90 eCall: een zoektocht bescherming van he

Mr. T.H.A. Wisman *

I. Inleiding

Op 24 april 2015 werd Verordening 2015/758[1] van kracht, waarin typegoedkeuringseisen worden geïntroduceerd voor de installatie van het zogeheten eCall-systeem. eCall wordt vanaf 2018 verplicht geïnstalleerd in alle auto's die gecertificeerd zijn voor de Europese markt. Bij een ongeluk zullen sensoren in het voertuig het systeem activeren[2] dat direct een minimumreeks van gegevens[3] naar een alarmcentrale (PSAP – public safety answering point) zal doorzenden, waardoor noodhulp-diensten in actie kunnen komen. eCall ondersteunt naast de 112-dienst ook diensten van derden (TPS-eCall).[4]

eCall is uitgerust met diverse technologieën. De locatie van de auto wordt vastgesteld door ontvangers voor satellietnavigatiesystemen. Deze wordt tezamen met de andere informatie verstuurd door middel van een GSM-modem. Hierna wordt via dit modem een spraakverbinding geopend met de noodhulpcentrale, waardoor communicatie tussen de telefonist en de inzittende(n) mogelijk wordt gemaakt. Het doel van eCall is het aantal verkeersdoden en ernstige verwondingen veroorzaakt door verkeersongelukken te verminderen en het middel hiertoe is het automatisch in gang zetten van de inzet van noodhulpdiensten.[5] Daarbij is de verwachting dat een beter beheer van ongevallen ook zal leiden tot minder files en secundaire ongevallen.[6]

Kortom, door de installatie van eCall worden maatschappelijke voordelen verwacht die een installatie zouden kunnen rechtvaardigen. Naast deze voordelen kleven er ook nadelen aan eCall, die samenhangen met de technologieën waarmee het is uitgerust. Deze maken vergaande inmengingen met het recht op respect voor het privéleven mogelijk, zoals vastgelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 7 van het Handvest van de Grondrechten van de Europese Unie (het Handvest). Het Handvest richt zich primair tot de (wetgevende) instellingen van de Europese Unie. Wetgeving van de Unie zou in overeenstemming moeten zijn met het Handvest, dat op zijn beurt een gelijkwaardige of hogere bescherming beoogt te bieden dan het EVRM.[7] De Europese Commissie (hierna Commissie) heeft de ambitie geuit om de grondrechten uit het Handvest *zo effectief mogelijk te maken*.[8] Zij beoogt dit onder andere te realiseren door systematisch de verenigbaarheid met het Handvest in de voorbereiding van wetgeving, het wetgevingsproces en de uiteindelijke wet zelf (het wetgevingstraject) te controleren. Toen Simon Hania, privacy en security officer

* Werkzaam als promovendus/docent aan de VU Amsterdam, afdeling Transnational Legal Studies, sectie Internet, ICT & Recht. Dit artikel is een bewerking van het Engelstalige artikel 'eCall and the Quest for Effective Protection of the Right to Privacy', European Data Protection Law Review, nr. 1 2016, p. 59-69.

1. Verordening (EU) 20156/758 van het Europees Parlement en de Raad van 29 april 2015 inzake typegoedkeuringseisen voor de uitrol van het op de 112-dienst gebaseerde eCall-boordsysteem en houdende wijziging van Richtlijn 2007/46/EG.
2. Het is echter ook mogelijk het systeem manueel te activeren.
3. MSD – minimum set of data, bestaande uit onder andere locatie, voertuig-identificatie-nummer (hierna VIN), aantal inzittenden en de richting van het voertuig Zie http://ec.europa.eu/transport/wcm/road_safety/erso/knowledge/Content/04_esave/ecall.htm, laatst gezien 24 februari 2015. Wat hierna wordt gezegd, wordt al in de hoofdtekst, in par. V, besproken. Opmerkelijk is dat de MSD niet wordt gedefinieerd in de kaderrichtlijn of één van de verordeningen. Als ik wil weten wat precies de MSD is, dan moet ik € 61,30 betalen voor een standaard, hetgeen de transparantie rond de gegevensverwerking niet ten goede komt (zie http://www.nen.nl/NEN-Shop/Norm/NENEN-157222011-en.htm, laatst gezien 24 oktober 2015). Dit komt praktisch neer op betaling vragen aan burgers om wetgeving in te zien, nu deze standaarden de eigenschappen bevatten waaraan producenten moeten voldoen willen ze hun producten vrij kunnen aanbieden op de interne markt van de EU. Eigenschappen die op hun beurt bepalend kunnen zijn voor de impact die het systeem heeft op de persoonlijke levenssfeer. In een presentatie die ik vond op het internet staat een overzicht van de categorieën: http://www.eena.org/ressource/static/files/ecall_standards_update_v2.pdf
4. Dit staat voor Third Party Service eCall. Dit maakt het mogelijk om private diensten te leveren door het eCall-systeem. De verordening praat zelfs over twee systemen, 112-eCall en TPS-eCall. De laatste schijnt van de hardware van de eerste gebruik te maken.
5. De verwachting is dat 2.500 (6.4% van 39.000) verkeersdoden per jaar zullen worden voorkomen en de consequenties van zware ongelukken zullen worden verlicht in 5.850 gevallen (15% van 39.000), zie http://europa.eu/rapid/press-release_IP-10-488_en.htm, laatst gezien 7 augustus 2015.
6. Overweging 6 en 7 van Verordening 305/2013 Gedelegeerde Verordening (EU) Nr. 305/2013 van de Commissie van 26 november 2012 tot aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad, wat de geharmoniseerde voorziening in de gehele Unie van een interoperabele eCall betreft.
7. Respectievelijk artikel 51 lid 1 en 52 lid 3 van het Handvest.
8. European Commission, Strategy for the effective implementation of the Charter, *COM (2010) 573*, p. 3.

