available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Mandatory implementation for in-vehicle eCall: Privacy compatible? ☆

Christophe Geuens, Jos Dumortier

ICRI, The Interdisciplinary Centre for Law & ICT, K.U.Leuven, IBBT, Belgium

Keywords:
In-vehicle eCall
Privacy, art. 29 Working Party
Data protection
PETs
2004/52/EC Directive

ABSTRACT

This article examines whether there are any objections to implementing a mandatory eCall system in the Community and how these could be dealt with. It starts with a short introduction to the motives why the European Commission considers a mandatory in-vehicle eCall. The art. 29 Working Party has issued a working document on eCall identifying several issues regarding personal data protection. The issues in this document will serve as a reference to determine whether there are any objections regarding data protection to implementing a mandatory eCall system. Additionally we will look at a possible eCall implementation in the Community.

1. Introduction

In-vehicle eCall is defined in the eCall Memorandum of Understanding as follows:

> *The in-vehicle eCall is an emergency call generated either manually by vehicle occupants or automatically via activation of in-vehicle sensors. When activated, the in-vehicle eCall system will establish a voice connection directly with the relevant PSAP (Public Safety Answering Point), this being either a public or a private eCall centre operating under the regulation and/or authorization of a public body. At the same time, a minimum set of incident data (MDS) will be sent to the eCall operator receiving the voice call.*

In-vehicle eCall systems have been available for quite some time but they have never really been adopted by motorists. To this day, they have been available only as an optional component, often part of a bigger package of commercial services. One such example is OnStar of GM, which apart from offering an eCall service also offers turn-by-turn navigation, stolen vehicle assistance, remote door-unlock, roadside assistance and other options. Other manufacturers such as PSA (Appel d'Urgence), BMW (Connecteddrive) and Volvo (OnCall) have their own system available. It is however not uncommon to find these services limited to the premium cars on the market or to a specific geographical market and mostly even to a specific brand. OnStar for that matter is only available in North America and on cars build by GM. In addition, none of these systems are interoperable. This lack of standardization is one of the major factors why eCall has yet to blossom in Europe. In addition there is also the cost of purchase and the cost of the subscription to the service.

For some time, the European Commission has been considering the mandatory implementation of eCall. In 2006, the European Parliament adopted a report by Gary Titley to bring eCall closer to the citizens (Titley, 2005). An in-vehicle eCall would reduce road fatalities with about 2500 deaths every year and the severity of accidents with 15% by reducing the response time of the emergency services in urban areas with 40% and in rural areas with 50%. This response time is reduced because the emergency services are notified instantly in case of an accident and are given the exact location of the

☆ This work relates to work done in the Flemish IBBT Next Generation ITS project: http://www.ibbt.be/en/project/nextgenits. First presented at the 4th International Conference on Legal Security and Privacy issues in IT Law (LSPI) Malta 3–5 November 2009.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2010.03.009

accident. Additionally, it would reduce the external cost of road traffic accidents with about € 4 billion every year. The overall reduction of costs resulting from road traffic accidents in the Community could even be as much as € 21 billion every year. Because of these presumed benefits, the Commission would like to see a higher degree of implementation for eCall and at this time it only seems possible through a mandatory implementation.

There is however strong resistance against in-vehicle eCall, especially if it would be made mandatory on all new cars in the Community. This resistance stems from fear for invasion in private life and risks regarding personal data. An in-vehicle eCall consists among other components of GNSS. To provide information on the accident location, the in-vehicle eCall aggregates previous vehicle positions. These aggregated data provide the current location of the vehicle but also the direction it is heading in to allow emergency services to locate the vehicle accurately. Only the three most recent vehicle positions are used by the system, but apart from the geographic location this position might also contain a digital time-stamp. The different locations and their associated digital time-stamp could be used to calculate the average speed over a certain distance, as is done now with average speed cameras in places such as London and Amsterdam. These cameras are located at certain intervals on the motorway and they record license plates of vehicles. For each interval the system registers the travel time and from that travel time the average speed can be calculated. This average speed calculation might have considerable consequences for the occupant or occupants of the involved vehicles. These consequences could be prosecution for traffic offences but also render void the insurance policy covering the accident damage. Additionally it could allow for the continuous monitoring of the movement, through the GNSS-component, of the vehicle in which the eCall is installed. This monitoring could lead to extensive profiling of a person's movements and deduction of different kinds of information there from. These concerns regarding data protection are addressed in the working document of art. 29 Working Party.

