot.gov/pdf/esv/esv19/05-0445-O.pdf.

21. *Id.*

22. *Id.*

cles involved in the accident, which provides the emergency responders with the specific characteristics of the vehicles.[23] ACN technology is helpful for emergency dispatch to recognize the severity of the collision and the extent of injuries so that emergency responders can bring adequate equipment or transport an injured passenger to the appropriate trauma center or hospital.[24] The BMW Group referenced a study conducted by Clark and Cushing, which suggested that a 6% fatality reduction is possible if the time delay for notification of EMS was reduced but the dispatch and treatment methods remained the same.[25] The BMW Group also referred to a study published by NHTSA, which stated that delayed treatment and improper management of the injured patient were two factors that most frequently contributed to avoidable deaths.[26]

A. Common Law and Event Data Recorders

State common laws may be able to provide some protection for consumers' privacy rights. For instance, the Illinois Supreme Court recognized a right to privacy in 1970 in *Leopold v. Levin*.[27] This right can be described as the right to be left alone and is based upon the premise that privacy is one of the fundamental human values that should enjoy the protection of the law under certain circumstances.[28] However, the Court in *Leopold* did not specifically state under what circumstances the right to privacy would be recognized.

For a number of years, the appellate courts of Illinois grappled with the development of a privacy right.[29] The courts focused on the privacy rights adopted by the Restatement of Torts, one of which is a cause of action for intrusion upon the seclusion of another.[30]

However, the appellate courts in Illinois could not agree whether such a cause of action actually existed under Illinois common law. This disagreement was only recently resolved when the Illinois Supreme Court officially recognized the tort of intrusion upon seclusion as one of the torts generally recognized under the umbrella of the right to

23. *Id.*
24. *See id.*
25. *Id.* at 1.
26. *Id.* at 2.
27. 259 N.E.2d 250, 254 (Ill. 1970).
28. *Id.*
29. Lovgren v. Citizens First Nat'l Bank, 534 N.E.2d 987, 988 (Ill. 1989).
30. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

privacy torts.[31] The court stated that, in adopting this tort, it was "join[ing] the vast majority of other jurisdictions that recognize the tort of intrusion upon seclusion."[32] The Restatement describes this tort as "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[33]

In pursuing civil relief for the use of EDRs in vehicles, consumers should encounter minimal obstacles in establishing three of the four elements for this tort as defined by the Restatement.[34] The collection of data by a third party by using an EDR is an intentional act. Establishing that the collection of such data intrudes upon the consumer's solitude or seclusion should not pose an obstacle because of the subjective standard. Similarly, the intrusion involves the private affairs or concerns of the consumer.

However, the fourth element, that the intrusion be highly offensive to a reasonable person, poses more of a challenge. Although the collection of EDR data may be offensive, the intrusion must be highly offensive. Moreover, the fourth element establishes an objective standard is premised upon a reasonable person instead of the subjective beliefs of the consumer. Furthermore, the Restatement sets forth several examples of invasion that are considered sufficient to support the cause of action, such as opening private and personal mail, searching a safe or wallet, examining private bank accounts, or compelling inspection of personal documents pursuant to a forged court order.[35] If the courts adopt this portion of the Restatement, then it arguably would be more difficult to establish a privacy right associated with EDR data because of the distinguishing characteristics between the Restatement examples and EDR devices in automobiles.

B. Event Data Recorders and Limited Protections of the Fourth Amendment

The Fourth Amendment of the U.S. Constitution states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be

31. Lawlor v. N. Am. Corp., 983 N.E.2d 414, ¶ 33 (Ill. 2012).
32. *Id.*
33. RESTATEMENT (SECOND) OF TORTS § 652B (1977).
34. *Id.*
35. *Id.*

> violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[36]

Thus, probable cause will clearly be a sufficient basis upon which governmental officials can access EDR data. However, there also is the preliminary question as to whether Fourth Amendment implications have even arisen in a given situation. One way to answer this question is whether a person has a reasonable expectation of privacy under the circumstances presented. Courts have consistently held that an individual operating an automobile or a passenger in an automobile has a minimal amount of an expectation of privacy with regard to the vehicle. In 1967, the United States Supreme Court in *Katz v. United States* outlined a standard for whether a person has a reasonable expectation of privacy under the Fourth Amendment.[37] A reasonable expectation of privacy exists if a person has an expectation of privacy and society deems the expectation to be reasonable.[38] The Court in *Cardwell v. Lewis* addressed the expectation of privacy further with regard to automobiles by holding that "one has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects."[39]

While this lesser expectation of privacy in automobiles may not hold true for many automobile owners and drivers, the Court in *United States v. Knotts* again reinforced this minimal threshold for conducting a search involving automobiles by holding that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[40] The court in *Knotts* found that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."[41] The Court further explained that the longer-term monitoring would depend on expectations of privacy.[42] For instance, the Court stated that "[l]aw enforcement agents and others . . . could not . . . secretly monitor and catalogue every single movement of an individual's car for a very long

36. U.S. CONST. amend. IV.
37. 389 U.S. 347, 353 (1967).
38. *Id.*
39. Cardwell v. Lewis, 417 U.S. 583, 590 (1974).
40. 460 U.S. 276, 281–82 (1983).
41. United States v. Jones, 132 S. Ct. 945, 964 (2012).
42. *Id.*

period."[43] GPS long-term tracking is very similar to EDR long-term tracking because both use a surveillance system to monitor a vehicle's whereabouts. If long-term GPS monitoring may infringe upon a reasonable expectation of privacy, then it would seem that extending the length of time an EDR can record and store data would impede on an individual's reasonable expectation of privacy. Furthermore, the test produced by the Court in *Katz* has been criticized for producing inconsistent results. "The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable."[44]