naar effectieve t recht op privacy

bij Tom Tom, aan stafleden van de Commissie vroeg of ze er bij stil hadden gestaan dat eCall de politie in staat zou stellen om met stealth-sms auto's te lokaliseren, kreeg hij een antwoord dat met die ambitie in schril contrast staat: 'Nee'.

eCall introduceert een aantal voorzienbare kwetsbaarheden die door derden, voor het doel van surveillance, kunnen worden geëxploiteerd. Het doel van dit artikel is om door middel van deze kwetsbaarheden vast te stellen waarom eCall in zijn huidige vorm geen effectieve bescherming van het recht op privacy garandeert. Hiervoor zal eerst worden geïnventariseerd wat de voorzienbare kwetsbaarheden zijn die eCall introduceert. Vervolgens wordt onderzocht of en hoe deze kwetsbaarheden worden geadresseerd in de Verordening. In paragraaf 4 wordt gekeken of in de eCall impact assessment[9] deze kwetsbaarheden zijn ontdekt. Hierna wordt vastgesteld welke partij(en) verantwoordelijk zijn voor de uiteindelijke ontwerpkeuzes van eCall, die een cruciale rol spelen bij de kwetsbaarheden die het systeem introduceert. In paragraaf 6 wordt beargumenteerd hoe effectieve bescherming van het recht op privacy bij de verplichte invoering van dit soort ICT-systemen kan worden bereikt en worden er, ter illustratie, enkele suggesties gedaan voor de wijze waarop dit recht kan doorwerken in het ontwerp.

II. De voorzienbare kwetsbaarheden van eCall

Er zijn vier voorzienbare kwetsbaarheden die worden geïntroduceerd door eCall. Deze hangen samen met het ontwerp van eCall.[10]
In de eerste plaats kan eCall mogelijk toestaan dat auto's worden gevolgd via GSM-masten. Zodra eCall zich standaard zou aanmelden bij een netwerk, kunnen, door middel van driepunts-lokalisatie, de reistijden en corresponderende bewegingen van een auto tot op de minuut en honderd meter nauwkeurig worden bijgehouden. Indien het starten van een auto uitgerust met het eCall-systeem zou leiden tot een dusdanige verbinding, zonder dat de eigenaar hierin een keuze heeft, resulteert dit in het, zonder toestemming, monitoren en registreren van reisbewegingen.[11]

De vraag is echter of het eCall-systeem een dergelijke privacy-inbreuk teweegbrengt. De wetsgeschiedenis vertelt een tegenstrijdig verhaal. In de 'impact assessment' van de Commissie staat dat het systeem zich normaliter aanmeldt bij een willekeurig netwerk dat aanwezig is.[12] Europarlementariër Judith Sargentini vroeg toenmalig Commissaris Kroes of auto's voortdurend in verbinding zouden staan met zendmasten.[13] Kroes bevestigde hierop hetgeen is omschreven in de impact assessment: eCall bedient zich van openbare mobiele communicatienetwerken en zodra de auto wordt gestart, meldt het boordsysteem zich automatisch aan bij het netwerk met de beste dekking.[14] Sargentini stelde hierop vervolgvragen onder meer over de partijen die betrokken zijn bij de aanmelding, eventuele aanmeldingen bij andere netwerken en of hierbij uniek identificeerbare informatie wordt overgedragen aan het telecommunicatienetwerk.[15] Hierop maakte Kroes een U-bocht en antwoordde dat het systeem in de normale bedrijfsstatus bij geen enkel telecommunicatienetwerk was aangemeld, maar enkel het 'radiospectrum scant' op beschikbare netwerken.[16] Deze mededeling hield een radicale ommezwaai in: van een systeem dat standaard een inbreuk maakt op het recht op privacy en gegevensverwerking naar een systeem dat beide rechten respecteert. Dat is geenszins een triviale kwestie vanuit het oogpunt