It is, however, not given that road safety solutions (seat-belts, crash helmets, ABS, eCall…) are an invasion of private life. In a Decision of 13 December 1979 in the case X. v. Belgium the Commission of Human Rights declared an application regarding mandatory seat-belt laws inadmissible. According to the Commission, mandatory seat-belt laws are part of a legislative body that aims at preserving the public from different kinds of danger and preserving society from the associated harm, such as the costs resulting from road traffic accidents. Pedestrian crossings are another example. Such legislation never affects the 'private life' of a person, regardless of how wide one interprets private life. There must be specific issues relating to data protection or private life, in X. v. Belgium impose seat-belt use, the mere fact that one regulates human behavior is not sufficient to draw that conclusion. For in-vehicle eCall there are 'private life' issues because the driver of the vehicle could be tracked continuously, which will however not be the case, and upon activation of eCall there is a transmission of personal data.

2. The art. 29 Working Party working document

The Working Party issued a working document on the data protection issues of eCall on 26 September 2006 (WP 125). It has issued this document as a result of the ongoing work on European level regarding eCall, most notably the Memorandum of Understanding and the European Parliament Resolution on bringing eCall closer to the citizens (2005/2211 (INI)). The Working Party recognizes the benefits of eCall but also identifies certain data protection issues, which it would like to be given the appropriate attention. Therefore it thought it necessary to address these issues in a working document.

This document is regarded by some as providing accurate guidelines concerning eCall within the Community legal framework. It highlights the issues to personal data for two different types of eCall services: a voluntary service and a mandatory service. Although the Working Party expresses its preference for a voluntary service, this article tries to show how a mandatory system could be implemented rather than waiting for the market to fully adopt the voluntary system (McClure and Graham, 2006). Therefore it looks at different sources on personal data protection and eCall, from both legal and industry side.

3. Addressing the issues of the art. 29 Working Party

One essential part of the working document is that the Working Party does not accept any eCall system that would allow a constant tracking of the user. Nevertheless, the Working Party could accept a system that stores the three most recent locations of the vehicle but requires an external factor to transmit the data. Such an external factor could be a manual activation by one of the occupants or an incident such as a road traffic accident. Without that external factor, there may be no transmission of data and eCall should remain disconnected from the network. Such a system is referred to by the Working Party as a 'sleeping' system. The working document seems to express four issues concerning personal data protection in an eCall service. First of all, the principles of data protection legislation must be upheld. Secondly, Privacy Enhancing Technologies should be incorporated in the service. Thirdly, users should be protected from illegitimate tracking and abuse of the service. Finally, there should be a legal intervention from the European Union. These issues will be discussed consecutively.

3.1. *Parenthesis*

One could ask the question why a commercial in-vehicle eCall system, as offered by different manufacturers, seems a lot less problematic than a mandatory one as discussed. The main difference is that the commercial systems are sold by mutual agreement which makes it much easier to comply with data protection legislation. Consent is one of the grounds for processing of personal data and this consent could be obtained in a mutual agreement (art. 7(a) 95/46/EC).

Both parties enter into the contract providing eCall services by mutual agreement. Application of data protection rules also implies that the service providers must foresee the possibility of revoking consent for the processing of location data and thus turning the system off (art. 9.2 2002/58/EC). In a mandatory eCall, this phase of interaction between the parties is taken out and people can only accept that they have the system present and operating in their car. The user has no say in the matter contrary to the commercial systems. This could explain the difference between the approach of commercial eCall and mandatory eCall.