Another Supreme Court case that addressed the issue of surveillance and Fourth Amendment protections is *Smith v. Maryland*.[45] In this case, a female robbery victim continued to receive threatening phone calls from a man that identified himself as the robber.[46] The police spotted a man who met the description of the robber's car and discovered that the car was registered to a man named Michael Smith.[47] The telephone company, at the request of the police, installed a pen register to record the telephone numbers Smith dialed from his home.[48] The telephone company implemented the register without the police presenting a warrant or a court order.[49] The register revealed that Smith had placed a call to the woman's phone.[50] Smith attempted to suppress the evidence because the police did not secure a warrant prior to the installation of the register, which he argued violated his Fourth Amendment rights.[51] The trial court denied the motion to suppress.[52] The court of appeals affirmed the decision, holding that "there [was] no constitutionally protected reasonable expectation of privacy in the numbers [that Smith] dialed."[53] Three judges dissented, arguing that Smith had a legitimate expectation of privacy in dialing telephone

43. *Id.*
44. Kyllo v. United States, 533 U.S. 27, 34 (2001).
45. 442 U.S. 735, 736 (1979).
46. *Id.* at 737.
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. *Smith*, 442 U.S. at 737.
52. *Id.*
53. *Id.* at 738.

numbers from his home and that the pen register constituted a "search" within the meaning of the Fourth Amendment.[54]

When the case reached the Supreme Court, the Court turned to *Katz* to analyze the Fourth Amendment protections. The Court noted that according to *Katz*, Fourth Amendment guarantees depend on whether there is a justifiable, reasonable, or legitimate expectation of privacy invaded by government action.[55] Even though the police department requested that the telephone company monitor Smith's telephone, the Court found that because the pen register was installed on telephone company property, Smith could not claim that his actual property was invaded or that the police were responsible for an intrusion onto a constitutionally protected area.[56] The Court also distinguished these circumstances from the facts present in *Katz* by holding that pen registers are significantly less intrusive than listening devices because pen registers only collect phone numbers dialed and not the "contents of communications."[57]

The Court additionally addressed the issue of third party disclosures and their limited protections. In noting that Smith did not have a reasonable expectation of privacy in keeping the numbers he dialed private, the Court further explained that "[a] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[58] The Court relied on another Supreme Court case, *United States v. Miller*, which held that a bank depositor also had no legitimate expectation of privacy concerning financial information once the information was voluntarily disclosed to a bank.[59] Once a person assumes the risk of disclosure, the Court found that it would be unreasonable for that person to expect the information to remain private.[60]

If a court, analyzing Fourth Amendment protections related to EDRs, were to utilize the reasoning in *Smith*, *Katz*, *and Miller*, the court may find that the recording of EDR data does not rise to the level of requiring protections guaranteed by the Constitution.[61] EDR data lacks protections because the "contents of communications" are not record-

54. *Id.*
55. *Id.*
56. *Id.*
57. *Id.*
58. *Id.* at 743–44.
59. 425 U.S. 435 (1976).
60. *Id.*
61. *Id.*

ed, just the numerical data.[62] Using a similar line of reasoning, drivers with EDRs installed in their vehicles would likely be deemed to have no legitimate expectation of privacy because the EDR is the property of a third party, the car manufacturers. As addressed in *Miller*, the Fourth Amendment does not prohibit obtaining information released to third parties even if the information is revealed on the assumption that it will be used only for a limited purpose.[63] Therefore, a government official, without first obtaining a search warrant, may be able to access EDR data by simply requesting that an automobile manufacturer record certain data. While NHTSA would support this argument, there is a key distinction between the fact patterns presented in this case from the concerns associated with EDRs. *Miller* focuses on highly targeted short-term surveillance of a person suspected of a crime, where EDR data focuses on long-term systematic surveillance in mass numbers without suspicion of criminal activities. This distinction may prove to be a significant difference, or over time, it may prove to be insignificant.

There are, however, limited exceptions concerning the third party disclosure doctrine. One such limitation is illustrated in *Ex parte Jackson*, where the Court determined that even though a party's letters were turned over to mail carriers, the contents of sealed envelopes sent via first class mail were afforded Fourth Amendment protection until opened by the recipient.[64] However, the Court limited the exception to only sealed envelopes and to the letter inside the envelope and did not extend protections to cover any address information or other information written on the outside of the envelope.[65] Applying this case to an EDR circumstance may be difficult because if parties normally have access to EDR data, then it is not considered "sealed."

A second exception to the third party disclosure doctrine concerns emails. In *United States v. Warshak*, the Court of Appeals for the Sixth Circuit held that an "[e]mail subscriber 'enjoyed a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial internet service provider (ISP).'"[66] The court went on to state that government officials could not compel a commercial ISP to turn over the content of an email without a war-

62. *Smith*, 442 U.S. at 739.
63. 425 U.S. 435.
64. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).
65. *Id.*
66. 631 F.3d 266, 274 (6th Cir. 2010).

rant.[67] This case illustrates how courts are willing to carve out exceptions to the third party disclosure doctrine for new forms of technology that society deems confidential. As technologies continue to develop, such as with EDRs, courts will have to assess whether the content of technological devices is significant enough to be afforded a reasonable expectation of privacy.

