COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

Joined By

AMERICAN CIVIL LIBERTIES UNION
ADVOCACY FOR PRINCIPLED ACTION IN GOVERNMENT
CENTER FOR DIGITAL DEMOCRACY
CENTER FOR FINANCIAL PRIVACY AND HUMAN RIGHTS
CENTER FOR MEDIA AND DEMOCRACY
CITIZENS FOR PRIVACY IN ALASKA
CONSTITUTIONAL ALLIANCE
CONSUMER ACTION
CONSUMER WATCHDOG
ELECTRONIC FRONTIER FOUNDATION
HOME SCHOOL LEGAL DEFENSE ASSOCIATION
LADY LIBERTY'S CONSTITUTION CLEARING HOUSE
LIBERTY COALITION
PATIENT PRIVACY RIGHTS
PRIVACYACTIVISM
PRIVACY JOURNAL
PRIVACY RIGHTS CLEARINGHOUSE
SECURE ARKANSAS
SECURE THE REPUBLIC
WORLD PRIVACY FORUM

and

MEMBERS OF THE PUBLIC

to the

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Federal Motor Vehicle Safety Standards; Event Data Recorders
49 C.F.R. Part 571
Docket No. NHTSA-2012-0177
RIN 2121-AK86

February 11, 2013

By notice published on December 13, 2012, the National Highway Traffic Safety Administration ("NHTSA") proposed to mandate installation of event data recorders ("EDRs") in "most light vehicles manufactured on or after September 1, 2014."[1] According to NHTSA, EDRs are devices "installed in a motor vehicle to record technical information about the status and operation of vehicle systems for a very

[1] Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74,144 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571) [hereinafter FMVS Standards; Event Data Recorders].

brief period of time (*i.e.,* a few seconds) and in very limited circumstances (immediately before and during a crash), primarily for the purpose of post-crash assessment of vehicle safety system performance."[2]

The agency states that "EDR data are 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."[3] The data stored may be accessed by third parties such as vehicle manufacturers, law-enforcement for post crash investigations, or repair shops for diagnostic purposes.[4] NHTSA concedes that there are significant privacy concerns with the collection of this data: "The agency acknowledges that consumer privacy concerns persist regarding EDR data: Who owns it, who has access to it and under what circumstances, and what are the purposes for which it may be used."[5] But the proposed rule provides no new privacy safeguards associated with the data collection mandate.

Pursuant to NHTSA's notice of proposed rulemaking ("NPRM"), the undersigned privacy, consumer rights, civil rights organizations, and members of the general public ["hereinafter Privacy Commentators"] hereby submit these comments and recommendations to address the substantial privacy risks posed by the agency's proposal. The Privacy Commentators acknowledge the value in EDRs for vehicle post-crash assessment and emergency response. The Privacy Commentators, also acknowledge that NHTSA addresses privacy in the NPRM. However, the agency fails to mitigate against privacy risks associated with EDR data collection, and fails to safeguard vehicle owner and operator personally identifiable information. Therefore, the Privacy Commentators recommend that NHTSA protect driver privacy and limit the collection and use of EDR data. This comment discusses the growing use of EDR data, as well as the various state laws that protect vehicle owners and operators from EDR data collection abuse. The Privacy Commentators specifically recommend that NHTSA: (1) explicitly restricts the amount of data that EDRs collect; (2) conduct a comprehensive privacy impact assessment before mandating EDR installation; (3) uphold Privacy Act protections and grant vehicle owners and operators control over their data; (4) require security standards to maintain the integrity of EDR data; and (5) establish best practices to fully protect the privacy rights of vehicle owners and operators.

I. Problems with EDR Data Collection

A. Auto Manufacturers Collect Large Volumes of EDR Data

EDRs may record "(1) pre-crash vehicle dynamics and system status, (2) driver inputs, (3) vehicle crash signature, (4) restraint usage/deployment status, and (5) post-crash data such as the activation of an automatic collision notification (ACN) system."[6] EDRs can also collect many other data sets, including vehicle location, safety belt usage, data services accessed (*e.g.,* phone use, GPS location, and Vehicle Mobile Services such as Ford's SYNC), and even audio recordings.[7]

---

[2] *Id.* at 74,145.
[3] *Id*.
[4] *Event Data Recorders and Privacy*, EPIC, http://epic.org/privacy/edrs/default.html (last visited Feb. 5, 2013).
[5] FMVS Standards; Event Data Recorders, 77 Fed. Reg. at 74,150.
[6] *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 Feb. 6, 2013).
[7] *CTIA Business Resources*, CTIA, http://www.ctia.org/business_resources/wic/index.cfm/AID/11932 (last visited Feb. 7, 2013).

