Consumers Union
Publisher of Consumer Reports

Docket Management System
U.S. Department of Transportation
Room PL-401
400 Seventh Street, SW
Washington, DC 20590-0001
Via: http://dms.dot.gov

National Highway Traffic Safety Administration
on
Docket No. NHTSA-02-13546; Notice 1
RIN 2127-AI72
Motor Vehicle Safety Standards:
Event Data Recorders

COMMENTS OF CONSUMERS UNION

Consumers Union submits these comments in response to the Administration's request for comments on the future role of the agency in the continued development and installation of event data recorders (EDRs) in motor vehicles.

I. Introduction

Consumers Union, publisher of *Consumer Reports*, believes that the installation of EDRs in motor vehicles provides enormous potential for increasing road safety. Accurate crash data, and a better understanding of which components of vehicles and of driver behavior are most associated with crashes, unquestionably serve an important societal purpose. However, the installation of EDRs, and more importantly, the collection and distribution of the information these devices record, raise several significant concerns for consumers. Consumers Union believes that NHTSA should take these concerns into account when developing its regulations for EDRs.

In addition, given that NHTSA's goal is to maximize the utility of this data in service of enhanced traffic safety, it is imperative that NHTSA play a central role in the collection, access, and management of EDR data. NHTSA's playing a prominent role will also help prevent improper access to or use of EDR data by third parties.

According to the August 2001 report produced by NHTSA's Working Group[1], the majority of vehicles on American roadways today contain some sort of data capture capabilities.

[1] According to NHTSA's website, the Working Group was made up of representatives from government, universities, the original equipment manufacturer industry, the aftermarket products industry, and the general public.

Washington Office
1666 Connecticut Avenue, N.W. Suite 310 • Washington, D.C. 20009-1039
(202) 462-6262 • fax (202) 265-9548 • http://www.consumersunion.org

Although the precise capabilities of the devices and the elements they capture vary considerably among manufacturers, most of them record airbag deployment, at minimum. But most consumers have no idea that such devices are active in their vehicles. If EDRs are to become a more widespread technology, and if they expand both in their prevalence and in the data elements they capture, it is critical that consumers be informed in a uniform and conspicuous way that their vehicles contain this technology. In addition, given that there are still myriad unknown ways in which this device can and may be used in the future, it is critical that NHTSA consider ways to protect consumer privacy as EDR technology moves forward.

Finally, in order to weigh properly the competing concerns regarding this technology, Consumers Union recommends that NHTSA create a commission to further examine the implications of the widespread installation of this technology in vehicles. This commission should include, among others, representatives from consumer advocacy groups.

We understand that NHTSA believes it has limited authority over privacy issues. However, we respectfully request that the agency not overlook its power as a federal agency to guide and set policy. By incorporating into the final EDR regulations standards concerning encryption and data access, NHTSA may speak to the protection of consumer privacy rights without straying from its legislative mandate and/or the bounds of authority. At a minimum, consumers have the right to know that EDRs are installed in their vehicles, that they are capable of collecting data recorded in a crash, and which parties may have access to this data.

II. Response to Questions

Question 2: Do you believe different types of EDRs should be used for different applications, such as private vehicles and commercial vehicles? If so, why? If not, why not?

We believe that different types of EDRs should be used for different applications. Primarily, different EDRs should be used for private automobiles than should be used for all other types of vehicles (such as commercial vehicles). The justification for this distinction is that while safety data is needed for both types of vehicles, the expectation of privacy is far different for the driver/owner of a commercial vehicle than it is for the driver/owner of a private automobile. In a commercial vehicle (which may be, for example, part of a large fleet of vehicles used for transport), the driver is a professional employee, often with a special license, driving the vehicle in the course of his or her employment, e.g., a truck driver or a shipping company employee. Such individuals are aware that all of the actions they take related to their work are in furtherance of the job requirements, and not for their own personal needs. Put simply, they are aware that the vehicle space is not theirs, but their employer's.

On the other hand, private individuals in vehicles they have purchased for private use have a different relationship to their vehicles. It is true that from a Fourth Amendment standpoint, the Supreme Court has constricted the privacy that an individual can reasonably expect with regard to search and seizure of the car and its contents. But from the standpoint of consumer privacy rights, most individuals are not aware that their vehicles are recording data that not only may be used to aid traffic safety analyses, but has the potential of being used against them in a civil or criminal proceeding related to an auto crash, or by their insurer to increase rates.

