UACES 45th Annual Conference

Bilbao, 7-9 September 2015



www.uaces.org

# eCall and the quest for effective protection of the right to privacy

*T.H.A. Wisman*[1]

On the 29th of April 2015 the Regulation 2015/758 (the regulation) was adopted.[2] The objective of this regulation is to increase road safety through the deployment of the so-called eCall in-vehicle system (eCall). eCall is part of the bigger framework on Intelligent Transport Systems.[3] eCall supports two services: the mandatory public 112-based eCall service and the voluntary third party service (TPS). The function of the 112-based eCall service is to automatically dial emergency-services when a car is in a serious enough accident and to communicate a minimum set of data (MSD), amongst which is the exact location of the car and the unique Vehicle Identification Number (VIN). There are three technologies crucial to the functioning of this system. First, there is GSM 2G which is necessary to establish an audio channel between the people inside the car and the Public Safety Answering Point (PSAP) where the eCall is received. Second, there are receivers compatible with positioning services provided by the Galileo and the European Geostationary Navigation Overlay Service (EGNOS, a regional satellite navigation system).[4] Third, are the sensors that register when the car is in a severe crash. The time that is saved by emergency services through the use of this system will inevitably result in less fatal accidents, a reduction of the severity of injuries and a decrease in the congestion caused by the accident (recital 7).[5] On top of that, there is the advantage that these services are called when there are no witnesses. Especially in rural areas this can make the difference between life and death. In short, this is an invention expected to bring major benefits to road safety. Besides road safety, the TPS eCall service is expected to bring benefits for industry, because it offers a platform for the provision of added value services, e.g. the tracking of stolen cars.[6]

Besides benefits eCall also presents challenges to the right to privacy. Especially the 2G-technology can be used to track the movements of a car. Since eCall is a measure that follows from EU law and it presents challenges to the right to privacy, it provides an interesting case study to the question how relevant EU law should pervade the design of this system and to compare this to its actual design (as follows from the regulation). There are some bumps on the road ahead, since the specifics of eCall's design are captured in standards which are complex technical documents which can only be obtained if you pay a fee. My interpretation of the working of eCall is not based upon my own technical expertise, but on online sources, presentations of the company that delivers the chip for the car

---

[1] Tijmen Wisman is researcher/lecturer at the Centre for Law and Internet (CLI) of Vrije Universiteit Amsterdam.

[2] Regulation 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC.

[3] See Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

[4] Recital 10 and Article 5 (4).

[5] The estimation is the prevention of 2 500 (6.4% of 39 000) traffic deaths per year, mitigate the severity of 5850 (15% of 39 000), see http://europa.eu/rapid/press-release_IP-10-488_en.htm, last seen August 7th 2015.

[6] See http://europa.eu/rapid/press-release_IP-13-534_en.htm?locale=en, last seen June 2015.

(NXP), interpretation of legislative history, expert comments and interviews I conducted with experts.[7]

This paper is structured around four questions. The first question is how the right to privacy and data protection are addressed in the regulation? The second question is why the right to privacy still remains a concern, followed by the third question: why the regulation fails to address these concerns. Fourth, I question if - in the hypothetical case that a member state would exploit these risks - the Charter would provide citizens of member states with protection? Finally, I construct an argument for the effective protection of the right to privacy in the design of eCall.

## Privacy and data protection in the regulation

In the regulation there are several recitals and provisions dedicated to the right to privacy (Article 7 Charter) and the closely related right to data protection (Article 8 Charter, Directive 95/46/EC and Directive 2002/58/EC (data protection directives)), which address a range of differing issues. Some of them pose direct obligations to manufacturers, others empower the Commission to adopt delegated acts on the specified matter.

There are general obligations formulated for manufacturers to implement all necessary measures to comply with Article 7 and 8 Charter (recital 22). There is an obligation that any processing of personal data by the 112-based eCall in-vehicle system (112-system) has to comply with the data protection directives (Article 6(1)), in particular to guarantee that it is not traceable in its normal operational status, nor subjected to any constant tracking (recital 21). Besides an obligation for manufacturers to ensure this non-traceability (Article 6(4)), they need to ensure that the data stored on the internal memory of the 112-system are automatically and continuously removed (Article 6(5))[8] and this data shall not be available outside the 112-system before eCall is triggered (Article 6(6)). On top of all this there is a list of information that manufacturers have to provide in the owner's manual, which will contribute to the transparency of the processing operation and can be viewed as a specification of data protection (Article 6(9)). The Commission shall adopt implementing acts to lay down practical arrangements for assessing if the manufacturers complied with these obligation (paragraph 4 to 6) and a template for user information referred to in paragraph 9 (Article 6(13)).