There is evidence that NHTSA will expand EDR capabilities and data usage. In the *January 2013 Significant Rulemaking Report of the USDOT*, which provides "a summary and the status for all significant rulemakings that DOT currently has pending or has issued recently,"[8] there is a pending rulemaking to expand data collection.[9] The pending rulemaking "would expand the utility of the amount and type of data Event Data Recorders (EDRs) capture in light vehicles in the event of a crash."[10] Additionally, the "rulemaking would make revisions to the optional data elements to account for the latest advances in vehicle safety."[11]

Additionally, NHTSA is conducting a comprehensive review of the National Automotive Sampling System ("NASS") and is looking to update the data collection methods.[12] The agency submitted a notice and request for comments on its modernization efforts of NASS.[13] NHTSA specifically sought comments on the future utility of current data elements, recommend additional data elements and attributes, and anticipated data needs. Several commentators called for increased usage of EDR data and expanded data collection by EDRs.[14] Although NHTSA currently only requires a limited scope of data from EDRs, the agency should now restrict the type of data that will be required pursuant the 2014 mandate. The agency has a responsibility regarding how automobile manufacturers may use the features linked to EDRs to collect non-crash related data on operators that may exceed 30 second intervals.

B. The "Market" for and Amount of EDR Data Collected has Expanded

The EDR proponents argue that the technology will improve safety of vehicles and roadways, but there is a significant potential for secondary uses that threatens to overshadow the original goals. Computing technology in automobiles is creating a new level of data services that vehicle owners and operators may access while traveling in lightweight vehicles. Computing technology is facilitating automation of many driving functions through applications such as cruise control, hands free telephone calling, turn-by-turn directions, and Telematic (satellite) communication based services. The increased use of computing components and telecommunication technology in cars is raising the level of data collection and sharing that is associated with drivers and owners.[15] Many of these technologies provide useful services to owners and operators. But the reuse of the data for unrelated purposes raises substantial privacy concerns.

---

[8] *January 2013 Significant Rulemaking Report*, U.S. DEP'T. OF TRANSP., http://www.dot.gov/regulations/january-2013-significant-rulemaking-report (last visited Feb. 7, 2013).
[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] *DataMod*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., http://www.nhtsa.gov/Data/DataMod/DataMod (last visited Feb. 11, 2013).
[13] National Automotive Sampling System, 77 Fed. Reg. 37, 471 (proposed June 21, 2012).
[14] *See, e.g.*, Toyota Motor North America, Inc., Comments re: "National Automotive Sampling System; Comprehensive Review and Modernization Effort", 4 [Docket No. NHTSA-2012-0084] (July 20, 2012) (suggesting specific data points to collect and connecting NASS-CDS to EDR database); Advocates for Highway & Auto Safety, National Automotive Sampling System Notice and Request for Comments, 3-4 (July 20, 2012); University of Michigan Transportation Research Institute, Comments on National Automotive Sampling System (NASS) Modernization Effort, Docket: NHTSA-2012-0084, 2 (July 20, 2012).
[15] Ford Focus 2013, Operator Manual p. 12-13.

Services such as OnStar leverage the additional technology cars have today to expand upon the data collected and provide real time data collection.[16] The expanded uses include stolen vehicle assistance, remote ignition block, remote door unlock, turn-by-turn navigation, and providing vehicle diagnostics. Insurance companies now use services by OnStar, among other providers, to offer programs that monitor drivers' habits in order to set their premiums.[17]

Programs like State Farm's Drive Safe & Save[18] and Progressive's Snapshot[19] collect the miles driven, acceleration, braking, speeds over 80 mph, and the time of day the vehicle is driven. The data is collected through telematic service providers like OnStar, SYNC, and In-Drive or through the installation of a data collection device into the car's diagnostic port, and the data is used to calculate the premiums for the driver. The Drive Safe & Save and Snapshot programs could incorporate the data now available in cars today, including whether the driver wears a seatbelt and the location of the vehicle. Such data could result in adverse determinations for auto owners and operators.