In another more recent case, the Court in *United States v. Jones*[68] assessed whether attaching a GPS to an individual's vehicle constitutes a search or seizure under the Fourth Amendment. In this case, Antoine Jones owned a nightclub that came under suspicion of narcotic trafficking.[69] The government obtained a warrant to attach a GPS device to a car registered in his wife's name.[70] The warrant authorized installation within ten days; however, the device was not installed until the eleventh day, and it tracked the car for the next twenty-eight days.[71] After the government indicted Jones with multiple criminal charges, Jones filed a motion to suppress the evidence obtained through the GPS device.[72] The Supreme Court concluded that the government's installation of a GPS device on Jones's vehicle did constitute a "search."[73] The Court emphasized the importance of property rights by stating:

> Our law holds the property of every man so sacred, that no man can set foot upon his neighbor's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbor's ground, he must justify it by law.[74]

Moreover, the Court distinguished this case from *Katz* in that the reasonable expectation of privacy test has been "added to, but not substituted for, the common-law trespassory test."[75]

Similarly, in *United States v. Knotts*, police officers, with the permission of the chemical company, installed a beeper inside a container of chemicals used to manufacture illicit drugs.[76] The monitoring signals of the beeper allowed police officers to track the car as the chemicals

67. *Id.*
68. 132 S. Ct. 945, 946 (2012).
69. *Id.* at 948.
70. *Id.*
71. *Id.*
72. *Id.*
73. *Id.*
74. *Jones*, 132 S. Ct. at 949 (citing Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.) 817; 2 Wils. K.B. 274, 291).
75. *Id.* at 947.
76. 460 U.S. 276 (1983).

were transported to the owner's property.[77] The installation of the beeper was not challenged, because the beeper had been placed into the container before the container came into Knotts's possession, with the permission of the third party chemical company.[78] Therefore, the collection and utilization of EDR data will align with the "*Katz* Test" because "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis,"[79] and will align with the *Jones* analysis when concerning a search or seizure under the Fourth Amendment.[80]

Although some of these cases may support the general proposition that there is no Fourth Amendment protection afforded to an EDR device within a vehicle, a further evaluation of the holdings is necessary to determine whether the data collected by an EDR falls within the purview of the Fourth Amendment. The Supreme Court in *Lewis* held that there was no Fourth Amendment protection arising from the monitoring of a beeper used to track a vehicle and its contents. Although there is no expectation of privacy arising from the signal generated from a tracking beeper, members of society arguably have a reasonable expectation that personal data, as opposed to a mere signal, maintained in a box unseen by others will not be seized by governmental officials without satisfying the prerequisite of probable cause. However, such a limitation regarding acquisition and use of EDR data is only applicable to governmental officials, and therefore, the Fourth Amendment affords no protection to individuals from private companies collecting, accessing, using, and distributing personal EDR data.

C. Judges Allowing the Use of Event Data Recorders

In *Sipes v. General Motors Corp.*, the court addressed the use of Diagnostic Energy Reserve Module (DERM), which is similar to EDR technology, as evidence in a motor vehicular crash.[81] The plaintiff argued that the airbag in an automobile was supposed to have deployed while the defendant argued that the DERM data demonstrated that this collision was not a situation in which the airbag should have deployed and that the airbag system was functioning properly.[82] The court stat-

77. *Id.*
78. *Id.*
79. *Id.* at 952 (citing United States v. Knotts, 460 U.S. 276, 278 (1983)).
80. *Id.* at 945.
81. Sipes v. Gen. Motors Corp., 946 S.W.2d 143, 147 (Tex. Ct. App. 1997).
82. *Id.*

ed that while the DERM data was certainly strong evidence that the airbag was functioning properly, "it is not irrefutable evidence that conclusively establishes a fact as a matter of law in the face of other contradictory evidence. Our judicial system has never accepted computers or [EDRs] to decide ultimate issues in lieu of courts and juries."[83]

In another case, *Bachman v. General Motors Corp.*, the plaintiffs alleged that the airbag in the defendant's Chevrolet prematurely deployed, which caused a collision.[84] The district court held a *Frye*[85] hearing to assess the admissibility of the EDR evidence.[86] During the hearing, General Motors' experts stated that EDR data is "generally accepted as reliable and accurate by the automobile industry and NHTSA."[87] Both the district court and later the appellate court allowed the data downloaded from the EDR to be admissible under the *Frye* standard.[88] In later years, the courts in *People v. Christmann*,[89] *People v. Hopkins*,[90] and *Matos v. State*,[91] relied on the decision in *Backman* to allow the use of EDR data in courts because it has been generally accepted as reliable in the scientific community. Thus, courts have generally held that EDR evidence is admissible in both civil and criminal proceedings.

D. Current State and Federal Laws Addressing Event Data Recorders

Currently, fourteen states have enacted statutes regulating EDRs.[92] Each of these fourteen states prohibits the downloading of any EDR data without the automobile owner's consent.[93] However, each of these fourteen states also promulgated exceptions that allow the

83. *Id.* at 153.

84. 776 N.E.2d 262, 271 (4th Dist. 2002).

85. Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923) (holding that scientific evidence is admissible if the methodology or scientific principles on which an opinion is based is "sufficiently established to have gained general acceptance in the particular field in which it belongs.").

86. Bachman v. Gen. Motors Corp., 776 N.E.2d 262, 271 (Ill. App. Ct. 2002).

87. *Id.*

88. *Id.* at 271, 282.

89. 776 N.Y.S.2d 437 (Just. Ct. 2004).

90. 848 N.Y.S.2d 460 (N.Y. App. Div. 2007).

91. 899 So. 2d 403, 407 (Fla. Dist. Ct. App. 2005).