> *eCall introduceert een aantal voorzienbare kwetsbaarheden.*

9. Een instrument dat de Commissie gebruikt om, tijdens de ontwikkeling van een wetgevingsvoorstel, vast te stellen welke onbedoelde negatieve gevolgen dit kan hebben, o.a. voor fundamentele rechten.
10. Een ander aspect is de organisatie rond gegevensverwerking. Dit aspect ziet meer op het recht op gegevensbescherming, hetgeen in dezen secundair is (dat wil zeggen pas aan de orde komt als een initiële inmenging met het recht op privacy heeft plaatsgevonden) en daarom buiten het bestek van dit artikel valt.
11. Iets dat door het EHRM in Uzun v. Germany is bestempeld als een inmenging met art. 8 EVRM, dat gelijkgeschakeld is met art. 7 HvGEU.
12. Impact assessment, p. 25.
13. Zie http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2013-008690+0+DOC+XML+V0//NL, laatst gezien 17 februari 2016.
14. Zie http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-008690&language=NL, laatst gezien 17 februari 2016.
15. Vraag met verzoek om schriftelijk antwoord E-009770/13 aan de Commissie, Judith Sargentini (Verts/ALE), 30 augustus 2013. Zie http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2013-009770&language=NL, laatst gezien 17 februari 2016.
16. Zie http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-009770&language=NL, laatst gezien 17 februari 2016.

van een Commissie die een cultuur van respect voor grondrechten nastreeft. De nieuwe koers van Kroes werd op de Commissie-website herhaald in de vorm van een informeel bericht met de geruststellende titel 'eCall – Do you have any concerns for your privacy? You shouldn't….'.[17] Een ontwerpkwestie die het verschil maakt tussen wél of niet inbreuk maken op de rechten vastgelegd in het Handvest is van zo'n groot belang dat deze in de wetgeving die het systeem introduceert expliciet dient te worden vastgelegd. Vooruitlopend op de volgende paragraaf: de Verordening blijft verrassend stil over dit aspect van het ontwerp. Gelet op de constitutionele ambities van de Commissie is dit onbegrijpelijk. Er zijn twee opties die beide evengoed het doel van verkeersveiligheid bereiken, maar de eerste heeft onmiskenbaar nadelige gevolgen voor de fundamentele rechten en de tweede niet. De eerste optie kan daarom nooit de subsidiariteitstoets doorstaan. Nu deze kwestie niet in de Verordening wordt geregeld, rijst de vraag wie over deze ontwerpkwestie de uiteindelijke beslissing neemt.[18]

«eCall geeft mogelijk toegang tot motormanagement-gegevens.»

De tweede kwetsbaarheid bestaat erin dat met behulp van de satellietontvangers het mogelijk is om, door middel van de GSM-modem, locatie-gegevens te verzenden. Hierdoor zouden snelheidsboetes kunnen worden uitgedeeld, of de informatie kan worden gebruikt door een verzekeraar om bijvoorbeeld de verzekerde van dekking uit te sluiten door een geconstateerde overtreding.[19] TPS-eCall maakt gebruikt van de GSM en satellietontvangers om commerciële diensten aan te bieden, zoals het vinden van een gestolen auto.[20]

De derde kwetsbaarheid bestaat in de toegang die eCall mogelijk geeft tot het motormanagementsysteem. In een artikel in het Technisch Weekblad in 2013 waarschuwen Bart Jacobs (hoogleraar computerbeveiliging aan de Radboud Universiteit) en Peter Rietveld (security-expert) voor de mogelijke verschuiving van functies (ook wel bekend als *function creep*) die dit systeem mogelijk maakt.[21] Rietveld waarschuwt dat de chip in eCall toegang geeft tot het motormanagementsysteem en dat dit ook mogelijkheden tot misbruik door kwaadwillenden geeft. Deze kwetsbaarheid hangt samen met het feit dat eCall inkomende signalen kan ontvangen. Ook de ANWB heeft haar vrees uitgesproken dat auto's van een afstand kunnen worden uitgeschakeld.[22] Geheel onterecht is deze vrees niet, aangezien de interesse in kwetsbaarheden van dergelijke systemen binnen de Unie op intergouvernementeel niveau duidelijk waarneembaar is. Aan het einde van 2013, nog voordat het eerste voorstel van de Verordening bij de Raad kwam te liggen, werd onder leiding van Nederland, het Verenigd Koninkrijk en Roemenië het programma van de European Network of Law Enforcement Technology Services (ENLETS) bekend gemaakt.[23] [24] Eén onderdeel van dit programma is het 'best practices programme' dat bestaat uit vijf onderwerpen. Eén van deze onderwerpen luidt: 'Front Line Policing, Vehicle Stopping'. Onder de kop 'Remote Stopping Vehicles' wordt uitgelegd dat dit onderdeel werkt aan een technologisch ingebouwde oplossing voor alle auto's voor de Europese markt, die de politie toestaat om auto's op afstand uit te schakelen. Er wordt aangegeven dat 'cars on the run' een bewezen gevaar voor burgers opleveren. Het met deze technologie preventief uitrusten van alle auto's in de EU zou de politie toestaan proportioneel te reageren. Doordat eCall inkomende signalen kan ontvangen, lijkt deze 'oplossing' nu in zicht.[25]

Ten slotte wordt iedere auto met een microfoon uitgerust om communicatie tussen inzittenden en een alarmcentrale mogelijk te maken. Deze microfoon kan op afstand worden gehackt en worden ingezet als afluisterapparaat.[26] Dit hacken kan gebeuren in de context van kwajongensstreken, bedrijfsspionage of door de politie die deze bevoegdheid krijgt toebedeeld in het Wetsvoorstel Computercriminaliteit III.[27] In de VS heeft de FBI reeds een verzoek gedaan aan een fabrikant van autoapparatuur om de microfoons op afstand te herprogrammeren tot afluisterapparaat.[28] Deze kwetsbaarheid is mogelijk ook aantrekkelijk voor criminelen die graag willen weten waarover in een bepaald voertuig wordt gesproken.