Further demands are made upon the design of the 112-system to render it impossible to exchange personal data with the system providing private or added-value services (the TPS-system/recital 15, Article 6(11)). Vehicle manufacturers have the duty to integrate technical forms of data protection and have to adhere to the principle of 'privacy by design'[9], when they comply with technical requirements (recital 23). These technical requirements fall under the competence of the Commission, which is empowered to adopt delegated acts to establish them (Recital 27, Article 5(8)). Thus, the Commission is responsible to take privacy into account of the design of eCall. Also 'privacy enhancing technologies' will be embedded in the system, in order to 'provide eCall users with the appropriate level of privacy protection, as well as the necessary safeguards to prevent surveillance and misuse', although it is not clear wat the 'appropriate level of privacy protection' is and whose

[7] Amongst others Simon Hania from TomTom and a person who works for the police who actively engages in surveillance practices.

[8] Except for the last three locations as these are necessary to determine the current location and the direction the vehicle was driving in.

[9] It is not specified what definition of privacy by design is followed.

duty it is to embed this technology (Article 6(7)). All in all, the right to data protection and to a lesser degree the right to privacy are addressed by the legislature, which will contribute to the extent the design of eCall respects these rights.

The fact that the legislature has adopted procedural rules on the processing of personal data as well as some hard demands on the design of eCall can be viewed as an implicit recognition that these matters fall under the essential requirements of the design of eCall.[10] They are not completely left to the Commission to decide on in delegated or implementing acts, nor shall they become entirely subject to a negotiation process within European Standardization Organizations (ESO's). This shows the willingness of the legislature to take privacy and data protection into consideration in the design.

## Why privacy still remains a concern

The legislature has taken an effort to protect the right to privacy in the regulation, yet there still remains reason for concern, despite the Commission's release of the newsflash: 'eCall – Do you have any concerns for your privacy? You shouldn't….'.[11]

The regulation made the installation of this system mandatory (recital 4, 7 and 11). This is the first interference with the right to private life: the mandatory fitting of private property with a 'state'-designed ICT-system is not a matter to take lightly. Of course the mandatory installation could be justified on the account of the deaths per year that it is supposed to prevent. The question remains if the advantages eCall is expected to bring, justify the mandatory installation of this potentially intrusive system into practically every car in the EU (Article 4). Especially because most of these deaths seem to occur in rural areas and voluntary adoption seems to be a viable option as well. It is all the more troublesome that industry is served through the mandatory deployment of this system, that serves as platform to provide commercial services. There are signs it actively lobbied for the mandatory deployment.[12]

One minor, yet important, detail is left unsettled in the regulation. The technology that poses a threat to the right to privacy in eCall is the mobile phone technology (2G).[13] Fitting every car with eCall is tantamount to placing a mobile phone in every car. What is important for the continuous traceability of the car is thus whether this mobile phone is on or off. The first thing eCall does when a car is started is establishing a radio connection with a public mobile wireless communications network.[14] The benefit of immediately connecting with the network is that it, in case of a crash, saves approximately ten seconds. The downside is that the car inherent to the way in which mobile phone

[10] In a nutshell: in EU legislative acts the essential requirements are laid down and the non-essential requirements are usually left to the Commission through delegated and implementing acts. This mechanism dates back to 'the New Approach' from 1985, which aim was to reduce the amount of detail in legislative acts to reduce the amounts of effort and time that went into intergovernmental negotiations over the contents of these acts.

[11] Zie https://ec.europa.eu/digital-agenda/en/news/ecall-%E2%80%93-do-you-have-any-concerns-your-privacy-you-shouldnt, laatst gezien op 3 maart 2015.

[12] See http://www.imobilitysupport.eu/library/ecall/ecall-implementation-platform/eeip-meetings/2010-3/19-oct-2010/1197-eeip-nxps-solution-to-ecall-19-oct-2010/file , slide 12 of this NXP presentation shows the little concealing sentence 'Need for European legislation on eCall ~ mandatory!'.

[13] The satellite technology consists of receivers and thus does not send out a signal that can be tapped into.