92. *Privacy of Data from Event Data Recorders: State Statutes*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/privacy-of-data-from-event-data-recorders.aspx (last updated Nov. 12, 2014) ("Fourteen states—Arkansas, California, Colorado, Connecticut, Maine, Nevada, New Hampshire, New York, North Dakota, Oregon, Texas, Utah, Virginia, and Washington—have enacted legislation relating to event data recorders").

93. *Id.*

downloading and use of data from EDRs, such as pursuant to a court order, for vehicle safety research, emergency medical care, maintenance of a vehicle, legal discovery, and after establishing probable cause related to a motor vehicle offense.[94]

For example, California's Vehicle Code includes a section concerning the disclosure of data from EDRs.[95] California requires disclosure that an EDR has been placed within an automobile by means of a written notice in the owner's manual accompanying the purchase of a new car.[96] California also requires an incorporation of a written disclosure notice into any subscription service agreement.[97] However, some states, including Utah and Connecticut, only require that disclosure of the EDR be set forth in the subscription manual agreement of a new car.[98] Oregon requires no disclosure whatsoever of the EDR at the time a vehicle is sold.[99]

Arkansas also requires notice regarding the existence of an EDR in a vehicle.[100] In 2005, Arkansas passed a law that requires the seller of an automobile to give written notice to the purchaser concerning the presence of an EDR.[101] In addition, if the automobile becomes involved in a motor vehicle accident, the automobile owner has the exclusive rights of ownership to the data.[102] An insurance company also cannot use the data without written consent from the owner.[103] The data can only be obtained by a third party without the consent of the owner in certain circumstances, such as releasing the data pursuant to a court order, an emergency investigation, emergency medical care, medical and vehicle safety research, or to diagnose, service or repair of the vehicle.[104]

However, there are thirty-six states that have not enacted statutes to address the disclosure of EDRs or to state conditions under which third parties may download the data. As previously mentioned the former Lieutenant Governor of Massachusetts, Timothy Murray, was

94. *Id.*
95. *Id.*; *see also* CAL. VEH. CODE § 9951 (West 2005).
96. *Id.*
97. *Privacy of Data from Event Data Recorders: State Statutes*, *supra* note 92 ("In the owner's manual of new cars. Also requires disclosure in agreements with subscription services.").
98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. *Privacy of Data from Event Data Recorders: State Statutes*, *supra* note 92.

involved in an automobile accident in one of the states that has yet to enact a statute governing the use and disclosure of EDRs. Placing aside the protections that may be afforded to the former Lieutenant Governor, there was no specific statutory provision governing EDR data requiring a court order before releasing the EDR data to accident investigators.[105] Hypothetically, if Murray had lived in California, the crash investigator would have needed to obtain a court order to access the EDR data.

All of these statutes demonstrate several important deficiencies. First, there is a lack of uniformity in the purported protections provided to individuals. Second, some states do not even mandate the basic necessity of obtaining a consumer's consent to obtain and utilize data available in EDRs. Third, statutes specifying that consent is required before gathering and using EDR data do not actually compel that actual consent is obtained. Rather, the statutes specify that consent be achieved by providing written notice, such as in the owner's manual or subscription agreement. Many consumers will never read or otherwise be made aware of these notices, and therefore, they will have not knowingly and willingly consented to the gathering, use, and dissemination of EDR data.

II. RISKS ASSOCIATED WITH EVENT DATA RECORDERS

While EDRs have a clear safety aspect, there are dangers that arise from the installation of these devices in all automobiles. One such danger is combining the collection of EDR data with the other massive amounts of information already collected on individuals, leading to the extreme losses in security, privacy, and personal data. This concept is referred to as informational privacy. Informational privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[106] The concept of, and control over, informational privacy continues to evolve as private sector and public organizations build upon databases of collected personal information.[107]

An example of the concerns that arise from the collection of massive amounts of data occurred with the 1965 proposal by the Social

105. Trop, *supra* note 1.
106. ALAN F WESTIN, PRIVACY AND FREEDOM 7 (Atheneum New York 1967).
107. *Id.*

Science Research Council (SSRC) to create a Federal Data Center that would have combined a large amount of government statistical data regarding individuals.[108] Ultimately, the proposals for such a program were rejected because of the privacy concerns over how the information is collected and utilized.[109] Representative Cornelius Gallagher, the former chair of the House Special Subcommittee on Invasion of Privacy, stated:

> [I]f safeguards are not built into such a facility, it could lead to the creation of what I call 'The Computerized Man' . . . . Through the standardization ushered in by technological advance, his status in society would be measured by the computer and he would lose his personal identity.[110]

Almost five decades removed from the SSRC's proposal, our country is still troubled with trying to balance privacy concerns against evolving technological advances associated with computers and the collection of massive amounts of data.[111] In the late 1970s, data collection became a "hot" privacy topic.[112] Federal agencies had begun to compare computerized files to identify federal employees who had provided false information on certain applications.[113] The concerns were no longer just limited to individual privacy concerns, but also to concerns over the potential to use the system as a means of surveillance.[114] In the late 1990s, privacy advocates voiced concerns over financial privacy as banks expanded the amount of information they collected and maintained about customers.[115] The amount of data that has been collected, and that can be collected and stored by both business and government organizations, has significantly increased with the ability of computers to store large quantities of personal data for long periods of time.[116] The control individuals once had over their own personal information continues to diminish as third parties continue to collect larger amounts of personal information.[117] Numerous

108. JAMES RULE & GRAHAM GREENLEAF, GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION 55 (Edward Elgar Publ'g 2008).