Therefore, EDRs in privately-owned vehicles need to collect fewer data elements than those collected by commercial vehicles. They should record only those technical elements needed by NHTSA and other qualified parties for improving traffic safety in general; these elements are detailed in our answer to Question 10 of the request for comments, below. In addition, these data should be collected in a fashion that protects the anonymity of the owner. When transmitted, the data should be divorced from any information that identifies the individual, such as the name, address, or social security number (SSN) of the owner. These personal identifiers are not critical to NHTSA's ability to analyze effectively the cause(s) of the crash, and should therefore not be recorded. In a commercial vehicle, on the other hand, regulating the recording of such personal information is less of a concern, since the event most likely occurred during the employee's work day, where such activity is already recorded in some fashion.

Question 7: Do you have any recommendations for storing and maintaining a national or other database?

Consumers Union believes that any information gathered for analysis from individual vehicular events should eventually rest in a database controlled by NHTSA, and that consumers and/or their legal representatives should have access to this data. Having NHTSA as the central, ultimate repository of this information will help to centralize and standardize any privacy protections or data encryption protocols developed to safeguard the data. Rather than have the data held by various parties, or even among various state or local governments, we believe that both the privacy interests of consumers and the analytical exigencies of improved traffic safety will be best served if NHTSA is the repository for all EDR data (both from private and commercial vehicles).

Question 10: What data elements should be considered for inclusion in an EDR?

The following are the data points the EDR should record:

- Longitudinal and lateral acceleration and principal direction of forces
- Seat belt status by seating location
- Number of occupants and location within/without the vehicle
- Pre-crash data, such as steering wheel angle, brake use, vehicle speed
- Time of crash
- Rollover sensor data
- Yaw data
- ABS, traction control, and stability control data
- Air bag operation data
- Tire pressure data
- VIN (alpha-numeric portion, not 6-digit serial number)

Question 11: Do you have any recommendations for the amount of data to collect, e.g., how long before the crash occurs should the data be collected? How should the data integrity be maintained?

As NHTSA and the IEEE working group note, EDRs only need to record data within a very short window of time before a crash in order to be constructive. Therefore, we recommend

permanent encoding of data for the 10 seconds prior to the crash. We also do not support the recording of data not related to actual crash events.

Deployment of the air bag in a vehicle should be the trigger for crash information becoming permanently recorded by the EDR; all other events that do not trigger air bag deployment should be overwritten by the EDR system. In addition, we believe that the technology that best maintains consumer privacy and minimizes any potential for abuse of EDR data is one that overwrites any recorded data after a certain set period, such as 250 ignition cycles (and which does not allow for access to non-crash-related data prior to overwriting).

Question 12: How should data be collected and stored in a motor vehicle? What measures should be in place to control traceability of EDR data to an actual vehicle or crash, such as EDR IDs or location and date stamping?

The most important issue to consider regarding traceability of EDR data is the balance between protection of consumer (i.e., vehicle owner) privacy and utility of the captured data. To that end, we support EDR IDs that do not contain any personal identification information. That is, the EDR should not collect as part of its data set an owner's name, address, phone number, social security number, license number, or any other information that makes it possible to connect the driving data contained in the EDR to an individual. However, we do believe that when the EDR is installed, it may have the first eleven digits of the vehicle identification number (VIN) of the vehicle coded into it, or alternatively, an EDR identification number which provides critical information, such as the make and model of the vehicle.[2]

Regarding protection of consumer privacy, our concerns are twofold. First, as we have stated above, the most important function of EDRs is the information they provide to improve understanding of vehicle crashes, and how we can make both vehicles and highways safer. Therefore, personal identifiers are not germane to the goals of EDRs. Second, the potential for crash data linked to an individual to be used for other than safety purposes requires that the information reside only with NHTSA. We address potential abuses of EDR data below.

We understand that there may be a need for certain individual pieces of information to be included within the EDR data set to maximize data utility, e.g., the VIN (which itself is linked to personal information about the vehicle owner). The information should be encrypted in a way that is only decipherable by individuals authorized to have access to the data, e.g., NHTSA analysts or verified parties to litigation stemming from a specific crash incident.