II. Various State Laws Protect Vehicle Owners and Operators from EDR Data Collection Abuse

Currently, thirteen states have laws that limit the use of EDR data.[20] All thirteen states require vehicle owner or operator express consent before third parties can access EDR data.[21] Additionally, in recognizing that insurance companies desire EDR data, certain states have prohibited insurance companies from requiring access to EDR data. Virginia, for example, prohibits insurance companies from reducing coverage, increasing premiums, applying surcharges, or denying discounts solely because a vehicle operator or owner refuses to grant her insurance company access to EDR data.[22] And Arkansas prohibits insurance companies from requiring EDR data access as a condition of an insurance policy.[23] Connecticut law requires law enforcement to obtain search warrants before accessing EDR data without owner consent.[24] Oregon conditions EDR data disclosure "to facilitate medical research of the human body's reaction to motor vehicle crashes" on the confidentiality of the last four digits of the VIN and the confidentiality of the owner or driver identity.[25] Some states go even further. For example, in Washington, any person that accesses EDR data without vehicle owner consent, and who does not otherwise have authority granted by narrowly tailored exceptions, is guilty of a misdemeanor.[26]

---

[16] Daniel Finnegan & Christopher Sirota, *Is Vehicle Data Recording Auto Insurance's Future?* 4 (2004), *available at* http://www.qualityplanning.com/media/1185/iso.qpc.vehicle%20data%20recording.v5links.pdf.
[17] *How It Works – Overview*, IN-DRIVE, http://www.in-drive.com/sf/howItWorks.html#IL (last visited Feb. 11, 2013); *How Snapshot Works*, PROGRESSIVE, http://www.progressive.com/auto/snapshot-how-it-works.aspx (last visited Feb. 11, 2013).
[18] *Drive Safe & Save*, STATE FARM, http://www.statefarm.com/insurance/auto_insurance/drive-safe-save/drive-safe-save.asp (last visited Feb. 11, 2013).
[19] *Snapshot: How Snapshot Works*, PROGRESSIVE, http://www.progressive.com/auto/snapshot-how-it-works.aspx (last visited Feb. 11, 2013).
[20] *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 visited Feb. 7, 2013).
[21] *Id*.
[22] Va. Code Ann. § 38.2-2213.1 (West)
[23] Ark. Code Ann. § 23-112-107 (West)
[24] Conn. Gen. Stat. Ann. § 14-164aa (West)
[25] Or. Rev. Stat. Ann. § 105.942 (West).
[26] Wash. Rev. Code Ann. § 46.35.030 (West).

Each EDR state law affirmatively protects consumers[27] and treats EDR data as "private," "exclusively owned by the owner of the motor vehicle," and "not [to] be retrieved or used by another person or entity."[28] Taken together, these laws create a substantive basis for EDR data collection best practices:

> **Transparency**— State EDR laws require manufactures of "vehicles sold or leased" that are equipped with EDRs to disclose that fact in the owner's manual,[29]along with the "type of data that is recorded, stored, or transmitted on the motor vehicle event data recorder."[30]
>
> **Control**—State EDR laws permit drivers to control their EDR data by requiring their express consent to access EDR data.
>
> **Purpose Specification**—State EDR laws limit the purposes for which EDR data is used.[31]
>
> **Enforcement**—State EDR laws enforce their provisions.[32]

The best state EDR laws are technology neutral regarding EDR data retrieval, and protect against unauthorized EDR data access through various means.[33] As discussed *infra* section III (E), NHTSA should adhere to state EDR law principles and incorporate state EDR language in EDR best practices.

III. Recommendations for NHTSA Privacy Rule Change

A. NHTSA Should Explicitly Restrict the Amount of Data EDRs Must Collect Pursuant to the 2014 Mandate

NHTSA should affirmatively limit the type of EDR information to which the agency can request access. Current EDR regulations mandate that EDRs record a minimum of 15 data elements.[34] These data elements include "vehicle speed, engine throttle position, brake use, [and] driver safety belt status . . . ."[35] Additionally, vehicles equipped with EDRs that record any of the 28 data elements specified in Table II of 49 C.F.R. 563.7 must capture this information pursuant to NHTSA regulations. In recognizing the increasing demand for EDR data access and EDR technological advances, NHTSA should promulgate regulations that explicitly limit the data elements that the agency will require.