Deze vier kwetsbaarheden tonen aan dat eCall het recht op effectieve bescherming van het recht op privacy ernstig ondermijnt en eventueel een inbreuk maakt door zich standaard te registreren bij mobiele netwerken. Deze kwetsbaarheden maken eCall uitermate geschikt om te gebruiken als surveillance-instrument om de reisbewegingen van de auto te volgen, gesprekken in de auto af te luisteren en de auto van een afstand uit te schakelen. De vraag luidt nu of én hoe deze kwetsbaarheden worden geadresseerd in de Verordening.

17. 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.
18. Hier wordt verder op doorgegaan onder de paragraaf 'Essentiële onderdelen'.
19. C. Geuens and Jos Dumortier, Mandatory implementation for in-vehicle eCall: Privacy compatible, *Computer Law & Security Review 26 (2010) 385-390*, p. 386. Bart Jacobs heeft hier ook voor gewaarschuwd, zie https://www.technischweekblad.nl/nieuws/nieuwe-chip-maakt-auto-doelwit/item4237, laatst gezien 10 december 2015.
20. Bron: een medewerker van ERTICO-ITS Europe vertelde dit per mail 'a platform founded in 1991 as a platform for the cooperation of all relevant stakeholders in the deployments of ITS systems in Europe', see http://ertico.com/vision-and-mission/, laatst gezien 17 september 2015. Ook zijn deze extra functies te vinden in een presentatie van NXP. Zie 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, laatst gezien 16 juli 2015.
21. Zie https://www.technischweekblad.nl/nieuws/nieuwe-chip-maakt-auto-doelwit/item4237, laatst gezien 10 december 2015.
22. Zie https://www.privacyfirst.nl/in-de-media/item/1026-telegraaf-11-februari-2016-vrees-voor-hacken-auto-op-snelweg.html , laatst gezien 18 februari 2016.
23. Council of the European Union, ENLETS Work programme 2014-2020, *Doc. 17365/13*: Brussels, 4 December 2013.
24. ENLETS is een informeel netwerk van de chefs van nationale politiediensten verantwoordelijk voor de implementatie van nieuwe technologieën, opgericht onder de Raad van de EU, dat voor het eerst onder leiding van Frankrijk in oktober 2008 bij elkaar kwam in Parijs. Council of the European Union, *Doc. 14669/08*, Brussels, 23 October 2008.
25. Rietveld voorziet dat deze kwetsbaarheid gebruikt gaat worden voor het omgekeerde; criminelen die dit gebruiken als oplossing om dure auto's zonder contactsleutel op te starten.
26. Bart Jacobs waarschuwde hiervoor al in 2013. Peter Rietveld bevestigde de exploiteerbaarheid voor dit doeleinde en wees erop dat sim-kaarten zeer gemakkelijk kunnen worden gehackt; dit waren zijn exacte woorden: 'building an attack-proof system2system authentication system over an untrusted network (such mobile) has until today never been successful. Chances that an attacker may actually breach such as system must not be underestimated.'
27. *Kamerstukken II* 2015-2016, 34 372, nr. 2 & 3 (p. 12).
28. Jonathan L. Zittrain, *The Future of the Internet and how to stop it*, Yale University Press 2008, p. 109.

III. Het recht op privacy en gegevensbescherming in de Verordening

In de Verordening staan verschillende overwegingen en artikelen die het recht op privacy en gegevensbescherming met betrekking tot de gegevensverwerkingen van eCall adresseren. De inhoud hiervan varieert van algemene toezeggingen over wetgeving, harde eisen aan het systeem tot bepalingen die specifieke verplichtingen voor fabrikanten bevatten.

Een algemene verplichting voor fabrikanten is dat zij alle nodige maatregelen dienen te nemen 'om te voldoen aan de voorschriften inzake privacy en gegevensbescherming van deze Verordening, overeenkomstig de artikelen 7 en 8 van het Handvest' (overweging 22, de voorschriften worden nader uitgewerkt in artikel 6 van de Verordening). De verwerking van persoonsgegevens door 112-eCall moet in overeenstemming zijn met Richtlijn 95/46/EG en Richtlijn 2002/58/EG (overweging 21, artikel 6 lid 1). Deze algemene verplichting moet met name garanderen dat 112-eCall niet opspoorbaar is en niet permanent wordt gevolgd (overweging 21), waarvoor de fabrikant moet zorgen (artikel 6 lid 4). De gegevens verwerkt in het kader van de Verordening mogen uitsluitend worden gebruikt voor het afhandelen van noodsituaties ontstaan door een ernstig ongeval (artikel 6 lid 2). Dit is een specifieke uitwerking van het doelbindingsbeginsel uit het gegevensbeschermingsrecht, dat erop ziet dat persoonsgegevens alleen mogen worden *verwerkt* voor een specifiek, welbepaald en gerechtvaardigd doeleinde.[29] Deze gegevens worden niet langer *bewaard* dan nodig is voor de afhandeling van de noodsituaties en worden volledig gewist zodra zij voor de afhandeling niet meer nodig zijn (artikel 6 lid 3). Dit is een specifieke uitwerking van het beginsel dat gegevens niet langer mogen worden bewaard dan noodzakelijk is ter realisering van het doel.[30]

Daarnaast moeten de fabrikanten ervoor zorgen dat in het interne geheugen van 112-eCall alleen de laatste drie locaties worden opgeslagen en de rest voortdurend worden verwijderd (artikel 6 lid 5).[31] De locatie wordt accuraat vastgesteld met satellietontvangers. Deze gegevens worden dus niet automatisch verzonden, maar opgeslagen op het interne geheugen van het systeem zelf.

