Before the
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION
Washington, D.C. 20590

Docket No. NHTSA-2002-13546

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

February 28, 2003

The Electronic Privacy Information Center (EPIC) respectfully submits these comments on the National Highway Traffic Safety Administration (NHTSA)'s role in the development and installation of Event Data Recorders (EDRs), or "black boxes," in motor vehicles. Our comments focus on the privacy implications of EDR technology.

We recommend that, in order to respect the privacy interests of drivers, the collection of driving-related information through EDRs must follow Fair Information Practices, including obtaining unambiguous or "opt-in" choice from drivers to collect such data. With respect to the proposed EDR database compiled by NHTSA, we recommend that in addition to complying with the letter and spirit of the Privacy Act of 1974, any such database be constructed with the goal of preserving the privacy of drivers so that only aggregate information is collected and made available to third parties.

EPIC is a non-profit research and educational organization that examines the privacy and civil liberties implications of emerging technologies. Our experience in the field has shown that the most effective way to tackle emerging threats to privacy posed by new technology is to craft strong, technologically neutral standards to protect the privacy interests at stake. The comments focus on the key privacy issues implicated by the use of EDR technology and suggests a policy framework of Fair Information Practices to effectively protect the important interests at stake.

Event Data Recorders

Event data recorders (EDRs) are electronic "black boxes" that collect and store information about the operation of a motor vehicle. The data recorded might include the date, time, velocity, direction, number of occupants, airbag data, and seat belt use. The devices might even include location data, which would raise additional significant privacy issues. In addition, there are open questions about how the data can be accessed, recorded and transmitted. There are several different types of EDRs in the market ranging from the Vetronix system, which is installed in cars produced by General Motors,[1] to the more elaborate MacBox system currently being tested by the Drive Atlanta project at the Georgia Institute of Technology. Each type of device collects different kinds of data for different purposes. The NHTSA has attempted to limit the definition of EDRs in the request for comments, but this does not address the public concern about these devices, as the different types of EDRs are available in the market. Any limitation of the purpose of EDRs must be part of a broader privacy protection framework as we argue below.

Advocates of EDR technology suggest that the information might be useful in accident reconstruction and developing safer vehicles through "real world" testing. Insurance companies want the data to settle claims expeditiously. These companies, along with car rental agencies, and others have also demonstrated interest in obtaining this data in support of efforts to control driving behavior through surveillance.

The former head of NHTSA, Dr. Ricardo Martinez, who now runs Safety Intelligence Systems Corporation (SISC), wrote a letter asking NHTSA to consider

[1] Timothy Staab, "Black Box Technology and GM Vehicles", Delta Analysis, at http://www.deltacrash.com/article.htm

mandating the use of EDRs. SISC, which was formerly Loss Management Systems, Inc., aims to find cost effective ways to service insurance claims and simplify investigation and litigation procedures. It has entered into a partnership with IBM and the Insurance Services Office, Inc. to promote a global auto-crash database that envisions a point where "information can be automatically and instantly transmitted from cars" to a centralized database.[2]

SISC supports the MacBox technology behind the Drive Atlanta program at Georgia Institute of Technology. The project also receives funding from NHTSA. The MacBox records location data, voice, and video images of a vehicle in addition to information about the vehicle's operation. It also uses Global Positioning System (GPS) and cellular technology to transmit information about the car back to a central command center. One of the principle researchers behind the project, Dr. Jennifer Ogle, co-authored a paper discussing the potential use of EDR technology in insurance.[3] The study examined the use of variable insurance premiums designed to "discourage risky driving behavior." The report says that, "For example, premiums may increase significantly for vehicle activity above 65 mph, accelerations over 8 mph/second, etc. " The system also tracks how much a person travels to adjust insurance premiums accordingly. The aim is to both punish driving patterns that are considered to be "risky" and to modify driving behavior through the constant surveillance enabled by EDR technology.