---

[27] *See*, *e.g.*, Wash. Rev. Code Ann. § 46.35.050 ("The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest . . . . A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition . . ." *See also* N.H. Rev. Stat. Ann. § 357-G:1 (VI) ("Violations of this section shall constitute an unfair or deceptive act or practice" under New Hampshire state law).
[28] *See*, *e.g.*, Ark. Code Ann. § 23-112-107 (West).
[29] Calif. Veh. Code § 9951. *See also* Me. Rev. Stat. Ann. Tit. 29-A §§ 1971-73.
[30] Ark. Code. Ann. § 23-112-107 (West).
[31] Va. Code Ann. § 38.2-2213.1 (West).
[32] Colo. Rev. Stat. Ann. § 12-6-402 (b) (West); Wash. Rev. Code Ann. § 46.35.030 (West).
[33] *See*, *e.g.*, Va. Code Ann. § 46.2-1088.6 (West).
[34] FMVS Standards; Event Data Recorders, 77 Fed. Reg. at 74,147. *See also* 49 C.F.R. 563.7, Table I.
[35] *Id*.

Accordingly, the current regulation at 49 C.F.R. §563.7 should be amended to include subsection (c):

> (a) Data elements required for all vehicles. Each vehicle equipped with an EDR must record all of the data elements listed in Table I, during the interval/time and at the sample rate specified in that table.
> (b) Data elements required for vehicles under specified conditions. Each vehicle equipped with an EDR must record each of the data elements listed in column 1 of Table II for which the vehicle meets the condition specified in column 2 of that table, during the interval/time and at the sample rate specified in that table.
> (c) Required data elements explicitly exclude audio and visual recordings. Table I and II represent an exhaustive list of data elements required by NHTSA. Vehicles equipped with an EDR are not required to record additional data elements.

Explicitly limiting the required EDR data elements will help to protect individual privacy.

B. NHTSA Must Conduct a Comprehensive Privacy Impact Assessment Before Mandating EDR Installation

Pursuant to the E-Government Act of 2002, NHTSA is required to conduct a privacy impact assessment ("PIA") before the 2014 mandate goes into effect. Under the E-Government Act of 2002, agencies "shall" conduct PIAs before

> (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that—(I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.[36]

Through the NPRM, NHTSA both mandates that vehicles become equipped with "information technology that collects, maintains, or disseminates information that is in an identifiable form" and initiates a new collection of information adhering to the standards outlined by the E-Government Act.[37] NHTSA's EDR PIA must be "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information"[38] and address the information that EDRs will collect, the purpose of the information collection, NHTSA's intended use of the information, with whom will NHTSA share EDR data, "what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared," how NHTSA plans to secure EDR data, and finally whether a system of records will be created pursuant to the Privacy Act.[39]

---

[36] E-Government Act of 2002 § 208(b)(1)(A), 44 U.S.C. § 3501 (2008), 44 U.S.C. § 3501 note (2002) (Privacy Provisions).
[37] FMVS Standards; Event Data Recorders, 77 Fed. Reg. at 74,145, 74,154.
[38] E-Government Act of 2002 § 208(b)(2)(B).
[39] *Id*.

An EDR PIA is essential to promoting transparency to motor vehicle owners and operators concerning EDR capabilities, including data capture and retention, and audio and video surveillance. The NPRM and current EDR regulations provide conflicting information concerning EDR technological capabilities. For example, NHTSA states that it does not require "recording of data for prolonged intervals" and "EDR requirements . . . standardize EDR recording for an extremely short duration (*i.e*., a few seconds immediately before and during a crash)." [40] The agency, however, also states, "EDRs compliant with Part 563 requirements *continuously record* and seconds later erase data *unless and until* a frontal air bag or in some cases, a side air bag deploys."[41] And although NHTSA states that it currently only requires "very brief" data capture, EDR manufactures have developed "real-time" monitoring technology.[42] So although NHTSA claims its objectives rely on "a very brief snapshot of EDR data in the time period immediately surrounding a crash," it is clear that EDR technology is capable of extensive and prolonged data capture.[43]