109. *Id.*

110. *Id.*

111. RULE & GREENLEAF, *supra* note 108, at 64.

112. *Id*. at 61–62.

113. *Id.* at 60.

114. *Id.* at 65.

115. *Id.*

116. Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH & INTELL. PROP. 1, 3 (2013).

117. Richard Warner, *Undermined Norms: The Corrosive Effect of Information Processing Technology on Informational Privacy*, 55 ST. LOUIS U. L.J. 1047, 1048 (2011).

private organizations now determine in which ways personal information will be collected, how the collected data will be utilized, and to whom the information is distributed.[118]

There is every reason to believe that more aggressive and advanced EDRs will be installed in automobiles as a greater number of parties become interested in purchasing the data being compiled. Such EDR technology already exists on airplanes, passenger ships, and railroad trains, and the array of data that EDRs capture on these vehicles continues to develop as more advanced technology emerges.[119] Airplane EDRs already collect a greater amount of data than EDRs used in automobiles, including the recording of audio transmissions.[120] When EDR technology first was introduced to pilots, the pilots were resistant to the technology for the same reason many oppose the installation of EDRs in automobiles—privacy concerns.[121] The Air Line Pilots Association (ALPA) strongly opposed the EDRs because they were apprehensive about the privacy implications for its pilots, even though the ALPA recognized that EDRs could assist in accident investigation.[122]

As private-sector organizations continue to gain more access to private information through EDRs, individuals will continue to lose control over their personal data. History has shown this to be true. Collection of information used to be limited to less intrusive areas, such as what magazines an individual purchased and read. Now, there is a vast array of information collected about individuals. Greater amounts of data will be collected in the future as the costs associated with collecting the data decrease. The amount of collected data will become increasingly greater and more widespread.[123] This collection of EDR data will also be added to the already-extensive mass surveillance databases.[124] While data collection systems have been evolving since the creation of the computer,[125] individuals, groups, and institu-

118. *Id.*

119. Mary W. Craig, *Thinking Outside the Black Box: How Creative Thinking Turned an Electronic Safety Tool into a Criminal Informant*, 81 TEX. L. REV. 1609 (2003).

120. *Id.*

121. *Id.*

122. *Id.*

123. Patrick Mueller, *Every Time You Brake, Every Turn You Make—I'll be Watching You: Protecting Driver Privacy in Event Data Recorder Information*, 2006 WIS. L. REV. 135, 164 (2006).

124. Warner, *supra* note 117, at 1049–50 (stating that mass surveillance is the use of "[s]ystematically harvested personal information . . . to determine what treatment to mete out to each individual . . . . Whether carried out by government agencies or private-sector organizations, it shapes the ways we approach major institutions and our treatment at their hands.").

125. *Id.*

tions still have the ability to maintain control over EDR data if restrictions are placed on how this data can be collected and utilized.

A. Misuse and Abuse of Event Data Recorder Data

One way in which EDR data is misused occurs in the collection of inaccurate or misleading information and then sold to other third parties. For example, an EDR could collect information on a certain vehicle that has been involved in multiple accidents over a short period of time, but with different drivers other than the owner of the vehicle. In scenario one, the owner involved in multiple accidents of the automobile applies for a particular job requiring the applicant to operate a vehicle as part of his or her job duties. The employer learns about the accident history of the personal vehicle of the applicant and determines not to hire the applicant based upon this information.

Or, in scenario two, the applicant was the driver of the vehicle in each accident, but it was determined that the applicant was never at fault for any of the accidents. Although the sought-after job does not involve any driving as part of the job duties, the employer still decides not to hire the applicant because the employer feels that the applicant must have an aggressive demeanor or personality; otherwise, he or she would not have been involved in multiple accidents.

Or, in scenario three, a car rental company refuses to rent a vehicle to a particular person because EDR data indicates that the individual's personal vehicle has been involved in multiple accidents in the past. However, information that the individual was not the driver of the vehicle at the time of the accidents was unavailable.

In any of these three scenarios, significant adverse decisions affecting a person's life and livelihood were decided based upon information obtained through the misuse of EDRs. The severe consequences to "innocent" individuals are unlimited. The data from EDRs could adversely affect automobile insurance rates. Governments may assess fines for vehicular traffic violations against individuals who were not the drivers of the vehicles at the time of the infractions. NHTSA does not address in its proposed rules the nature and extent that private parties, including car rental companies, may contract for access to EDR data. Because NHTSA has not itself addressed the potential issues in-

volving third parties and EDR data, there are currently no limits on how EDR data can and will be used with rental companies.[126]

B. Insurance Companies Misusing the Information

Many insurance companies now offer premium incentives to their insurers who demonstrate safe operation of their vehicles. For instance, State Farm provides its customers with a discount up to fifty percent on their automobile insurance for being a "good driver."[127] State Farm uses the driver's OnStar, In-Drive, or SYNC communication system to record information allowing the insurance company to determine whether the vehicle's operator is following the rules of the road.[128] Another large insurance company, Progressive, offers a similar program where automobile owners can save premium dollars because of the information Progressive collects.[129] Progressive states that it records information such as the frequency with which a driver abruptly applies the brakes of the vehicle, the number of miles the vehicle is driven, and how often an automobile is driven between midnight and 4 a.m. to assess if the driver is eligible for a discount.[130] While it arguably may be intrusive for Progressive to monitor such factors, automobile owners have the option of not participating in the program.