Nog een harde eis die aan het systeem wordt gesteld is dat er geen uitwisseling van persoonsgegevens mogelijk mag zijn tussen het op 112 gebaseerde eCall-boordsysteem en andere systemen die Third Party Service (TPS) eCall of een dienst met toegevoegde waarde verlenen (overweging 15, artikel 6 lid 11). De Commissie moet aan deze eis gehoor geven door de vaststelling van gedetailleerde technische voorschriften (overweging 27, artikel 5 lid 8). Een andere eis die weliswaar niet is gericht op privacy, maar hier wel gevolgen voor kan hebben, is dat de eCall-boordsystemen gebaseerd moeten zijn op een 'interoperabel, gestandaardiseerd, beveiligd platform dat het mogelijk maakt in de toekomst toegang te bieden tot andere boordtoepassingen of -diensten' (overweging 16). De Commissie moet bij alle relevante belanghebbenden nagaan of aan deze eis wordt voldaan, of dat er nog voorschriften nodig zijn waarvoor het uiterlijk op 9 juni 2017 een wetsvoorstel moet doen gebaseerd op die behoefte (artikel 12 lid 2).

Aan de fabrikanten wordt de eis gesteld om technische voorschriften na te leven die door de Commissie worden vastgelegd.[32] Daarnaast worden er eisen gesteld aan de fabrikanten wat betreft het functioneren van de computersystemen aan boord. Zij dienen volgens de Verordening technische gegevensbescherming in de boordsystemen te integreren en de 'inbouwde privacy-benadering'[33] toe te passen (overweging 23). De integratie van 'privacybevorderende technologieën' in 112-eCall dient gebruikers van eCall garanties te verschaffen ter voorkoming van surveillance en misbruik van het systeem (artikel 6 lid 7).[34] Of dit specifieke implicaties heeft voor het ontwerp van het systeem en wat deze dan zouden inhouden, wordt door de Verordening in het midden gelaten.

Een eis die wel in de overwegingen is te vinden maar niet in de artikelen, is dat de alarmcentrales[35] de gegevens die over het 112 systeem worden verstuurd, niet aan derden mogen overdragen zonder *uitdrukkelijke instemming* van de betrokkene (overweging 25).[36] Hiermee lijkt te worden gerefereerd aan de *uitdrukkelijke toestemming*, hetgeen een zwaardere eis is dan de gewone ondubbelzinnige toestemming; een vorm die ook wel wordt gebruikt voor bijzondere persoonsgegevens. Manieren om hieraan te voldoen zijn bijvoorbeeld geschreven toestemming met een handtekening. Dit laat twee openingen om deze gegevens alsnog te verwerken. Ten eerste kunnen derde partijen die mogelijk inte-

> *112-eCall mag niet opspoorbaar zijn en niet permanent worden gevolgd.*

29. Dit beginsel, vastgelegd in artikel 6 lid 1 sub van Richtlijn 95/46/EG, is de hoeksteen van gegevensbeschermingsrecht, dat betekent dat gegevens alleen voor een specifiek doel mogen worden verwerkt.
30. Dit is vastgelegd in artikel 6 lid 1 sub E Richtlijn 95/46/EG. Het is wel interessant dat deze bepaling strijdig lijkt te zijn met een bepaling in artikel 7 (Gedelegeerde) Verordening 305/2013 waarin een bewaarplicht wordt geformuleerd voor de alarmcentrales om de ruwe MSD – dit is hoe de doorgezonden minimumreeks van gegevens wordt weergegeven voordat deze wordt gepresenteerd aan de eCall-alarmcentralist (art. 2 sub o) – voor een termijn overeenkomstig nationale regelgeving. Het doel van deze bewaarplicht is dat de alarmcentrales aan de bevoegde autoriteiten kunnen aantonen dat zij voldoen aan de gespecificeerde conformiteitseisen die staan opgesomd in art. 3.
31. Dit geeft uitvoering aan een eis die de Groep gegevens bescherming artikel 29 reeds stelde in 2006. Zie Article 29 Working Party, Working document on data protection and privacy implications in eCall initiative, *1609/06/EN*, 26 september 2006, p. 5.
32. De Commissie is krachtens artikel 5 lid 8 gemachtigd gedelegeerde handelingen vast te stellen waarbij deze voorschriften worden vastgelegd.
33. Dit is een vertaling van privacy-by-design, een idee dat privacy in het ontwerp van het systeem wordt gerespecteerd.
34. Dit geeft uitvoering aan een eis die de Groep gegevens bescherming artikel 29 al stelde in 2006. Zie Article 29 Working Party, Working document on data protection and privacy implications in eCall initiative, 1609/06/EN, 26 september 2006, p. 5-6.
35. Wat niet in deze Verordening staat, maar in Verordening 305/2013/EU, is dat de eCall-alarmcentrales worden beschouwd als de verantwoordelijken in de zin van art. 2 sub d van de Richtlijn 95/46/EG (artikel 6); dit is de partij die het doel en de middelen van de verwerking van persoonsgegevens vaststelt.
36. Dit lijkt invulling te geven aan de eis van de 'European Data Protection Supervisor' om te zorgen dat function creep van deze data wordt voorkomen. Zie Opinion of the EDPS on the proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall system and amending Directive 2007/46, p. 3.

