International Working Group
on Data Protection
in Telecommunications

675.42.10 4 April 2011

FINAL DRAFT

Working Paper

Event Data Recorders (EDR) on Vehicles

Privacy and data protection issues for governments and manufacturers

49th meeting, 4-5 April 2011, Montreal (Canada)

Scope

1. The fast pace of technological developments in the Information Society (IS) and in Intelligent Transport Systems (ITS) in particular has increased the processing of personal data in vehicles (cars and trucks) both for private and for commercial purposes.

2. The almost universal availability of network access points together with large bandwidth capability now create the opportunity to connect those smart vehicles to the network and to provide access to the data produced. This emerging technological trend will make the smart vehicle one of the components of the so-called Internet of Things.

3. Without appropriate privacy and data protection safeguards, drivers as well as passengers of "smart vehicles" may not have the ability to control or at least monitor their data processing, and even be unaware that such processing is taking place.

4. Although technological applications in the automotive sector are diverse, this paper considers only those aspects related to the data of the event recorder (EDR).

EDR: Definitions and facts

5. In the event of a vehicle crash or accident, data obtained from sensors are recorded via an onboard device, generally called an "Event Data Recorder" (EDR). EDRs typically process data during a limited timeframe covering only the vehicle crash, accident or serious incident (immediately before, during and after the event).

6. The EDR can be introduced into the vehicle during the production process or added later (aftermarket EDR). The recorded data can be downloaded using computer software which is not always commercially available to end users.

7. The data collected and registered in case of an accident does not simply reflect the technical status of the vehicle (fuel consumption, airbag functionality) and the time of the crash, but they will also register and describe (directly or indirectly) in a dynamic way the driver's behaviour (e.g., brake oil pressure at the beginning and end of braking, vehicle speed, including during braking, engine speed, percentage throttle, use or not of safety belts).

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

8. They are, therefore, personal data related to the driver and, in some cases, passengers (e.g., the information concerning the use of seat belts).

EDR coupled with other on-board systems

9. Based on agreements with mobile service providers, EDRs are being linked to onboard communication systems which transmit the relevant information to a remote location when the event occurs. A collision notification system (or in-vehicle emergency call system) can therefore be activated automatically or manually and provide data to emergency services. Initiatives have been launched in the US[1] and in the EU[2] in order to promote the implementation of such systems and to enforce standards across the different transport sectors and applications.

10. In order to get more evidence of an accident, sometimes EDRs are also associated with onboard cameras (Video Event Data Recorder-VEDR) which significantly increases the collected information related to the driver's behaviour and to third parties involved in the accident.

Driver-related personal data and the use of EDR

11. Driver-related personal data collected and transmitted via EDR (and also via a VEDR), especially when associated with electronic communication and localisation systems, offer numerous possible uses to a growing number of stakeholders:
    a. manufacturers, drivers (as well as other individuals affected by car accidents), owners (e.g., in the car rental or fleet management sectors) and insurance companies, could use EDR data as evidence in order to check the accuracy of witness statements in cases of litigation;
    b. police and other enforcement authorities (e.g., authorities in charge of car safety could use the information to complement other sources of information related to a vehicle accident);
    c. employers, for organisational or security reasons;
    d. insurance companies, to cluster the consumers and offer particular tariffs (e.g. "pay as you drive" or even "pay where you drive");
    e. researchers (particularly vehicle and road safety sectors could use these data in order to improve the design of road infrastructures);
    f. marketing organisations which could fine tune consumer behaviour analysis based on EDR data and deliver highly tailored advertising, or other organisations offering services based on the level of risk identified through the analysis of such data.

12. The above developments require a careful consideration of the rights to private life and data protection for drivers as well as for other potential passengers. An appropriate balance with other individual rights and interests, as well as with the public interest in the safety of the transport network must be established.

---

[1] The US National Highway Traffic Safety Administration (NHTSA) in August 2006 ruled (49 CFR Part 563) that manufacturers were not required to install Event Data Recorders in new vehicles. The NHTSA however required manufacturers who install EDRs to include a minimum standard set of data to be recorded: at least 15 types of crash data including pre-crash speed, engine throttle, brake use, measured changes in forward velocity, driver safety belt use, airbag warning lamp status and airbag deployment times. Manufacturers have until September 2012 to comply with the standards defined by the NHTSA. http://www.nhtsa.gov/EDR

[2] The European Union "*E-call initiative*" is detailed in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, eCall: Time for Deployment*, Brussels, 21.8.2009, COM(2009) 434 final; http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm.

13. In 2008, the European Commission issued a Communication describing an ITS action plan[3] for Europe together with a proposal for a directive recently adopted by the Council and the European Parliament[4]. This Directive, which will have to be implemented in Member States by February 2012, encourages the use of anonymous data where appropriate for the performance of Intelligent Transport Systems applications and services[5]. Data protection and liability figure among the priority areas of the action plan and the Directive which aim at supporting more efficient, environment-friendly, safer and more secure freight and passenger mobility within the European Union.

14. The Research and Technological Development Framework of the European Union has launched a large number of RTD projects which have been finalised or are still being carried out with a view to enhancing road safety.[6] In some jurisdictions, laws have been proposed[7] or have already adopted to address (*inter alia*) the drivers' privacy issue in the context of EDR[8] or proposed.[9]

15. Simultaneously Data Protection Authorities are noticing the increasing introduction of EDR and other smart vehicle technologies to support vehicle fleet management.[10] In the case of the European *E-call* initiative, the Article 29 Working Party has already made a series of recommendations[11].