However, there is an important distinction between the collection of data by insurance companies regarding the operation of a vehicle and collecting personal information with EDRs. Insurance companies collect driving data by installing or providing their own device. This occurs only with the consent of the vehicle operator. Individuals utilizing an insurance company's incentives to receive discounts do so knowing that the insurance company will track and record the operation of their vehicles. The owners of the vehicles, in turn, receive benefits, such as monetary discounts, for giving their consent and participating in the program. In contrast, EDRs installed for purposes other than determining insurance premiums do not provide the vehicle operator a way to opt-out of data collection. EDRs continually monitor and record events associated with the operation of the vehicle and in

126. Federal Motor Vehicle Safety Standards: Event Data Recorders, 77 Fed. Reg. 74,144, 74,153 (Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571).

127. *Drive Safe & Save*, STATE FARM, http://www.statefarm.com/insurance/auto_ insurance/drive-safe-save/drive-safe-save.asp (last visited May 10, 2015).

128. *Id.*

129. *How Snapshot Works*, PROGRESSIVE, http://www.progressive.com/auto/snapshot-how-it-works/ (last visited May 10, 2015).

130. *Id.*

most cases, without the knowledge of the operator. The owner of the vehicle is also not receiving any immediate benefit from the data collection or the sharing of information. It is possible that insurance companies could start requiring EDR data to analyze a driver's past driving history before offering insurance coverage. In that scenario, the EDR data could be used to deny coverage to certain drivers or to increase insurance rates.

C. An Automobile Manufacturer Misusing the Information

General Motors (GM) is one of the largest automobile manufacturers in the world and began widely installing EDRs, and similar data collection devices, in cars beginning in 1990.[131] In 2001, GM identified a defect in its cars' ignition switches.[132] Ignition switch failures can cause brakes and airbags to fail. GM recalled six different car models from 2005 to 2011.[133] In 2009, Mr. and Mrs. Hair lost their twenty-year-old son, Benjamin, when his car ran into a tree two miles from his home.[134] Benjamin's accident left his parents with many questions.[135] The car seemed to have simply drifted off the road and hit a tree on the same road upon which Benjamin had driven almost on a daily basis.[136] Additionally, no other cars were involved in the incident. Unfortunately, the Hairs were unaware at the time of the accident that Benjamin's car was one of the 2.5 million automobiles recalled by GM for an ignition switch defect.[137] The Hairs sued GM for the wrongful death of their son due to GM concealing the ignition switch defect.[138] According to the complaint, Benjamin's car contained an EDR that would disclose if the ignition switch defect contributed to the accident.[139] The complaint further states that GM knew about the EDR and the information it

131. *GM Supports Event Data Recorder (EDR) Mandate to Improve Vehicle Safety*, GM NEWS (Feb. 26, 2010), https://media.gm.com/media/us/en/gm/news.detail.print.html/content/Pages/news/us/en/2010/Feb/0226_edr.html.

132. *Tax Scandals, Lawsuits, and Rotunda Renovations: This Week's News Briefs*, C-VILLE (May 28, 2014, 2:59 PM), http://www.c-ville.com/tax-scandals-lawsuits-and-rotunda-renovations-this-weeks-news-briefs/#.U4i86Ch_j04.

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.*

138. *GM Sued for Concealing Event Data Recorder in Ignition Switch Death of Eagle Scout Ben Hair*, PRNEWSWIRE (May 21, 2014), http://www.prnewswire.com/news-releases/gm-sued-for-concealing-event-data-recorder-in-ignition-switch-death-of-eagle-scout-ben-hair-260149391.html.

139. *Id.*

could provide, but intentionally withheld this information and allowed the vehicle and the EDR to be destroyed after the accident.[140] While large car manufacturers, such as GM, are aware of the critical information EDRs can provide, many individuals remain in the dark when it comes to accessing the same EDR information. So long as individual car owners remain uninformed that their cars contain EDR technology, car manufacturers are able to hide and destroy information that may be detrimental to their company.

D. Future Invasiveness of Event Data Recorders

In the future, more aggressive technology will likely be used to develop advanced EDRs to collect more detailed, specific, and invasive data. For instance, future EDR devices may identify the locations to which the vehicle was driven in the hours before an accident, the number of passengers in the vehicle at the time of an accident, and whether the radio was off or on at the time of a crash. Moreover, personal information concerning communications, including conversations involving an occupant of the vehicle, and whether the driver or another occupant of the vehicle was using a cell phone in the moments preceding a crash may be recorded in future years.

More advanced EDR technology is currently proposed for the airplane and railroad industries.[141] In 2000, the National Transportation Safety Board (NTSB) suggested that the Federal Aviation Authority require cockpits to have video recorders installed.[142] The NTSB said that there have been past investigations with insufficient data to determine the cause of an accident and that if a video camera had been recording images of the cockpit, there might have been sufficient information to make such a determination.[143] There also has been a suggestion that a video camera not only be installed in the cockpit, but that cameras should also be installed in the rest of the plane to monitor activity in other areas.[144] The cameras can record evidence of aggressive or unruly passengers. The video recordings also could resolve issues as to whether a passenger was mistreated on a plane.[145]

140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *See id.*
145. *Id.*

Not only is the airline industry assessing the need for more significant data recording, but the railroad industry is also considering installing digital cameras and microphones on trains.[146] These devices could provide information on the actions and conduct of crew and pedestrians involved in an accident.[147]

We might not be as far away from implementing more advanced data collection as some may believe.[148] In 2012, Congress appropriated $25 million for NHTSA to investigate and analyze "the need for more data from the pre-crash, crash, and post-crash phases" of accidents.[149] As EDRs become more standardized and sophisticated, it is easy to imagine that NHTSA will continue to push for more data collection for longer periods of time. As such, it is likely that newer EDRs will have the technological capabilities to increase the nature and scope of the data recorded and collected. As more data is collected and available for analysis, the greater the value of the information and the greater the number of people that will obtain the information for their own purposes.