resse hebben in zulke gegevens, bijvoorbeeld autofabrikanten of verzekeraars, deze trachten te verkrijgen middels toestemming en deze toestemming weer verbinden aan een gunstiger polis voor verzekeringen. Hoewel deze praktijk vandaag de dag wordt geaccepteerd door de Autoriteit Persoonsgegevens, kleven er bezwaren aan. Het komt er in feite op neer dat men zijn persoonsgegevens verkoopt. Dit betekent dat er aan het recht op privacy in de vorm van onbespied rondrijden een prijskaartje komt te hangen. Een andere mogelijkheid om dit soort gegevens te verwerken, is door ze te laten communiceren in het kader van de TPS-eCall. TPS wordt slechts genoemd in artikel 6 lid 9 sub i, waar is vastgesteld dat deze verwerkingen slechts mogen plaatsvinden op basis van uitdrukkelijke toestemming.

Prijskaartje aan onbespied rondrijden.

Al met al is er een aanzienlijk aantal bepalingen dat zich richt op het recht op privacy en gegevensbescherming. De bepalingen blijven echter allemaal steken op het niveau van afspraken. Partijen worden verboden om bepaalde handelingen te verrichten, of worden verplichtingen opgelegd. Bij de verplichtingen ten aanzien van het ontwerp valt op dat deze zijn geadresseerd aan de autofabrikanten, terwijl deze niet het functioneren van het uiteindelijke systeem bepalen; dit gebeurt binnen de normaliseringsorganisaties. Het verbod om gegevens niet verder te verwerken is vastgelegd in regels. Hierdoor is het volgen van dit verbod afhankelijk van de betrouwbaarheid van de partij die de gegevens verwerkt én of er eventueel conflicterende regels zijn waar hij zich aan dient te houden. De Uniewetgever laat hiermee zien dat hij zorgen omtrent deze rechten heeft meegenomen bij het opmaken van deze wetgeving en dat hij voornemens is geweest deze weg te nemen in de Verordening. De kwetsbaarheden die eerder zijn vastgesteld, alsmede of eCall zich registreert bij mobiele netwerken of deze slechts scant, laat hij onbesproken. Dit staat haaks op de ambities van de Commissie om een cultuur van grondrechten te vestigen waarin de rechten uit het Handvest in ieder stuk wetgeving volledig worden gerespecteerd. In de volgende paragraaf wordt beschreven waar het in de voorbereiding van de Commissie van dit wetgevingsvoorstel is misgegaan: de impact assessment.

IV. De impact assessment van de Commissie

De introductie van het Handvest van de Grondrechten van de EU breidde de taak van de Commissie uit: zij werd naast hoeder van de Verdragen ook die van de grondrechten vastgelegd in het Handvest. Zij positioneerde zichzelf in haar mededelingen als de instelling die de grondrechten van de Unie niet alleen zou bewaken, maar actief zou uitdragen en zou streven naar een 'fundamental rights culture'.[37] Het voornemen van de Commissie is om de proportionaliteit en noodzakelijkheid van wetgevingsvoorstellen te toetsen en hierdoor toe te zien op de constitutionele legaliteit van haar eigen handelen.[38] Dit kritisch toetsen dient al aan te vangen bij de voorbereidende fase van het opstellen van wetgevingsvoorstellen. Het voornaamste instrument dat de Commissie hiertoe tot haar beschikking heeft, is de *impact assessment*. Dit instrument dient om de impact van wetgevingsvoorstellen op onder andere fundamentele rechten vast te stellen. Hierbij wordt er mede gekeken naar onbedoelde negatieve gevolgen.[39] Uiteindelijk moet de staf van de Commissie, bij het overwegen van de verschillende opties, ook kijken naar begeleidende maatregelen die de negatieve effecten kunnen matigen.[40] Dit maakt de impact assessment, in theorie, een zeer geschikt instrument om al in een vroeg stadium technologie in wetgeving te screenen op kwetsbaarheden die kunnen worden geëxploiteerd voor andere doeleinden én om in deze wetgeving maatregelen verplicht te stellen die dit secundair gebruik tegengaan. Hierdoor kan worden bijgedragen aan een ontwerp dat het minst inbreuk mogelijk maakt op het recht op privacy, oftewel de subsidiariteit.[41] Andere aspecten die met deze assessment worden meegewogen zijn milieu, economische en andere maatschappelijke factoren.[42]