Next, the EDR PIA must fully disclose all types of events that enable EDR algorithms to capture and store data. Current regulations require EDRs to "capture and record" data in "frontal air bag deployment" and "side or side curtain/tube air bag deployment" crashes, and other "events" subject to certain conditions.[44] The regulations define "events" as "crash[es] or other physical occurrence[s] that cause [] the trigger threshold [change in speed] to be met or exceeded, or any non-reversible deployable restraint to be deployed, whichever occurs first."[45] The NPRM acknowledges that even "non-crash impacts such as curb and pothole strikes might enable an EDR algorithm and cause it to store data . . . "[46] NHTSA must clarify exactly which events will trigger its data collection before collecting the data. NHTSA should also advance the interest of transparency to motor vehicle owners and operators by directing lightweight vehicle manufacturers to provide clear indication to the operator when EDR technology is engaged and recording or transmitting data.

An EDR PIA will promote transparency and enable oversight. The Privacy Impact Assessment will disclose the scope of the EDR capabilities and provide a basis for a privacy determination.

C. NHTSA Must Uphold Privacy Act Protections and Grant Vehicle Owners and Operators Control Over Their EDR Data

NHTSA should adhere to its own policy that gives vehicle owners control over their data. We the undersigned organizations agree with NHTSA's "longstanding policy" that "treat[s] EDR data as the property of the vehicle owner."[47]

---

[40] FMVS Standards; Event Data Recorders, 77 Fed. Reg. at 74,151.
[41] FMVS Standards; Event Data Recorders ,77 Fed. Reg. at 74,151 (emphasis added).
[42] *MVT 100 Site & Blog*, GOBIZ, http://gobizcorp.wordpress.com/ (last visited Feb. 11, 2013). *See also Feature Spotlight: So Here is How OnStar Works (Infographic)*, GM AUTHORITY, http://gmauthority.com/blog/2011/06/feature-spotlight-so-here-is-how-onstar-works-infographic/ (last visited Feb. 11, 2013).
[43] FMVS Standards; Event Data Recorders ,77 Fed. Reg. at 74,151.
[44] 49 C.F.R. § 563.9 (a)-(b).
[45] 49 C.F.R. §563.5 (b).
[46] FMVS Standards; Event Data Recorders, 77 Fed. Reg. at 74,148.
[47] FMVS Standards; Event Data Recorders, 77 Fed. Reg. at 74, 151.

In addition to this policy, NHTSA states that "[i]n handling EDR and related personal information, the agency complies with applicable provisions of the Privacy Act of 1974 . . ."[48] Because VINs are unique identifiers collected and maintained by a federal agency, VINs qualify for Privacy Act protections. A thorough search in the Federal Register, NHTSA's federal regulations, and both the NHTSA and Department of Transportation websites did not return any results for a Privacy Act system of records notice on the current EDR data that the agency maintains. The agency should therefore immediately make available a Privacy Act system of records notice that discloses the type of personally identifiable information that it maintains on individuals, routine use disclosures, access, amendment, and retention policies pursuant to its current collection of EDR data.

The Privacy Act explicitly bestows certain rights on individuals concerning their information. These rights of the Privacy Act ensure that:

- an agency must give individuals access to the accounting of disclosure of their records;[49]
- any agency or individual to whom the records are disclosed must also receive "any correction or notation of dispute;"[50]
- an individual may request access to records an agency maintains about him or her, as well as have copies made;[51]
- the agency must permit the individual to amend a record about him or her and acknowledge the request in writing within 10 days, as well as timely correct the record if necessary or provide a reason for refusal of the proposed amendment, as well as allow a review of the refusal;[52]
- an agency must make notes of requested amendments within the records;[53]
- an agency must collect records "about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;"[54]
- an agency must "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;"[55]
- each individual must be informed whom the agency asks to supply information;[56]

[48] *Id*.
[49] 5 U.S.C. §552a(c)(3).
[50] 5 U.S.C. §552a(c)(4).
[51] 5 U.S.C. §552a(d)(1).
[52] 5 U.S.C. §552a(d)(2), (d)(3).
[53] 5 U.S.C. §552a(d)(4).
[54] 5 U.S.C. §552a(e)(1).
[55] 5 U.S.C. §552a(e)(2).
[56] 5 U.S.C. §552a(e)(3).