III. BALANCING THE BENEFITS OF EVENT DATA RECORDERS WITH PRIVACY CONCERNS

A balancing of competing interests must take place to determine who should access EDR data, the purposes for which the data will be utilized, and any restrictions associated with the data. "[W]e cannot hope to answer [complex balancing questions] until we have a way of ascribing weights to the things being balanced. And that is exactly where parties to privacy debates are most dramatically at odds."[150] Adequate limitations on EDR data cannot be established without first addressing both the privacy concerns and benefits of obtaining EDR data.

Privacy proponents argue that EDR data will be added to the "big data" already compiled on individuals, which will allow third parties to

146. Craig, *supra* note 119 (stating that "[c]ockpit and surface vehicle video recording have the potential to be a very significant investigative tool. However it raises the same issues that earlier recording methods did: what other uses or misuses can the recording be put to and to what extent does the employer's administrative needs trump employees' privacy rights.").

147. *Id.*

148. *Data Modernization Project: Better Data, Safer Roads*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., http://www.nhtsa.gov/Data/DataMod/DataMod (last visited May 10, 2015).

149. *Id.*

150. JAMES B. RULE, PRIVACY IN PERIL: HOW WE ARE SACRIFICING A FUNDAMENTAL RIGHT IN EXCHANGE FOR SECURITY AND CONVENIENCE 183 (2007).

build more extensive consumer profiles.[151] This will further hinder an individual's ability to control his or her personal information. On the other hand, safety and traffic research will reap enormous benefits by analyzing the large amounts of data EDRs will be able to collect. Because there are positive and negative implications concerning EDR data, the ideal solution would be to place reasonable limitations on EDR data collection.

Even the Federal Trade Commission (FTC), an agency whose mission is to protect consumers from invasive technologies, agrees that the accumulation of massive amounts of information can be beneficial.[152] In a 2013 address delivered to the Technology Policy Institute Aspen Forum, Edith Ramirez, Chairwoman of the FTC, highlighted the benefits of "big data" collection, such as the ability to increasingly make precise predictions about weather, deliver better products and services to consumers at lower costs, and improve the quality of health care at lower prices.[153] Ramirez explained that while big data can be extremely useful, the challenges it poses to consumer privacy must be the responsibility of those collecting and using the consumer information.[154] While it would be ideal for the businesses collecting the data to be the ones responsible for implementing safety policies and procedures for collecting the information, businesses' main goals are to make a profit. Automobile manufacturers and those responsible for collecting and extracting the EDR data may not have the consumer's privacy interests as their foremost priority. Thus, consumers will likely need additional protection to ensure that their information is not used in inappropriate or wrongful ways.

If car manufacturers are not able to vigilantly monitor and implement the most stringent privacy policies regarding EDR data, is there another group, perhaps the FTC, better suited for this role? In a speech given by Ms. Ramirez, she advocated that the FTC does have a role in overseeing big data.[155] Under the FTC Act, the FTC's mission is to prevent unfair or deceptive acts or practices that may affect interstate

151. *Id.*

152. Edith Ramirez, *The Privacy Challenges of Big Data: A View from the Lifeguard's Chair*, FED. TRADE COMM. (Aug. 19, 2013), http://www.ftc.gov/sites/default/files/ documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819 bigdataaspen.pdf.

153. *Id.*

154. *Id.*

155. *Id.*

commerce including matters relating to privacy and data security.[156] Such responsibility includes the FTC filing legal action to protect consumers. To date, the FTC has brought more than forty data security cases against companies that have collected large amounts of data.[157] However, while the FTC has the authority to investigate EDRs and the relevant privacy concerns associated with EDRs, it has not brought this issue to the forefront or suggested that it plans to take any action with respect to automobile manufacturers.

IV. LEGISLATION MUST BE ENACTED TO STANDARDIZE USAGE AND DISCLOSURE OF EVENT DATA RECORDERS

In 2011, Congressman Michael Capuano of Massachusetts, along with Congressman Jim Sensenbrenner of Wisconsin and nine additional co-sponsors, filed a Black Box Privacy Protection Act in 2011.[158] The proposed bill would: (1) require automobile manufacturers to notify vehicle owners when EDRs are installed in their vehicles, (2) require manufacturers to disclose the devices' data collection capabilities, (3) make it illegal for any third party to download or retrieve EDR data without the consent of the owner or a court order, and (4) allow the vehicle owner the option to disable the device.[159]

While Congressman Capuano's proposed legislation is a step in the right direction, it goes too far. Congressman Capuano's bill precludes agencies like EMS, AACN, and NHTSA from obtaining EDR data, which is essential to assess safety procedures. Furthermore, Congressman Capuano's bill gives vehicle owners the option to disable the EDR function,[160] which may be an election made by many. If a significant number of vehicle owners opt-out of having their EDR data collected, then there are negative consequences. We are limiting NHTSA's ability to conduct accident reconstruction analysis. The efficiency of EMS and AACN to provide life-saving services is reduced. We also are precluding automobile manufacturers from obtaining data that may help develop safer vehicles.

156. *Id.*

157. *Id.*

158. Press Release, Congressman Michael E. Capuano, Congressman Capuano Introduces Legislation Giving Consumers More Control over Their Car's "Black Boxes" (June 29, 2011), *available at* http://capuano.house.gov/news/2011/pr062911.shtml.