In de impact assessment uitgevoerd voor het eCall-systeem werden drie opties voor de inzet van eCall overwogen: geen actie, vrijwillige benadering en regulerende maatregelen (ofwel de verplichte uitrol).[43] Tot eind 2009 volgde de Commissie nog de vrijwillige benadering, maar deze zou niet leiden tot voldoende vooruitgang. De mogelijkheid die de artikel 29 Werkgroep opperde om elke auto uit te rusten met een eCall-systeem en het aan de rijder over te laten of het systeem wordt geactiveerd, wordt niet in de impact assessment besproken, terwijl deze het best verenigbaar is met het ideaal van zelfbeschikking. Er wordt uiteindelijk gekozen voor een volledige verplichting. Een andere suboptie was het verplichten van het in stelling brengen van de PSAP's en de ondersteuning van eCalls door aanbieders van draadloze mobiele-communicatienetwerken, maar deze aanbieders, de PSAP's en de autofabrikanten waren niet voor.[44] Hun argument hiertegen was dat een deel van de investeringen in eCall niet tot implementatie zou leiden. Dit zou vervolgens leiden tot marktfragmentatie. Wat opvalt bij de inschatting van de maatschappelijke impact van de verplichte optie is dat er niets wordt gezegd over fundamentele rechten, alleen over persoonsgegevens die door publieke autoriteiten worden behandeld. Dit wordt gezien als een

37. European Commission, Strategy for the effective implementation of the Charter, COM (2010) 573, p. 4.
38. European Commission, Strategy for the effective implementation of the Charter, COM (2010) 573, p. 7.
39. 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. 38.
40. European Commission, Impact Assessment Guidelines, 15 January 2009, SEC (2009) 92, p. 48.
41. De noodzakelijkheid uit het EVRM wordt vastgesteld door middel van de proportionaliteitstoets die uiteenvalt in de geschiktheid, noodzakelijkheid (in Nederland beter bekend als de subsidiariteit) en proportionaliteit in de strikte zin (stricto sensu, ook wel de belangenafweging).
42. Onder maatschappelijke factoren worden fundamentele rechten geschaard.
43. Commission Staff Working Paper Impact Assessment, SEC (2011) 1019 final, Brussels 8.9.2011, p. 15.
44. Commission Staff Working Paper Impact Assessment, SEC (2011) 1019 final, Brussels 8.9.2011, p. 30.

pluspunt.[45] De impact assessment heeft een overwegend economische focus. Fundamentele rechten worden er niet in genoemd. Er is één paragraaf van twaalf regels gewijd aan de bescherming van persoonsgegevens. Hierin wordt onder meer aangegeven dat eCall voldoet aan de gegevensbeschermingsrichtlijnen,[46] maar een expliciete toets vindt niet plaats. Er staat ook dat eCall het niet toestaat om van een afstand gelokaliseerd te worden.[47] Let wel, in hetzelfde document staat dus dat het systeem standaard is aangemeld bij een mobiel communicatienetwerk.[48] Tot slot is het enigszins vreemd dat in deze paragraaf staat dat de 'opinion' van Artikel 29-Werkgroep[49] is gevolgd, terwijl hierin een vrijwillige benadering van eCall werd bepleit. Kortom, eCall is niet getoetst aan het Handvest en het gegevensbeschermingsrecht wordt slechts oppervlakkig aangehaald.

Het is niet duidelijk waarom het recht op privacy door de staf van de Commissie buiten beschouwing is gelaten. De reden hiervoor kan liggen in het feit dat het toetsen van dit recht in de impact assessment een hoop kennis vergt van jurisprudentie van het EHRM en het HVJEU. Ook is er een parallel met de mededelingen en impact assessments rond de slimme meter – evenals eCall een ICT-systeem dat in de privésfeer wordt geplaatst op basis van Uniewetgeving – waarin het recht op privacy ook buiten beschouwing wordt gelaten. Binnen het gegevensbeschermingsrecht ligt echter de nadruk op het reguleren van de verwerking van persoonsgegevens, opdat deze wordt gelegitimeerd. Bij het beroep van de Commissie op dit recht wordt de noodzaak van de initiële inmenging stilzwijgend aangenomen. De verplichte installatie van eCall, alsmede de noodzaak om persoonsgegevens door dit systeem te laten verwerken, zijn twee essentiele inmengingen met het recht op privacy die de Commissie nalaat te toetsen.

Wat hiernaast opvalt aan de impact assessment is dat geen van de kwetsbaarheden uit paragraaf II is opgemerkt. In de richtsnoeren voor het uitvoeren van een impact assessment wordt de Commissie geïnstrueerd om te letten op *waarschijnlijkheid* en *omvang*[50] van de negatieve effecten en breder te kijken dan monetaire en kwantitatieve effecten.[51] Ook de onomkeerbaarheid van de impact moet in overweging worden genomen. Met het oog op de bevindingen uit paragraaf II kan worden vastgesteld dat verscheidene effecten van eCall op het recht op privacy zeer waarschijnlijk zijn en al ruim voor het opmaken van het wetgevingsvoorstel bestonden. De omvang van de privacy-inbreuk die volgt op een geëxploiteerde kwetsbaarheid is groot. Het verplicht uitrusten van alle auto's gecertificeerd voor de Europese markt komt er op neer dat, met het oog op aanverwante ontwikkelingen in verscheidene lidstaten, iedere auto wordt uitgerust met surveillance apparatuur die het lokaliseren, afluisteren en uitschakelen van auto's op een afstand mogelijk maakt. Nu eCall ook deel gaat uitmaken van een nieuwe markt tussen autobezitters en dienstenaanbieders, is het onwaarschijnlijk dat deze ontwikkeling een halt zal worden toegeroepen. De 'fundamental rights reflex'[52] die de Commissie beoogde met het invoeren van de impact assessment was bij eCall niet alleen onvoldoende; hij heeft nooit plaatsgevonden. Om een zo effectief mogelijke bescherming van het recht op privacy te realiseren, hadden er eisen aan het ontwerp van eCall moeten worden gesteld in de Verordening, die de negatieve effecten zouden voorkomen dan wel verlichten.