Question 16: What damages may result from inappropriate access to EDR data? What roles do technical solutions, such as data partitioning, encryption, and secure databases/vaults, play in addressing privacy concerns?

As mentioned above, there are significant potential dangers that may result from inappropriate access to EDR data. We outline several below.

[2] Inclusion of only the first eleven digits of the VIN will ensure that only necessary information (country of origin, make, vehicle type, gross vehicle weight rating, car line, series, body style, engine, check digit, model year, and assembly plant) is associated with each EDR. The remaining six digits should not be included in the EDR, as they do not bear on crash analysis, and may implicate individual identifying information.

- *Auto Insurance Pricing-Out.* One concern with the availability of extremely detailed crash data is its use by auto insurers. With the increased detail provided by EDRs, insurers may be able to obtain information such as *precisely* how many miles per hour a driver was going prior to a crash. While we do not deny that auto insurers are entitled to base their rates upon a driver's past risk experience in order to better spread risk, we are concerned that the availability of sub-level specific detailed information could be used by insurers to determine future rates in an unfair manner. In addition, there remains the possibility that EDRs may malfunction from time to time. Should an insurer continue to base its pricing decisions on incorrect EDR data, we are concerned that consumers will not have adequate means to ensure that the units within their vehicles are repaired, and that they do not suffer adverse pricing consequences as a result of such malfunction.
- *Insurers Requiring EDRs as a Condition of Coverage.* It is foreseeable that in the near future, many more vehicle manufacturers will start putting more comprehensive EDRs in their vehicles. Since EDRs have the potential to provide detailed data about vehicle behavior (e.g., vehicle speed prior to a crash), there is the possibility that auto insurers may begin, as EDRs become more prevalent, to require an insured to have an operational EDR in their vehicle as a condition of coverage – i.e., auto insurers may refuse to issue coverage unless the consumer has purchased a vehicle with an EDR, or a certain type of EDR, installed. Therefore, we recommend that NHTSA include in its regulations or guidance that auto insurers not be allowed to force consumers to have EDRs installed in their vehicles as a condition of coverage.
- *Public Access to Private Crash Data.* EDR data may well be of interest to engineers, auto safety experts, and analysts from various fields of expertise. Experts in private or academic circles may want to access EDR data in order to further automotive safety and engineering research. However, there is currently no one place where such an expert might go to access these data. The most inclusive existing databases on vehicle crashes reside with NHTSA, insurers, and state departments of motor vehicles. If NHTSA develops such a central repository and the data can be accessed by the public (which we support), it is important that NHTSA maintain the anonymity of drivers in the database.[3] It is also important that NHTSA create and enforce protocols governing how any outside parties may gain access to EDR data, and keep track of which parties have requested such data.
- *Use of EDR Data in Crash-Related Litigation*. One of the most important factors creating a need for thorough consumer education and protection regarding EDRs is their potential use in litigation, both civil and criminal. It is foreseeable that in both criminal prosecution of automobile accidents, as well as in the civil litigation that may result from accidents, parties will seek to discover the data contained in these devices to aid in legal argument. What is more, if the data that EDRs collect become increasingly standardized, it is feasible that EDR data, and the information they may reveal about a driver's pre-crash behavior, will become a vital element in such litigation. Therefore, we believe that NHTSA should not neglect the legal implications of EDR data in considering what standard data elements should be collected. The data elements should advance only the cause of traffic safety, and should neither hinder nor help either plaintiffs or defendants in crash-related litigation. Therefore, NHTSA should ensure that the data elements capture information as close to the actual crash as possible, and not

[3] It is our understanding that academics would be obtaining this data from NHTSA *after* it has been fully encrypted and any personal identifiers have been removed, since they would not be interested in the driving habits of a particular individual, but rather aggregated driving data.

collect data on general driving habits or history. NHTSA should also ensure, through its guidelines, that both plaintiffs and defendants in any potential litigation have equal and easy access to specific crash data contained in an individual vehicle's EDR.