Clearly the privacy implications of such a monitoring program are significant. The project currently is being tested with volunteers who are fully apprised of the

[2] IBM, Insurance Services Office, and Safety Intelligence Systems Corporation Press Release available at http://www.accidentreconstruction.com/news/apr02/041702a.asp

[3] Commuter Choice And Value Pricing Insurance Incentive Program, available at http://www.hhh.umn.edu/centers/slp/projects/conpric/projects/gawk.pdf

technology and have consented to being monitored. If EDR technology is mandated by the NHTSA or becomes required through the coercive pricing of insurance rates, there needs to be a very strong set of privacy safeguards established to protect the interests of drivers before any such technology becomes widely deployed.

Signifance of Automobile Privacy in American Culture

Over the past century, ownership of automobiles has expanded from being the privilege of the very elite to becoming essential to the transportation and livelihood of most Americans. Regulating the use of automobiles has become crucial to safety on roads, but along with these regulations, the regulation of private uses of automobiles presents risks to individual privacy. Any intrusion on automobile use has been predicated on the government articulating public safety goals. The use of EDR technology must follow a similar model where any public safety goal is first proven to be necessary and effective and then must be used only in a manner that minimally infringe on the rights of individuals.

Creating A Fair Information Practices Privacy Architecture

The privacy issue concerns not just who "owns," i.e. controls the use of the data (which should be the operator of the vehicle), but the entire set of information practices, including how the data is collected, processed, transmitted and stored. The Organization for Economic Cooperation and Development (OECD) developed robust Privacy Guidelines in 1980, which have been adopted by several countries, government agencies, and corporations. These guidelines would provide an effective framework for addressing

the privacy issues surrounding EDRs as they provide strong, technologically neutral privacy rules.

The Guidelines incorporate eight core principles:

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Purpose Specification Principle except:
   (a) with the consent of the data subject; or
   (b) by the authority of law.

5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle: An individual should have the right:
   (a) to obtain from the a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
   (c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and
   (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8. Accountability Principle: A data controller should be accountable for complying with measures, which give effect to the principles stated above.

There are different EDRs in the market that collect varying amounts of information. A clear purpose specification, for example, would determine what information needs to be collected and would limit the uses of the data for surveillance. There need to be clear guidelines for how the data can be accessed and processed by third parties following the use limitation and openness or transparency principles. Similarly the data quality principle and the security principle provides guidance on the standards for protecting transmission of the information from the vehicle and how the data should be handled to ensure that there is a robust audit trail. The NHTSA needs to conduct further analysis to develop appropriate guidelines following the Fair Information Practices framework. Even if the NHTSA were not to mandate the use of EDR technology, it should consider developing such a framework for vehicles that do have EDR installed.

The Deutsche Akademie Fuer Verkehrswissenschaften (German Academy of Traffic Science) has recently released a report on the use of black box data in German courts.[4] The document proposes limits on the collection of information for purposes such as reconstruction of accidents in civil and severe criminal cases, and grants control of the data to the vehicle operator. NHTSA might consider the German approach, and also build on the experience and expertise of the international community in EDR technology while building its own privacy framework.

[4] German Academy of Traffic Safety Report is available at http://www.deutsche-verkehrsakademie.de/pdf/empfehlungen_2003.pdf

Proposed NHTSA Auto-Crash Database

The NHTSA should follow the letter and spirit of the Privacy Act of 1974 in developing the auto-crash database. We plan to submit comments on the Privacy Act notice, if and when it becomes available. The proposed nationwide database of auto-crash data should respect the privacy interests of drivers by containing only de-personalized information about automobiles in the event of an accident. The privacy of drivers should be protected using Privacy Enhancing Technologies (PETs) during the collection stage, rather than later at the processing stage where although a database administrator might choose to withhold that information, it might still be subject to disclosure. If a particular person is identified with a record there must be strict guidelines for giving access to that information following the Privacy Act.

Conclusion

NHTSA must not mandate the use of black box technology without ensuring that strong privacy safeguards are in place to protect the interests of drivers. Indeed, strong privacy safeguards might further any public safety interests the agency has in EDR technology, by promoting adoption of the technology by drivers who do not feel the presence of these devices are a risk. EPIC encourages the agency to engage in further public discussions to develop a Fair Information Practices framework to cover the use of automobile black boxes. We would be happy to participate in such discussions.

Respectfully submitted,

Mihir Kshirsagar, Policy Analyst
Electronic Privacy Information Center
1718 Connecticut Ave NW, Suite 200
Washington, DC 20009