3.2. *Uphold principles of data protection legislation*

The principles referred to are those held in the Data Protection Directive and other applicable directives. This Directive is the general Directive on processing of personal data within the Community. It states different grounds for a legitimate processing of personal data (art. 7 (c)–(e) 95/46/EC). Processing is allowed for the execution of a legal obligation to which the controller is subject. This could be the basis for a mandatory eCall system imposed by law. But then we must ask the question whether a government could issue legislation imposing such a system, which entails an infringement upon the private life of people. Relevant in this regard is case law referring to art. 8 ECHR (recital 10 95/46/EC; art. 37 EU-Treaty). This article is the basis for the protection of privacy within the Community and the national legislation of the Member States. It holds cumulative conditions for infringing measures. This means that if one condition is not fulfilled the measure is inadmissible under art. 8 ECHR as set out in Malone (1984).

Restrictions on the right to privacy, in case determining where someone is at a given point in time, require a law that is 'accessible and foreseeable' (Gomien, 2002). 'Accessible' refers to the fact that the law is published in such a way as to be accessible to those who could be subjected to it as was demonstrated in the case of Rotaru (2000). According to Malone (1984), 'foreseeable' refers to the fact that the subject can determine the circumstances and conditions when he could be subject to the law. Rotaru (2000) clarifies this by stating that the law must be formulated with sufficient precision as to allow any individual to regulate his conduct.

With regard to an eCall system, this seems to imply that the law must clearly state when one is tracked by an eCall system and when one will not be tracked. In addition to 'accessible and foreseeable' the interference must be 'necessary in a democratic society'. The Court determines this by considering whether the aim of the interference is legitimate and whether the means of restricting are proportionate to the aim of the measure (Gomien, 2002). When determining the legitimacy of the aim, the Court accepts in Perry (2003) a margin of appreciation for the competent national authorities, therefore this is seldom an issue and almost certainly not for eCall (Gomien, 2002). To be proportional, a measure should provide adequate safeguards against abuse as stated by the ECJ in Malone (1984) and Rotaru (2000). Deducting from Perry (2003) and Rotaru (2000), this would mean that an eCall service and all information gathered from it could only be used for providing assistance by emergency services in case of an accident but should not be used for example to determine the causes of the same accident. This would also be contrary to the goal of eCall and the supposed legal aim of its implementation, specifically quickening response time of emergency services in case of an accident to reduce the consequences of that accident.

Given a legitimate law imposing mandatory in-vehicle eCall, we would also have a legitimate ground to operate the system, which is a second issue with eCall (art. 7 (c) 95/46/EC). Additionally operating eCall is also possible given that the data protection directive allows for the processing of personal data to protect vital interests of the data subject. Given the purpose of in-vehicle eCall this is also a possible ground for legitimacy. In-vehicle eCall is about saving lives of people involved in traffic accidents or mitigating the consequences of those accidents. It seems reasonable to consider this a vital interest of the data subject, especially given X. v. Belgium. The Working Party considers that in some cases eCall might be triggered although there would be no need for emergency services. The question is then if it is at all possible to avoid such false positives. The conditions for activation are set in advance and if they are fulfilled, the system will be activated. For the time being, adaptive eCall systems that asses whether emergency intervention is needed are not available and quite likely impossible to make at this point in time. Therefore a trade-off between road safety and data protection will be necessary. It is also a fact that in some cases the consequences of the accident only surface at a later stage and are not visible at the time of the accident except after thorough medical examination executed in a hospital. This is especially true for head injuries (Medline Plus). That is one of the reasons why racing drivers are put through thorough physical examination after a crash. Sometimes head injuries only surface at a later stage; hours or even days after the crash and they possibly carry life-ending consequences. This makes it difficult to determine when a vital interest is at play because sometimes it is impossible to determine at first sight or even after a normal medical examination whether a person is injured.