[14] Then Commissioner Kroes was asked about the functioning of the system and told Parliament that when the car starts the system will register in the networks. See http://bit.ly/1Na51gc, last seen June 2015.

technology operates, continuously will be tracked by telco providers and consequently potentially by public authorities as well.[15] As such, eCall does constitute an interference with the right to private life.[16] My own view is that the ten seconds saved in case of a crash by the continuous connection, does not outweigh the disadvantage of continuous traceability of the car. The least the legislature should have done to counterbalance the privacy risk is offer the owner of the car the choice either to drive connected or disconnected. By omitting this, the choice to drive disconnected has silently been taken away. This aspect of the design allows public authorities for instance to send a stealth sms through which they can monitor the location and the movement of the car.[17] When Simon Hania, privacy officer of TomTom, informally asked the people of the Commission involved in eCall whether these implications were fully taken into account, the answer was 'no'.

Another rather unsettling privacy risk created by eCall is the fact that a microphone will be installed in every car produced for the EU from 2018 onwards. Just like the microphone on a mobile phone it can be turned on from a distance.[18] It is likely that the standardized operation of this technology will make it easy and cheap for public authorities or malevolent parties to hack the on-board microphone and turn it into a tap. Parties that engage in industrial and political espionage or in tackling tactical operations of dissident groups, will have an interest in exploiting these vulnerabilities.[19] In the US there is at least one such case in which the FBI requested a manufacturer of onboard services (including microphones) to activate these microphones in order to tap into the conversations taking place in the car.[20] In the Netherlands a bill is proposed that allows public authorities to hack automated works, a category which covers eCall, and turn on a microphone.[21]

## What the regulation misses

[15] Even if the telco provider cannot directly link the number of the sim-card connecting to the telephone mast, public authorities will be able to gain access to the numbers linked to the car owners.

[16] Although the ECtHR has argued in the past that location data is less intimate than telecommunications data and therefore does not merit the same protection (see *Uzun v. Germany*, application no. 35623/05, 2 September 2010, § 52), this view has been criticized. For criticism see Paul de Hert, A Human Rights Perspective on Privacy and Data Protection Impact Assessments, p. 60. The continuous mapping of a person's travelling movements, especially when cross-referenced with maps containing information of physical addresses, enables the drawing of a detailed picture of a person's life. It is not the nature of this data that ultimately determines its intimacy, but the information that can be derived from it. From this perspective location data can be more intimate than telecommunication data.

[17] The precision of this depends on several factors, amongst which the number of telephone masts in the area. The accuracy of this method may differ from 50 up to 100 meter. However, there have been people who researched their own location data and came up with a strikingly accurate picture of their travelling movements. See http://www.zeit.de/datenschutz/malte-spitz-data-retention.

[18] It is even possible to turn it on when a mobile phone is off.

[19] A most revealing story of a private surveillance company that was in the news recently was about 'Hacking Team'. Among its primary targets were Privacy International and Human Rights Watch. See http://www.theguardian.com/technology/2015/jul/11/hacking-team-hack-state-surveillance-human-rights, last seen August 2nd 2015.

[20] Jonathan L. Zittrain, *The Future of the Internet and how to stop it*, Yale University Press 2008, p. 109.

[21] Wetsvoorstel Computercriminaliteit III. See http://www.circleid.com/posts/20130508_government_hacking_proposed_law_in_the_netherlands/, last seen August 28th 2015.

There are some weaknesses in the way the right to privacy is addressed in the regulation. There is especially a lot to be found on the right to data protection in the regulation. The right to privacy is actually only addressed once in a general matter in the form of an instruction to the manufacturers to comply with Article 7 Charter by implementing the necessary measures (recital 22). Also manufacturers are instructed to adhere to the principle of 'privacy by design' when they comply with technical requirements (recital 23). Yet, the regulation does not elaborate on what these instructions entail, or how the manufacturers should comply with these highly abstract demands. More so, the Commission and ESO's have the final hand in the detailed technical requirements laid down in the standards to which the manufacturers have to adhere. What exactly is in these standards that poses a risk to the right to privacy is unknown, but it is highly likely that these standards prescribe the on-status of eCall. Unless the manufacturer is willing to deviate from the standards, which brings a pile of costs with it which renders it highly unlikely, the room for the manufacturer to protect privacy through the design is limited. Therefore it seems these instructions lack practical value. From a more general point of view, the mere possibility that these standards hold the power to impact the right to privacy is irreconcilable with the rule of law, since these standards are not considered law in the first place.