159. *Law Would Stop Your Car from Spying on You*, NBC NEWS (June 24, 2013, 9:18 AM), http://www.nbcnews.com/id/52279217/ns/technology_and_science-tech_and_gadgets/t/law-would-stop-your-car-spying-you/#.U0xNUuZdUXg.

160. RULE & GREENLEAF, *supra* note 108.

While EDRs have obvious safety benefits if utilized in correct ways, a balance must be struck between privacy rights and public safety. More safeguards are needed to ensure consumers are protected against the loss of their privacy. If the privacy issues raised by EDRs are not addressed, there will be a public backlash when these devices become mandatory with minimal or no restrictions on their use.[161] To ensure the public is protected, limitations must be implemented on the utilization, collection, and distribution of the data collected.[162]

Due to the shortcomings of the Fourth Amendment and the need for additional regulation, states have been enacting their own statutes to address the privacy concerns of automobile drivers. Several courts, in addressing and balancing the factors involving technology, have noted that legislation may be the solution. The Court in *United States v. Jones* said, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[163] The Court went on to say that the "[l]egislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[164] While the Court analyzed the legality of GPS devices in *Jones*, EDR devices have some similar characteristics, such as tracking the location of an individual, and the same rationale arguably would be applicable to EDRs. Thus, it seems reasonable that if courts believe that the legislature should enact laws governing GPS data, then the legislature should also enact laws governing EDR data.

Several states have recognized the need for legislation governing EDRs and have passed laws to protect the citizens of their respective states.[165] However, this has resulted in a patchwork of statutes providing for different levels of protection in different states. Thus, there is a need for the federal government to enact legislation that would preempt state laws regarding EDRs, and the public arguably would welcome such legislation. Participants in a survey regarding travel data were asked to identify the three greatest concerns that they have regarding the collection of data.[166] The participants identified the nature

161. Frank Douma & Sarah Aue, *ITS and Locational Privacy: Suggestions for Peaceful Coexistence*, 78 J. TRANSP. L. LOG. & POL. 89, 107 (2011).

162. *Id.*

163. 132 S. Ct. 945, 962 (2012).

164. *Id.*

165. *Privacy of Data from Event Data Recorders: State Statutes*, *supra* note 92.

166. Caitlin D. Cottrill, An Analysis of Privacy in Intelligent Transportation Systems (ITS) and Location Based Services (LBS) 160 (2011) (unpublished Ph.D. dissertation, University of Illinois

of the data, with whom the data will be shared, and the purpose of collecting the data.[167] Utilizing this empirical information and applying it in the context of EDRs, federal legislation should address the following four areas: (1) who owns the information collected from the EDRs, (2) what type of information will be collected, (3) under what circumstances can the information be disclosed to other parties, and (4) the means by which an automobile owner is notified that an EDR is present in the vehicle and collecting data.

First, the legislation should specify that the automobile owner is the owner of the EDR data. This will place individuals in the strongest position to protect their privacy because they own the data, as opposed to automobile manufacturers or insurance companies who want to access the data. NHTSA already stated in both its 2006 and 2012 proposals regarding EDRs that the automobile owner owns the EDR information.

Second, EDRs should only collect information that is deemed essential and relevant to assess a motor vehicle accident. This will limit the intrusiveness of data collection and prohibit the collection of data beyond the intended purpose of enhancing vehicle and highway safety.

Third, the legislation should specify under what circumstances the EDR data could be disclosed to third parties. For instance, the legislation could limit the types of agencies or companies that can have access to EDR data, such as NHTSA, car manufacturers, and AACN. The legislation could also specify that further access and distribution of the EDR information by pre-determined third parties, without the owner's explicit written consent, be prohibited. Thus, third parties would be prohibited from disclosing, selling, or distributing the data to any other individual or corporation. This will ensure that third parties do not later sell collected data to marketing or advertising companies or other third parties who could possibly use the information adversely. Moreover, limitations could be incorporated into the legislation prohibiting distribution of EDR data or using the data in a way that would be deemed inconsistent with analyzing safety procedures. The legislation should also provide that law enforcement can obtain the data with probable cause or that the data can be utilized pursuant to any order entered by a court in any criminal or civil proceeding.

at Chicago), *available at* https://dspace-prod-ib.cc.uic.edu/bitstream/handle/10027/9631/Cottrill_Caitlin.pdf?sequence=1.

167. *Id.*

Lastly, the legislation should state how the presence of an EDR in a vehicle is to be disclosed to the automobile owner. The disclosure requirements or standard should be modeled after Arkansas law, which requires written notice to be provided when the new vehicle is purchased from a dealership, and the notice should also be contained in the owner's manual accompanying the car and any subscription service agreements.[168]

CONCLUSION

After NHTSA's initial proposal was released in 2006, privacy consumer groups, civil rights organizations, and members of the public urged NHTSA to implement stricter regulations concerning who can utilize the information collected by EDRs. Six years later, NHTSA released its modified proposal in 2012, which was criticized for not adequately addressing and reducing the privacy concerns regarding who can assess the collected data.[169] Due to the lack of uniformity between state statues, and NHTSA not adequately addressing privacy concerns involving EDRs, federal legislation must be enacted to address these issues. The use of EDRs cannot be mandated without ensuring that strong privacy safeguards are in place to protect the interests of automobile owners and drivers.

168. *Privacy of Data from Event Data Recorders: State Statutes*, *supra* note 92.

169. Federal Motor Vehicle Safety Standards; Event Data Recorders, 70 Fed. Reg. 74,144, (Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571).