There is a final issue under current European data protection rules regarding disclosure of the location of the caller. The answer is found in the e-Privacy Directive in art. 10 (b) on caller line identification for emergency calls (2002/58/EC). This Directive is relevant because we will make use of public communications-services in a public communications network (art. 3.1. 2002/58/EC). It holds specific rules for disclosing location data. This is data relating to the geographic location of the terminal equipment of the communication. Do these rules allow disclosing the location? This article states that the objection against the transmission of caller line identification and transmission of location data must be lifted on a per-line basis for organizations dealing with emergency calls and recognized as such by Member States for the purpose of responding to such calls. Location data refers to information relating to the geographical location of the terminal equipment, in this case the car with eCall ((art. 2 c) 2002/58/EC). In case of eCall these organizations will most likely take the form of a Public Service Answering Point (MoU, 2004). This art. 10(b) seems to refer to the goal we have previously mentioned for allowing eCall under general data protection legislation. A 'call' is defined by the Directive as follows:

A connection established by means of a publicly available telephone service allowing two-way communication in real time

An emergency call is a call made for emergency purposes. This provision seems to provide an additional answer to certain data protection issues regarding communication data in addition to what has already been elaborated in this section.

3.3. *Include PETs*

The Working Party also considers that privacy enhancing technologies (PETs) should be incorporated in the design of the eCall system. This refers to a principle to be applied in designing privacy-sensitive applications: 'privacy by design' (recital 46 95/46/EC; Koorn et al., 2004). This principle refers to the notion that privacy should be considered from the first step of the design process and that every component should be privacy-compliant in itself and preferably that the interaction between components is also privacy-compliant. To achieve this, technical controls could be implemented to protect personal data (Koorn et al., 2004). They could reduce the need for elaborate organizational and procedural measures for data protection that always rely on people to be implemented. Such measures require extensive enforcement to guarantee adequate implementation; consuming a lot of time and resources. PETs do not rely on human interaction and should as a result be more reliable than procedural and organizational measures.

There is however no mention of the specific PETs that must be implemented. This is in line with the Data Protection Directive which does not refer to specific technologies either. The Directive only requires appropriate measures and that is determined by a balance of interests between the sensitivity of the personal data and the cost of the measures to the controller (art. 17 95/46/EC). This makes the legislation adaptable to new evolutions and technologies in different situations, but could also cause some uncertainty regarding its application. This uncertainty seems needless in most situations providing that the applied PETs are reliable. If that is not the case, one could have reason to worry about compliance and one should not implement the PET.

With regard to in-vehicle eCall, we could think in the direction of PETs that only publish the data needed for the operation of emergency services in case of an accident. This means that the data used to aggregate the vehicle location should not be made public to anybody under any circumstance. In Belgium there are possibly even legal objections to the use of GNSS data in criminal prosecution. These could fall under the rules for observation using a technical means (art. 47 sexies-septies Code of Criminal Procedure). This would require a mandate from the public prosecutor (Procureur du Roi) prior to employing the system. Cumulatively, it is only allowed when there are serious indications of criminal activity possibly resulting in a correctional sentence of minimum one year. In Belgium this is not possible for traffic violations such as speeding; these are only subject to fines and possible loss of license for a specified period. Technical means should only be used as a measure of last resort when other methods of investigation are inadequate. One should therefore not use the GNSS data just because they are easier to use but because they are the only data that can be used (Meese, 2003). As a result, it seems doubtful that it is legally possible in Belgium to use the data from the eCall system to determine if the data subject has committed a traffic violation.

Additionally, only those services that need the full accident data generated by eCall should be given that data. It appears logical that a list of services that have an interest in receiving the accident information the moment it happened should be drawn up and for every service should be determined what data they need and an appropriate PET governing the proliferation of the accident data should be implemented in the system. For example, a service providing traffic information should only be given the location of the accident. Proliferation for statistical purposes should be done anonymously and only general location data should be provided. Any service that is not on this list should not be given any information regarding the accident. In short, accident data should only be transferred on a need-to-know basis.