- an agency must publish the establishment or revision of the notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access, contest content, and learn the categories of sources or records in the system;[57]

- assure that all records used by the agency in making determinations about an individual are accurate, relevant, timely, and complete as reasonably necessary to maintain fairness;[58]

- make a reasonable effort to notify an individual when a record about him or her is made available to another individual when it is a matter of public record;[59]

- the agency shall promulgate rules establishing procedures that notify an individual in response to record requests pertaining to him or her, including "reasonable times, places, and requirements for identifying an individual," instituting disclosure procedures for medical and psychological records, create procedures, review amendment requests, as well as determining the request, the status of appeals to denial of requests, and establish fees for record duplication, excluding the cost for search and review of the record;[60]

- an individual may bring civil action in U.S. district court against an agency within two years of the date of the cause of action or within two years of the date of discovery by an individual of misrepresentation by the agency, when it makes a determination not to amend an individual's record according to his or her request or fails to maintain the record with accuracy, timeliness, relevance, and completeness, adversely effecting the individual.[61]

Implicit within these rights is control of individual data. By granting individual access, amendment, and control of personal records held by the federal government, Congress sought to preserve individual privacy and empower individuals to control their information by restricting the amount of information federal agencies could collect and requiring agencies to be transparent in their information practices. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies."[62] Congress also emphasized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[63]

So despite the agency's claim that "it does not have any authority to establish legally binding rules regarding the ownership or use of a vehicle's EDR data," the Privacy Act outlines clear parameters governing NHTSA's use of EDR data and individuals ownership of that data. In mandating the installation of EDRs in most light vehicles, the NHTSA is further expanding the industry-wide data collection regime and must take responsibility for the privacy implications created.

Accordingly, NHTSA should issue best practices, *see infra* subsection E, that acknowledge vehicle owner and operator property rights in EDR data.

---

[57] 5 U.S.C. §552a(e)(4)(G), (H), (I).
[58] 5 U.S.C. §552a(e)(5).
[59] 5 U.S.C. §552a(e)(8).
[60] 5 U.S.C. §552a(f)(1), (2), (3), (4), (5).
[61] 5 U.S.C. §552a(g)(1)(A), (B), (C), (D).
[62] S. Rep. No. 93-1183 at 1 (1974).
[63] Pub. L. No. 93-579 (1974).

D. NHTSA Should Require Security Standards to Maintain the Integrity of EDR Data

One of the ways EDR data is accessed is through the Onboard Diagnostic connector (OBD-II).[64] The OBD-II was federally-mandated to allow access to engine and emissions diagnostics data, but has become a central access point to a number of on-vehicle computers.[65] Most modern vehicles have an OBD-II port located under the dash.[66] The OBD-II port provides access to a number of the internal automotive networks including telematic services such as OnStar, and advance car features such as Roll Stability Control and Active Cruise Control.[67]

NHTSA should support the development of best practices for securing EDR data from manipulation, abuse or misuse. Vehicle owners should maintain control over EDR data both physically as well as legally as several states have done through statutes. The OBD-II is used to download information from EDRs is not universally physically secure, which may allow access and manipulation of EDR data. Further, EDRs, as well as lightweight vehicle's wireless and non-wireless computer systems, are routinely not encrypted. Physical access to the OBD-II is not required to compromise the computer systems of a vehicle and consequently the EDR data.[68] Modern vehicles use a number of wireless devices including Bluetooth and cellular connections that expose the various computer systems in a vehicle to hacking.[69] The same compromising of computer systems in vehicles can occur via the physical port or hacking through a wireless signal.

A set of best practices that guide EDR manufacturers in developing sound cryptography measures to protect information collected, accessed or used would support privacy protection. However, sound cryptographic techniques do not rely upon hiding the cryptographic process, often referred to as an algorithm, from public review. Sound cryptographic processes are made so by the rigors imposed by public disclosure and testing of algorithms, and perhaps even more significantly, by the environment in which the cryptography is implemented.[70]

Strong cryptography should be applied to secure all electronic communications from an EDR or lightweight automobile. Threats to address include: (1) injection of false information; (2) deletion of information; (3) denial of service attacks; (4) vehicle registration identity theft; (4) service identity theft; (5) malicious software; (6) cyber attacks; (7) pranks; (8) and various types of surveillance.[71]

NHTSA should require the physical ports to be secure and the EDR data encrypted in order to protect the security, integrity, and accuracy of the data. The Institute of Electrical and Electronics Engineers ("IEEE") released the IEEE 1616a Standard that provides proper safeguards against data tampering, VIN theft, odometer fraud, and provides standards for protecting EDR data from misuse.