- *Use of GPS and other Locator Devices.* Certain manufacturers, both original equipment and aftermarket, have discussed the possibility of including GPS technology within EDRs. In the event of a car accident, GPS can help to summon aid rapidly to injured individuals. However, absent such exigent circumstances, there exists the potential for abuse of the GPS and the potential to locate a vehicle at any given time. For example, an auto insurer could use a GPS to determine where an insured drives his or her car. We believe, in the interest of consumer privacy, that NHTSA should carefully examine and limit the use of GPS technology in EDRs, and include any such limitations in any rules, regulations, or guidelines it promulgates. If a GPS is functional in EDRs at all, it should only be activated to assist first responders in locating a vehicle after a crash; it should not be functioning other than in crash situations. In addition, we would like the police to be limited by law or regulation to using GPS systems for emergencies like vehicle crashes.

III. Recommendations for National Highway Traffic Safety Administration Action

a) *NHTSA Commission.* Given both the potential utility of EDR technology, as well as the numerous as-yet-unknown consequences of the implementation of these devices, we recommend that NHTSA establish a commission to study fully the practical, "real-world" consequences that will result from the widespread installation of these devices. This commission should include, among others, consumer advocates.

b) *NHTSA Management of Data Access.* Because of the myriad potential uses and abuses of EDR data, it is critical that NHTSA take a management role in overseeing who may have access to the data. NHTSA should remain the central repository for this data, and ensure that if data is accessed by other parties, that it does not contain any personal identifying information. The data should be equally accessible by all parties, whether they be the vehicle owners/drivers themselves, academics, or parties to litigation.[4]

c) *Consumer Notification.* NHTSA states that the utility of EDR technology increases as the device becomes more prevalent in vehicles on the road. As these devices come into widespread use, effective and conspicuous consumer notification about these devices is important.

To that end, we believe that NHTSA should include in any regulations, standards, or guidelines it promulgates protocols for consumer notification. Automakers installing these devices - GM, for example - are discussing EDRs in the owners' manuals that accompany each new vehicle sold. We recommend that new car sellers be required to notify consumers of the EDR when the vehicle is sold; this notification should be mailed separately one to two weeks after a consumer completes purchase of their vehicle. Notice and information to the consumer should also be clear, conspicuous, and comprehensible. This ensures that the information does not get lost either in the owner's manual, or in the flurry of paperwork given to a consumer at time of purchase.

[4] The difference in access by these various parties, of course, is whether or not each would be allowed to view any information that identifies individual drivers/owners.

d) *Downloading Capabilities and Access.* Determining the first party to download the data will determine, in large part, who has access to the data. NHTSA should provide that the data should be downloaded only by the local or state police at the scene of an accident, who will in turn be authorized to transmit the data to NHTSA for analysis and encrypted storage. The individual driver/vehicle owner involved in the accident and his or her legal representatives should also have access to the data. NHTSA's regulations should further stipulate that a vehicle manufacturer, or any private or academic party requiring access to the data can have access to aggregate data, but not to individual information; NHTSA may transmit these data to the requesting parties, leaving out all personally identifying information (*including* VIN or EDR ID).

e) *Protocols for Consumer Redress for Malfunctioning EDRs*. Consumers may suffer potentially serious consequences, economic and otherwise (e.g., insurance pricing, crash-related litigation outcomes), should the EDRs in their vehicles malfunction. Therefore, NHTSA should include in the regulations protocols for evaluating the accuracy of EDR devices. These protocols should include the party or parties responsible (e.g., vehicle manufacturers, NHTSA) for ensuring that the devices are functioning properly. Such protocols will also ensure that the crash-related data NHTSA receives are in fact correct and of use in advancing the cause of traffic safety.

IV. Conclusion

EDRs have an important role to play in enhancing our knowledge of the causes and effects of automobile accidents. However, because they can be designed to capture more detailed information than has previously been available at a crash event, the potential exists for the information to be used in ways that could violate a consumer's privacy interests. NHTSA should use its authority to set forth standards regulating the data elements to be captured by all EDRs. These data elements should be the minimum necessary to enhance traffic safety analyses.

Any information capable of identifying an individual should either not be recorded by the EDR, or should be encrypted. In addition, NHTSA should be the official repository for this information, and should be the source through which parties should seek access to the information. Parties other than the individual/driver involved in the crash and his or her legal representative or local or state police should be required to obtain the driver's permission before being allowed to access the data. These steps will aid in protection of this sensitive information.

May 7, 2003

Respectfully submitted,
CONSUMERS UNION

R. David Pittle
Senior Vice President, Technical Policy

David Champion
Director, Auto Test

Ami Gadhia
Esther Peterson Fellow

Sally Greenberg
Senior Product Safety Counsel