As a concluding note on PETs, it is important to remember that PETs only work in the information chain they have been implemented in. As soon as the data is taken out of that system, the protection of the PETs is neutralized (Borking and Raab, 2001). This could be done by exporting the data to a different system, copying it to a USB-stick or by having hard-copies of the information. Therefore it is impossible to rely on the PETs alone for compliance with data protection rules. In some cases other additional measures might be necessary to guarantee compliance with data protection rules. This is also clearly mentioned by the wording 'appropriate technical and organizational measures'. The human factor should not be neglected.

3.4. *Safeguard against illegal tracking and abuse of the system*

The Working Party clearly said it rejects the possibility of tracking someone constantly in case of a voluntary system. This should neither be possible for a mandatory system given the more infringing nature. The mandatory aspect should only refer to the fact that the system must be present in the car and ready for use without any request from the buyer or user. It should be a 'sleeping' system, identical to the voluntary eCall, without the possibility of switching eCall off, contrary to the voluntary eCall. A sleeping system could be a first element to address the issue as acknowledged by a UK report (McClure and Graham, 2006). This report notes that it is easier to track people from their mobile phone usage than it would be from eCall because eCall is absent from the network until it is activated by an external factor. This difference should safeguard data subjects to a certain extent already.

A second safeguard could be derived from data protection law. Every processing of personal data needs a specific goal and the data cannot be processed for any other goal incompatible with that goal (art. 6(b) 95/46/EC). eCall collects data for providing assistance in case of an emergency. One could make a case that as a consequence this data cannot be used for criminal prosecution or for establishing responsibility for an accident. This might be supported by rules of Criminal law in some countries, remember the example of Belgium earlier. Maybe use for any goal other than providing assistance in case

of an accident should be excluded by law. For any processing contrary to the goal of eCall, the controller and any other person involved in the illegitimate processing should be subject to the penalties imposed under national data protection law (art. 24 95/46/EC).

Belgian data protection law for example holds specific provisions concerning illegitimate processing of personal data (art. 37-43 WVP). Concurrence with other offences is possible under Belgian Law if their respective conditions for applicability are met (art. 65 Belgian Criminal Code). The Belgian Criminal Code states how penalties should be imposed on perpetrators in case of concurrence of different crimes (art. 58-65 Belgian Criminal Code). This considerably expands the sanctions imposable on an illegitimate processing of personal data in case it could also qualify as an offence under criminal law. This will, however, only apply after the illegitimate processing has taken place and as a result can only rely on a power of deterrence to safeguard against illegitimate tracking and abuse.

3.5. *European legal intervention*

The Working Party also says that there is need for a legal intervention on the European level to provide appropriate data security in case of eCall. This legal intervention is also needed for the proliferation of eCall (COM (2003) 542 final). The best option is probably a Directive comparable in concept to the Directive for the interoperability for electronic road tolling systems (2004/52/EC). That Directive aims at harmonizing the technical infrastructure for electronic road tolling throughout the Member States. Thereto it holds a number of provisions determining when an electronic road tolling system should comply with the rules and what technical options can be chosen. There is also a specific provision on privacy (art. 2.7 2004/52/EC). This gives some idea on a possible structure of the eCall Directive. The advantage of a Directive is also that it determines the margin of appreciation left to the implementation by the Member States.

The content of the Directive can be inspired on the Memorandum of Understanding issued by the eCall Driving Group of the eSafety Forum (MoU, 2004). The importance of this MoU lies in the list of signatures. This list contains a number of EU Member States and also Switzerland, Norway and Iceland but also a considerable number of private companies such as Infineon, Vodafone and Siemens and maybe even more important ACEA. ACEA is the European Automobile Manufacturers Association. Their signature on behalf of their Members indicates that the manufacturers are also supporting the development and implementation of eCall. Some members of ACEA, such as BMW (Connecteddrive), GM (OnStar), Volvo (OnCall) and PSA (Appel d'Urgence), already operate a proprietary system today.

In addition, the MoU also holds in its annex B the content of the MSD that should be transmitted to the PSAP or private service providers operating as PSAP under the regulation of a public body. This MSD should contain time-stamp, precise location, vehicle identification, service provider identifier and eCall qualifier. The vehicle identification could be the VIN-number but could also be the registration plate of the vehicle. The eCall qualifier is to provide an indication on the external factor, manual or automatic, triggering eCall giving some idea of the gravity of the incident. The MoU states this as the minimum qualifier data, therefore additional data could be added to this qualifier.