---

[64] Hampton C. Gabler, *et. al.*, *Use of Event Data Recorder (EDR) Technology for Highway Crash Data Anlaysis* 97 (Dec. 2004), *available at* www.harristechnical.com/downloads/nchrp_w75.pdf.
[65] *Id*.
[66] Karl Koscher, *et. al*., *Experimental Security Analysis of a Modern Automobile* 1 (2010), *available at* www.autosec.org/pubs/cars-oakland2010.pdf.
[67] *Id*. at 1-2.
[68] *Id*. at 1.
[69] *Id*. at 4.
[70] BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 21-46 (2d ed. 1996).
[71] *See* Karl Koscher, *et. al*., *Experimental Security Analysis of a Modern Automobile* 13-14 (2010), *available at* www.autosec.org/pubs/cars-oakland2010.pdf.

Additionally, NHTSA should require the wireless systems vehicles use to be encrypted to prevent the compromising of vehicle computer systems and EDR data.

Finally, there should be no assumption that EDR data is accurate and free of error without a universal standard and protocols in place that support a full evaluation of data collection, retention, and use based on the vehicle's make model, computing system (including software), physical details about the crash or incident as well as specifications and the performance record of the EDR device in question. Best practices should warn against refusing access to EDR data for independent investigation of the device or its data. Owners and operators should be able to question the record collected about them and if errors are found they should be a means for correction. Computing devices are not free from errors, for this reason efforts should be put forth to improve on EDR technology and provide greater transparency, accountability, and oversight from manufacturing to data collection, retention, and use.

E. NHTSA Should Establish Best Practices to Fully Protect the Privacy Rights of Vehicle Owners and Operators

In addition to the foregoing recommendations, NHTSA should aggregate the best practices as set out by numerous state laws that seek to protect EDR privacy. It is contrary to reasoned decisionmaking for the agency to mandate massive data collection and not fully amend its current regulations to protect individual privacy. Numerous states, including Nevada, Oregon, Texas, North Dakota, and Washington have implemented strong legislation that upholds EDR privacy. This coalition recommends that NHTSA build upon good state practices and promulgate a set of EDR privacy protection best practices.
The best practices should incorporate the following definitions:

Owner

> (1) A person having all the incidents of ownership, including the legal title of the motor vehicle, whether or not the person lends, rents or creates a security interest in the motor vehicle;
> (2) A person entitled to possession of the motor vehicle as the purchaser under a security agreement; or
> (3) A person entitled to possession of the motor vehicle as a lessee pursuant to a lease agreement if the term of the lease is more than 3 months.[72]
> (4) If a third party requests access to a recording device to investigate a collision, the owner of the motor vehicle at the time the collision occurred.[73]

Access

> Means download, extract, scan, read, or otherwise retrieve.[74]

The best practices should incorporate the following language limiting law enforcement, insurer, and other third party access to EDR data:

---

[72] NEV. REV. STAT. § 484D.485(6)(d). *See also* WASH. REV. CODE § 46.35.010 (1*). See also* TEX. REV. CIV. STAT. ANN. § 547.615 (a).
[73] WASH REV. CODE § 46.35.010 (1)(d).
[74] VA CODE ANN. § 38.2-2213.1

EDR Data Control

> The data on a motor vehicle event data recorder is exclusively owned by the owner of the motor vehicle and may not be accessed or used by any person other than the owner of the motor vehicle without the written consent of the owner. If a motor vehicle is owned by more than one person, all owners must consent to the retrieval or use of the data from a motor vehicle event data recorder.[75]