Another weakness of the focus on the right to data protection is that it does not prevent the collection of data taking place, but focusses instead on the manner in which the data are collected and subsequently used.[22] Viewing eCall as merely an interference with the right to data protection, results in omitting the assessment of the necessity of the initial collection of personal data, an assessment that should naturally follow from the protection offered by the right to privacy. It deserves stipulation that AG Villalón has held that the compatibility of legislation with the right to data protection in no way means it is also compatible with the right to privacy.[23] The focus of the regulation on the right to data protection is irreconcilable with the Commission's own attitude towards fundamental rights protection in its own policies. More specifically, the Commission is supposed to assess the potential impact of its legislative initiatives on all the rights guaranteed by the Charter and to check their legality and compatibility with it.[24] The Commission accorded to the Charter the function of an instrument 'to keep abreast of changes in society and scientific and technological developments.'[25] The impact assessment is supposed to help prepare for the fundamental rights proofing legislative proposals.[26] Yet, upon reading the eCall impact assessment it does not assess the impact on the right to privacy. There is only a section title dedicated to the protection of personal data and here the privacy risk is dismissed by stating that the system is dormant, unless an accident happens or when an occupant presses the manual button.[27] eCall

[22] C-293/12 and C-594/12, *Digital Rights Ireland* (Opinion), 12 December 2013, § 59.

[23] Idem, § 60.

[24] CFTC, Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM (2010) 573, p. 7.

[25] CFTC, Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM (2010) 573, p. 3.

[26] Report on the practical operation of the methodology for a systematic and rigorous monitoring of compliance with the Charter of fundamental rights, COM(2009) 205 final, Brussels, 29.4.2009, p. 6.

[27] Commission Staff Working Paper Impact Assessment, Commission Recommendation on support for EU-wide eCall service in electronic communication networks for the transmission of in-vehicle emergency calls based on 112 ('eCalls'), SEC(2011) 1019 final, Brussels 8.9.2011, p. 12.

understood as an alarm call is only activated then, yet the system despite its 'dormant' state connects with telephone masts. In this respect labelling the system 'dormant', which hints towards a state of passivity, is somewhat misleading. The system evidently allows telco providers to collect location data and the necessity of this collection is not questioned in the impact assessment. Please note that this collection is not even recognized in the impact assessment, nor in the regulation itself. It seems to be the blind spot on the retina of the Commission.

Furthermore, most of the provisions in the regulation are addressed to the 112-based eCall in-vehicle system, but not to the TPS eCall, e.g. Article 6(1,4,5,7). According to a presentation of NXP the software of the system offers road pricing and stolen vehicle tracking, which proves that outside of the normal operational status constant tracking is possible.[28] It is unclear why the provisions on data protection are not addressed to TPS, since these services naturally fall under the data protection directives.

Another factor that is not contributing to the transparency of the processing operation set in motion by eCall is that this is defined in a standard. These standards do not excel in clarity, nor are they publicly available, as they can only be purchased at an ESO. On the other hand they do entail requirements for eCall's design, which have to be met in order to comply with the standard and gain access to the internal market. In short, they produce legal effects, yet do not meet the requirement of accessibility. When the MSD is mentioned in the regulation it consistently refers to the standard EN 15722:2011 'Intelligent transport systems – eSafety – eCall minimum set of data (MSD)' (Article 5(8)(d)). Evidently this does not meet the demand of accessibility. Although the regulation does provide the duty for manufacturers to deliver information on the types of data collected and processed by the system and the recipients of this data (Article 6(9)(e)), it is irreconcilable with EU data protection laws to leave out such key information in a legislative act which is mainly concerned with the processing of personal data.

## The failure of fundamental rights protection by the EU in the face of surveillance risks created by eCall

Does the Charter protect individuals against a member state that would surveil its citizens through eCall? Recent case law indicates a negative answer to this question. In *Willems* the ECJ had to decide about a similar matter. The Raad van State, the highest administrative court in the Netherlands, posed preliminary questions regarding Regulation no 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. One of these questions was whether this regulation read in conjunction with Articles 6 and 7 of Directive 95/46 and Article 7 and 8 of the Charter:

'must be interpreted as meaning that it requires Member States to guarantee that the biometric data collected and stored pursuant to that regulation will not be collected, processed and used for purposes other than the issue of passports or other travel documents.'[29]

In other words, the question was whether EU legislation prevented the repurposing of data collected on the legal basis of EU law. These new purposes consisted of the identification of victims of disasters

[28] See http://www.imobilitysupport.eu/library/ecall/ecall-implementation-platform/eeip-meetings/2010-3/19-oct-2010/1197-eeip-nxps-solution-to-ecall-19-oct-2010/file, last seen 6th of July 2015.