The Commission pushes for a technical architecture based on E-112 (COM (2003) 542 final). This should facilitate pan-European implementation of eCall and ensure interoperability, as has been done for electronic road tolling. This might collide with the systems as they are currently operated by the car manufacturers. Their eCall systems mostly pass through a call centre providing telematics services and only in second instance information related to an accident is relayed to a PSAP. Furthermore, most of them are SMS-based using regular cell-phone connections instead of E-112. By using the E-112 system PSAPs can be contacted directly. Another advantage of the E-112 system is that as long as there is a mobile operator providing coverage, even if it is not the provider of the user, a connection can be established with the PSAP. The E-112 system is subject to European data protection rules and everybody operating under the E-112 regulation is as a result restricted by these data protection rules (2002/21/EC; 2002/22/EC; 2002/58/EC).

Reference was already made to Community data protection rules regulating emergency calls and considering the definition of eCall by the MoU these seem to be applicable to eCall (art. 10.1 2002/58/EC). A Directive regulating eCall could clarify these existing data protection rules and add further protection where needed as was done by the e-Privacy Directive for electronic communications (art. 1.2 2002/58/EC). It could also improve the proliferation of the technology throughout the cars sold in the Community (COM (2003) 542 final).

The German motorist association ADAC published several recommendations on its website on how an in-vehicle eCall should be implemented. Some of these we have already mentioned, but their position is interesting as it reflects a view on a practical implementation. They have grouped their recommendations in five areas: activation, pan-European standardization, in-vehicle, additional service buttons and data protection. The activation should be automatic, but manual activation must also be possible. When the system is activated manually, there should be a means to abort the communication and end any data transmission.

The European wide standardization entails an architecture based on E-112 but also a common European data format for the minimum data set that is required for in-vehicle eCall. The system should offer the emergencies dispatching centre (PSAP) a voice connection and the dispatchers themselves should be able to communicate in English in addition to the language of their country. The system should be made mandatory on all new cars to guarantee a minimum level of operation. It should also be a solid component built into the vehicle to provide the best possible reliability in case of an accident. There should also be an emergency power-supply for the component in case the main battery fails. Use of the mobile phone of the occupant of the vehicle for communication is thus not acceptable for ADAC. For them that option is not reliable enough in case of an accident. The system should also be able to offer additional services. The owner of the vehicle should have the free choice on the service provider of these services.

The Commission accepts this but only in as far as these services are not detrimental to the primary eCall functionality. Their data protection recommendations mostly concur with what has been set out previously in this article. Data protection rules must be obeyed, the system can only transmit data when activated manually or automatically and there should be no profiling of vehicle movements. Furthermore, the transmitted data can only be used for providing assistance in case of an emergency. Only their final recommendation concerning data protection is a bit odd and seems contrary to their recommendation of mandatory installment on new cars. The driver must be given the possibility to switch off the system at first use. From a user's point of view this seems logical considering data protection issues. However, it appears of little use making a system mandatory to provide for a minimum level of operation and then allowing it to be switched off at first use rendering it in fact inoperative and unable to perform its task. Installing in-vehicle eCall in all new cars is a first step to a comprehensive implementation. But in order to achieve this implementation fully and improve road safety, the system should also be operational and one should not be able to switch it off. eCall can only fulfill its function when switched on.

We can however concur with the second part of this recommendation, namely that the users should be clearly and comprehensively informed of the data generated and transmitted by in-vehicle eCall and what it means in the bigger picture of in-vehicle eCall. From the point of view of data protection it appears logical that the system can be switched off. But from the point of view of road safety this appears detrimental to the goal of eCall and would also impose needless costs on vehicle manufacturers and consumers for equipment that would not be used.