Insurer Access to EDR Data

> An insurer may not require as a condition of insurability consent of the owner for access to data that may be stored within an event data recorder and may not use data retrieved with the owner's consent before or after an accident for the purpose of rate assessment.[76]
>
> (1) Data on a motor vehicle event data recorder does not become the property of a lienholder or insurer solely because the lienholder or insurer succeeds in ownership of a motor vehicle as a result of an accident.
> (2) An insurer may not condition the payment or settlement of an owner's claim on the owner's consent to the retrieval or use of the data on a motor vehicle event data recorder.
> (3) An insurer or lessor of a motor vehicle may not require an owner to consent to the retrieval or use of the data on a motor vehicle event data recorder as a condition of providing the policy or lease.[77]
>
> Upon petition of an insurer, a court may order that data from a motor vehicle event data recorder be retrieved or used without the consent of the owner of the motor vehicle after an accident if the court determines that:
> (a) The owner has a policy of insurance for the vehicle issued by the insurer;
> (b) The data is necessary to reconstruct the facts of the accident and to allow the insurer to determine the obligations of the insurer under the insurance policy; and
> (c) An accurate and timely determination of the facts of the accident cannot occur without the data.
> (2) A petition under this section must be filed in the circuit court for the county in which the owner of the motor vehicle resides.[78]

Law Enforcement Access to EDR Data

> Data from a motor vehicle event data recorder may be retrieved or used without the consent of the owner after an accident if a court orders the production of the data based on a determination by the court that:
> (1) A law enforcement officer has probable cause to believe that a crime has occurred and that the data is relevant to the investigation of the crime; or

[75] OR. REV. STAT. § 105.928
[76] N.D. CENT. CODE § 51-07-28
[77] Or. Rev. Stat. § 105.932.
[78] Or. Rev. Stat. § 105.938.

(2) A law enforcement officer, firefighter or emergency medical services provider seeks to obtain the data in the course of responding to or investigating an emergency involving the physical injury or the risk of physical injury to any person.[79]

Retrieval or use of data for responding to medical emergency, for medical research or for vehicle servicing or repair.

(1) Data from a motor vehicle event data recorder may be retrieved or used without the consent of the owner to facilitate or determine the need for emergency medical care for the driver or passenger of a motor vehicle that is involved in a motor vehicle crash or other emergency, including the retrieval of data from a company that provides subscription services to the owner of a motor vehicle for in-vehicle safety and security communications systems.
(2) Data from a motor vehicle event data recorder may be retrieved or used without the consent of the owner to facilitate medical research of the human body's reaction to motor vehicle crashes if:
(a) The identity of the owner or driver is not disclosed in connection with the retrieved data; and
(b) The last four digits of the vehicle identification number are not disclosed.
(3) Data from a motor vehicle event data recorder may not be retrieved or used without the consent of the owner to diagnose, service or repair a motor vehicle.[80]

Conclusion

For the foregoing reasons, NHTSA should: (1) explicitly restrict the amount of data that EDRs must collect pursuant to the 2014 mandate; (2) conduct a comprehensive privacy impact assessment before mandating EDR installation; (3) uphold Privacy Act protections and grant vehicle owners and operators control over their data; (4) require security standards to maintain the integrity of EDR data; and (5) establish best practices to fully protect the privacy rights of vehicle owners and operators.

The agency's draft regulation fails to establish privacy safeguards commensurate with the data collection mandate proposed.

Contact: Lillie Coney, EPIC Associate Director; Khaliah Barnes, EPIC Administrative Law Counsel; and Jeramie Scott, EPIC National Security Fellow, Electronic Privacy Information Center (EPIC), 1718 Connecticut Ave., NW, Suite 200, Washington, DC 20009. +1 202 483-1140.

Respectfully Submitted,

Organizations:

American Civil Liberties Union
Advocacy for Principled Action in Government
Center for Digital Democracy
Center for Financial Privacy and Human Rights

[79] OR. REV. STAT. § 105.935.
[80] OR. REV. STAT. § 105.942.

Center for Media and Democracy
Citizens for Privacy in Alaska
Constitutional Alliance
Consumer Action
Consumer Watchdog
Electronic Frontier Foundation
Electronic Privacy Information Center
Home School Legal Defense Association
Lady Liberty's Constitution Clearing House
Liberty Coalition
Patient Privacy Rights
PrivacyActivism
Privacy Journal
Privacy Rights Clearinghouse
Secure Arkansas
Secure The Republic
World Privacy Forum

Individuals:

Kaye Beach
Barb Caffrey
Janine Cicadas
Addison Fischer
Eric Holloway
Anthony A. Huffman
Deborah Hurley
Virginia J. Miller
Jack O'Connor
Samuel Parra
Neil Villacorta
Yolande Williams