[29] Joined Cases C-446/12 to C-449/12, *Willems*, 16 April 2015, § 43.

and accidents, the detection and prosecution of criminal offences and for the conduct of investigations of acts constituting a threat to state security. The ECJ considered that EU legislation was not applicable, because these purposes were all matters of national interest. The fact that the data was collected on the basis of an EU regulation, the fact that there is legislation in the EU as well as from the CoE (Convention 108) that regulates the use of data and the fact that this interpretation goes against the purpose specification principle, rendering compliance with the right to data protection largely meaningless, were all left out of the written considerations of the ECJ.

Apply this (albeit arguably flawed)[30] logic to the repurposing of eCall for national interests such as fighting crime, terrorism or even tax fraud, and it becomes clear that the fundamental rights protection of the EU leaves the citizens of member states empty handed against these *purpose creeps*.[31] The regulation can lay down obligations to process personal data only for the handling of emergency situations, once the national legislator draws up a law that establishes purposes in the national interest, these obligations become obsolete.

The protection of fundamental rights against privacy risks created through EU legislation exploited by the national legislator, can (in the light of recent case law) only be countered by national laws or the ECHR.

## An argument for effective protection of the right to privacy in the design

Traditionally the respect for the private sphere is safeguarded by law and structurally protected by the impossibility to penetrate this sphere without taking special measures.[32] The installation of eCall dissolves a significant part of this structural protection. Human and fundamental rights are just one factor that curtails surveillance practices. Another one is plain economics.[33] Costs are an important limit exerted upon public authorities their use of surveillance competences. Already in 2010 a working paper written by Ian Brown made the point that in the near future it will cost more to exclude people from total surveillance than to include them.[34] The introduction of eCall in its current form significantly contributes to lowering the threshold for the state to engage in surveillance practices regarding traveler movements by car and eavesdropping on conversations in the car.[35] Effective protection of the right to privacy starts with the design of eCall.

---

[30] See Steve Peers, http://eulawanalysis.blogspot.se/2015/04/biometric-data-and-data-protection-law.html, last seen August 7th, 2015.

[31] T.H.A. Wisman, Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things, *European Journal of Law and Technology* 2013, Vol 4, nr. 2. See http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2486441.

[32] H. Surden, *Structural Rights in Privacy*, SMU Law Review 2007/60, p. 1605.

[33] http://tegenlicht.vpro.nl/afleveringen/2013-2014/bureau-voor-digitale-sabotage.html. Interview with Eleanor Saitta from 12:50.

[34] Ian Brown, *The challenges to European data protection laws and principles*, European Commission Directorate-General Justice, Freedom and Security, 20 January 2010.

[35] Compare the calculations made by two American scholars on the reduction of costs by the introduction of GPS, http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones. It should be noted that they treat the case where a tracking device is installed by the designated public authority. In eCall the installation of a tracking device is the standard.

The effective protection of fundamental rights clearly resonates with the principle of effectiveness of the ECtHR.[36] The aim of this principle is to make human rights protection practical and effective, rather than illusory and theoretical. The ECHR has connected this principle in the past with the doctrine of positive obligations and found that Article 8 ECHR might require from states the adoption of measures designed to secure respect for private life. Another relevant consideration of the Strasbourg Court is that 'an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference'.[37] The ECtHR has held relevant the parallel developments in the field of information technology that unlocked a new spectrum of actions. The ECJ, also, has taken potential violations of fundamental rights into account while assessing the legality of an injunction of a filtering system that would enable the monitoring of online communications.[38] The principle of effectiveness together with an assessment of foreseeable future use of technical possibilities provided by eCall occasions a critical reevaluation of the necessity of these possibilities.

The fashion in which to execute the necessity test should be instructed by the two most important features of eCall: its mandatory character and the fact that it consists of technology that allows for interferences with the right to privacy. With the adoption of the regulation the choice whether to drive a car equipped or unequipped with EU designed technology is out of the realm of the citizen. The obligatory character of this intrusive technology, the nature of the interferences it enables, the interests to be protected from this interference and finally the absence of a pressing social need as well as a legal ground to design the system in a way it allows more functions to be performed than the informing of emergency services, merits a critical reevaluation of the necessity and proportionality of its functions. In contrast with the approach that follows from the regulation, an approach should have been chosen in which eCall strictly adheres to the necessity test, resulting in a design that only allows its operation in so far as is strictly necessary to attain the goal of the system i.e. road safety.