4. Conclusion

The answers given to the issues raised by the art. 29 Working Party and the possible structure of an in-vehicle eCall Directive should demonstrate that there could be a good case for implementing a mandatory system in the Community. Data protection legislation and case law indicate with reasonable clarity the limits data protection imposes. Legislative intervention through a Directive could give in-vehicle eCall a solid base for harmonized implementation and safeguarding against illegitimate tracking and abuse. The 2004/52/EC Directive could serve as an example for the structure of such a Directive. The MoU could serve as a basis for the content and tenure of the Directive. E-112 is proposed by the Commission to serve as a basis for the technical aspects while current data protection rules could provide safeguards for personal data supplemented with specific provisions where needed. The tools for implementation of a mandatory system seem to be available in the Community. Judging by the signatures of the MoU, the industry seems to be supporting mandatory in-vehicle eCall as well. The only thing that seems to be missing is the finishing touch.

Christophe Geuens (*christophe.geuens@law.kuleuven.be*) *Legal Researcher, ICRI – K.U.Leuven – (The Interdisciplinary Centre for Law & ICT) – IBBT (Interdisciplinary Institute for Broadband Technology)*.

Jos Dumortier (*jos.dumortier@law.kuleuven.be*) *Director, ICRI – K.U.Leuven – (The Interdisciplinary Centre for Law & ICT) – IBBT (Interdisciplinary Institute for Broadband Technology)* (*www.law.kuleuven.be/icri*; *www.ibbt.be*).

REFERENCES

Borking JJ, Raab CD. Laws, PETs and other technologies for privacy protection. The Journal of Information, Law and Technology 2001;(1), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking; 2001. retrieved from website JILT:.

Communication from the Commission to the Council and the European Parliament, information and communications technologies for safe and intelligent vehicles, COM (2003) 542 final; 2003.

Criminal Procedure Code, website Moniteur Belge: http://www.juridat.be/cgi_loi/loi_F.pl?cn = 1808111730.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; O.J.; 31/07/2002. L 201.

Directive 2004/52/EC of the European Parliament and of the Council on the interoperability of electronic road toll systems in the Community, O.J.; 30/04/2004. L 166, p. 124–43.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281; 23.11.1995. p. 31–50.

European Parliament resolution on road safety: bringing eCall to citizens (2005/2211(INI)), http://www.europarl.europa.eu/oeil/file.jsp?id = 528362; 2005.

Gomien D. Short guide to the European Convention of Human Rights. Strasbourg: Council of Europe; 2002.

Head injury, Medline Plus: http://www.nlm.nih.gov/medlineplus/ency/article/000028.htm.

Koorn R (editor), Van Gils H, ter Hart J, Overbeek P, Tellegen R. Privacy-enhancing technologies. White paper for decision makers. Ministry of the Interior and Kingdom Relations, http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf?refer = true; 2004.

Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data, Official gazette; 18 March 1993 (WVP).

Malone v. The United Kingdom, ECHR; 1984. application no. 8691/79.

Mcclure D, Graham A. eCall – the case for deployment in the UK. London: UK Department of Transport; 2006. ref: SBD/TEL/1100a.

Meese J. Bijzondere opsporingsmethoden en andere onderzoeksmethoden. Nieuw Juridisch Weekblad Volume 2003;47:1134–53.

Memorandum of Understanding for the realization of interoperable in-vehicle eCall, http://www.esafetysupport.org/en/ecall_toolbox/memorandum_of_understanding_mou/; 28 May 2004. retrieved website eSafety support.

Perry v. The United Kingdom, ECHR; 2003. application no. 44647/98.

Rotaru v. Romania, ECHR; 2000. application no. 28341/95.

Titley G. Report on road safety: bringing eCall closer to the citizens. Committee on Transport and Tourism, http://www.europarl.europa.eu/oeil/file.jsp?id = 5288362; 2005. ref.: 2005/2211(INI), retrieved from European Parliament Legislative Observatory.

WP 125Working document on data protection and privacy implications in eCall initiative, WP 125, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_en.pdf; 2006.

X. v. Belgium, Commission decision 13 December 1979, application nr. 8707/79.