16. The timing of a large scale implementation of these tools, the complexity of the topic and the considerable investment needed (possibly also in road infrastructures) give urgency to a clear regulatory framework, although this should not occur without an extensive public debate. The principle of "P*rivacy by design*" should be inherent in the development and clarification of this framework[12].

17. Against this background, the Working Group

---

[3] Action Plan for the Deployment of Intelligent Transport Systems (ITS) in Europe (COM(2008) 886)

[4] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transports and for interfaces with other modes of transport, OJ 2010, L 207/1.

[5] Art. 10(3) of Directive 2010/40/EU.

[6] See *Intelligent Car Brochure*, p. 16 at http://ec.europa.eu/information_society/activities/intelligentcar/docs/right_column/intelligent_car_brochure.pdf.

[7] See, at federal level, the attempt done with *The Motor Vehicle Safety Act of 2010* (H.R. 5381).

[8] California was the first state to enact such legislation requiring manufacturers to disclose to customers whether event data recorders or "*black boxes*" are installed in vehicles. For privacy legislation related to Event Data Recorders ("Black Boxes") in Vehicles search the National Conference of State Legislatures website at http://www.ncsl.org. More detailed information on the state of the play regarding EDR in the U.S.A. can be found at the National Highway Traffic Safety Administration website (http://www.nhtsa.gov/EDR).

[9] See, at federal level, the attempt done with *The Motor Vehicle Safety Act of 2010* (H.R. 5381).

[10] French DPA (CNIL), Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme public ou privé; Délibération 2010-096 du 8 avril 2010 portant recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules; Italian DPA (Garante per la protezione dei dati personali) on Geolocation in Public Transportation and Passenger Security, 5th of June 2008, in http://www.garanteprivacy.it, doc. no. 1672796.

[11] Article 29 Working Party, *Working document on data protection and privacy implications in eCall initiative*, WP 125, at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_en.pdf

[12] See ISO/TR Technical Report 12859 on Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems

calls

on regulators, in co-operation with Data Protection Authorities and the relevant industry stakeholders, to

a) set forth, clarify or confirm urgently an appropriate legislative framework (in order to establish the lawfulness of the data processing and to prevent or mitigate unauthorised use of the personal data collected and/or transmitted by EDR and, possibly, other smart vehicle technologies) and
b) promote the adoption of the relevant technical standards

recommends

I. Transparency

The data processing carried out through EDRs (and other smart technologies) in vehicles should be *completely transparent* to the vehicle's owner and user(s). Users should be put in a position to easily understand what items of personal information concerning them are collected and stored, as well for what purposes they are sought.

To this end:

a. *manufacturers/integrators* should make customers aware of the processing of personal data in the vehicle including any ability to locate the vehicle's position. A notice (written or voice) should be present in the vehicle. Clear and detailed information shall be provided via the owner's manual;
b. *data controllers* (such as employers, insurers, car rental companies, etc.) should fully inform the users regarding (i) the purpose(s) of the processing for which the data are collected; (ii) the category of the personal data processed; (iii) the recipients or categories of recipients of the data; and (iv) their access rights

II. Owner's consent

As a rule, devices capable of storing personal data onboard should only be activated with the free and informed consent of the owner and after the user(s) have been informed. Mandatory installation of onboard devices capable of storing and communicating personal data to third parties requires an appropriate legislative basis that clearly identifies the envisaged purpose(s) of the recorded personal data.

III. Data quality

EDRs should only store personal data which are adequate, relevant and not excessive in relation to the purpose(s) for which they are processed. The use of anonymised data should be preferred wherever possible.

Decisions following an event relating to the vehicle should not be taken solely on the basis of information gathered through an EDR. In order to better analyse their quality, the data collected must be interpreted by certified experts and carefully evaluated along with all other relevant evidence and circumstances.

IV. Privacy by Design

Privacy by Design should be the guiding principle of any development and implementation of EDRs and other similar technological device built into a vehicle (or interacting with a vehicle). Such systems should therefore be designed to minimise the need for processing personal data and to prevent the potential abuses of that personal data.

V. (Personal) Data Access

Before any implementation, privacy issues should be considered in order to clearly identify who can access the personal data recorded in the EDRs and under which conditions (e.g. judicial warrant), particularly with regard to data subjects other than the driver, to whom (in principle) full and free access to his/her own data should be recognised. Appropriate and clear procedures should be established in order to allow data subjects to properly exercise their rights. A privacy and data protection impact assessment is considered as a useful tool for this analysis.

VI. Data security and integrity

Standardized data security measures to prevent unlawful access, alteration or loss need to be defined and universally adopted. Robust cryptographic techniques and proper authentication systems should be used to limit the risk of unintended data transfers or harmful attacks. The end-user should be able to verify, in a straight-forward manner, that EDRs and similar devices implemented in the vehicle are in full compliance with these standards. In a context of interconnected devices, stringent security measures are even more essential.

VII. Employee monitoring

In addition, laws relating to employee monitoring should be taken into account and fully respected when the employer installs devices which permit the monitoring of the driver's behaviour as well as the detection of the position of the vehicle (e.g. Journey Data Recorder or localisation systems).