The legislature could have easily prevented these surveillance-capabilities from arising in the first place. First, the system could have been designed in a way that it would only make a connection with the 2G-network if an accident had occurred. Instead, the choice was made to be connected when the motor runs. Moreover, the legislature remains silent about this important feature and thus leaves it to the executive to take decisions about this precarious matter. Second, there is no necessity for the microphone. It might contribute to the persons in the car communicating to the emergency services and to report their status, but the added value of reporting their status is highest when they are actually incapable of communicating. Even if the microphone would be deemed necessary, the design could have provided for a solution where the microphone was cut of power through a physical feature of the design, which would only be terminated in the case of a crash or when triggered manually. The only vital information for emergency services is where the accident took place and the number of people involved.[39] Even the unique number of the car (VIN) is not necessary to include in

[36] The object and purpose of the Convention is to protect human rights and thus requires an interpretation of its provisions that 'render its guarantees practical and effective'.*Sabanchiyeva and Others v. Russia*, application no. 38450/05, 6 June 2013, § 132.

[37] *S. and Marper v. The United Kingdom*, application nos. 30562 and 30566/04, 4 December 2008, § 71.

[38] C-70/10, *Scarlet Extended,* 24 November 2011, § 52.

[39] Apparently the system communicates the number of buckled seatbelts.

the MSD. In the event of a crash there is no necessity for any party to know the person to who this number belongs. The VIN can serve as a client number. The unique addressability of the car is necessary to provide services to its owner and makes it possible to track individual vehicles. In other words, industry has a big interest in this feature which has an adverse effect on the right to privacy. Conclusively, all considerations above make it hard to maintain that the current design of eCall complies with the necessity test.

For the right to privacy not to be diminished to a merely theoretical and illusory right, it should protect against *actual interferences* as well as the *risk to interferences* with ones private life. The regulation fails to deliver here, because it only offers protection against the interferences it foresees, yet it neglects the interference and associated risks constituted by the connection eCall makes with telephone masts and the risk posed by the installation of the microphone. It would have been in line with the Commission's ambitious agenda, to make the rights contained in the Charter 'as effective as possible', to take these risks into account while setting demands for the design of the system.[40] The only way to eliminate the risk to interferences created by eCall is to exclude from the design the features that allow for surveillance practices. The Commission, which is the designated party to promote and safeguard fundamental rights in its relation with ESO's, is in the perfect position to take the responsibility for a design that effectively protects the right to privacy. It is up to the Commission to make sure that the ESO's do not have the space to take decisions regarding the design which produce surveillance risks. Decisions which affect fundamental rights have no place with ESO's which are private bodies.[41]

## Concluding thoughts

eCall is a typical example of the possibilities offered by the steady increase in availability of ICT and the ever decreasing costs, which contributes to important goals of public policy and collective interests. Although great in its advantages, eCall is similarly great in the interference and risks to interferences it introduces with the private life of motorists in the EU. With the ever continuing sophistication of technology its potential for surveillance will only increase. Future plans for the EU are already discussed and include Collaborative Intelligent Transport Systems, which are popularly referred to as 'eCall on steroids'. Despite the fact that the regulation does address the right to privacy, the potential for surveillance is left uncurbed. The result is that private property is equipped with 'public' technology which exposes citizens to the risk of (arbitrary) government interference. What the regulation and its impact assessment show is that these risks and actual interference constituted by the continuous connection sought by the system are not even taken into consideration by the legislature, let alone properly assessed if they are proportional and necessary to realize road safety.

The design of eCall seems to be inspired by commercial motivations, which should have no place in legislation that makes these systems mandatory. The legislature has served corporate interests through the adoption of the regulation in its current form. The regulation thus leaves the impression of the improper merger of state and corporate interests. The power of the legislature has been used as a crowbar to open up a traditionally secluded private sphere to install a device able to mediate

[40] CFTC, Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM (2010) 573, p. 3.

[41] C-355/10, *Parliament v. Council* (Opinion), 17 April 2012, §28, 61.

between consumer and companies, but also for the state to control its citizens. This is tantamount to the coercive equipping of virtually all motorists in the EU with a tracking and tapping device. The Commission as policy entrepreneur and most important actor to mediate all different interests, had a special responsibility towards the deployment and design of eCall. The words of the Commission dedicated to the fundamental rights culture it seeks to promote and underscores as the 'essential underpinning of the detailed examination of the necessity for and proportionality of the proposals that the Commission puts forward', sound hollow in the face of its actual practice.[42]

[42] CFTC, Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM (2010) 573, p. 5.