De impact assessment beoogt onder andere de proportionaliteit van de inmenging vast te stellen.[53] De verwachting is dat eCall het aantal verkeersdoden met 6,4% terugbrengt (op jaarbasis 2.500 van de 39.000 verkeersdoden per jaar). Om aan de proportionaliteitstoets te voldoen, moeten deze voordelen zwaarder wegen dan de nadelen. Dit is in de impact assessment onvoldoende onderbouwd, mede doordat belangrijke nadelen niet zijn opgemerkt. Bovendien is het koppelen van eCall aan een uniek identificatienummer niet noodzakelijk om te kunnen ingrijpen bij een ongeluk. Onduidelijk blijft waarom voor deze oplossing is gekozen. Vermoedelijk had dit de voorkeur van het bedrijfsleven dat dit nummer kan gebruiken als relatienummer. De werkelijke reden van de indringendheid van eCall vindt ogenschijnlijk zijn grondslag in motieven die ver afliggen van het optreden door hulpdiensten in een noodsituatie. De vitale informatie voor deze diensten heeft geen betrekking op identiteit.

Uit het bovenstaande volgt dat er een discrepantie bestaat tussen ambitie en praktijk, die invloed kan hebben op ontwerpkeuzes van eCall, die op hun beurt een beslissende invloed kunnen hebben op de vatbaarheid van het systeem om gebruikt te worden voor andere doeleinden dan het assisteren bij ongelukken. Deze keuzes zijn niet in de wetgeving vastgelegd. Nu de wetgever hier niet over heeft besloten, rijst de vraag: wie maakt deze keuze dan wel?

> *Impact assessment om impact van nieuwe wetgeving op fundamentele rechten vast te stellen.*

V. Essentiële ontwerpkeuzes

Volgens artikel 5 lid 8 Verordening 2015/758 wordt de Commissie gemachtigd overeenkomstig artikel 8 om gedelegeerde handelingen vast te stellen die zien op de gedetailleerde technische voorschriften en testen voor de EG-typegoedkeuring van voertuigen wat betreft het 112 eCall-systeem, diens onderdelen en technische eenheden. Deze voorschriften en testen zijn gebaseerd op de voorschriften vervat in artikel 5 lid 2 t/m 7 en de beschikbare normen voor eCall, met inbegrip van de normen die onder

45. Commission Staff Working Paper Impact Assessment, SEC (2011) 1019 final, Brussels 8.9.2011, p. 30.
46. Richtlijn 95/46 en Richtlijn 2002/58.
47. Commission Staff Working Paper Impact Assessment, SEC (2011) 1019 final, Brussels 8.9.2011, p. 13.
48. Commission Staff Working Paper Impact Assessment, SEC (2011) 1019 final, Brussels 8.9.2011, p. 25.
49. Het onafhankelijk advies- en overlegorgaan van Europese privacy-toezichthouders WG 29.
50. Vertaling van likelihood en magnitude.
51. European Commission, Impact Assessment Guidelines, 15 januari 2009, SEC (2009) 92, p. 38.
52. European Commission, Strategy for the effective implementation of the Charter, COM (2010) 573, p. 4.
53. European Commission, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC (2011) 567 final, Brussels, 6.5.2011, p. 6.

Het recht op privacy van de automobilist moet effectief worden beschermd.

lid 8 worden genoemd.[54] Het gaat om de volgende voorschriften:

> 'Pan-European eCall operating requirements' (a), 'eCall high level application requirements' (b), 'eCall end to end conformance testing' (c), 'eCall minimum set of data (MSD)' (d), 'Operating requirements for third party support' (e).

Een belangrijk deel van het ontwerp van eCall is dus vastgelegd in Europese normen. Dit zijn technische documenten die alleen maar inzichtelijk zijn wanneer je ervoor betaalt. Om de Nederlandse norm te kopen die ziet op de manier waarop eCall opereert bij het opstarten – NEN-EN 16072:2015 en Pan European eCall-operating eisen – moet men € 61,30 betalen.[55] Deze normen worden vastgesteld door Europese normaliseringsorganisaties, die mede beogen de technologische evolutie van het eCall systeem te faciliteren.[56] Het is opmerkelijk dat de documenten, waarin de werking van onderdelen van eCall die van doorslaggevende betekenis zijn voor de vraag of eCall standaard bij het opstarten verbinding maakt en daarmee een inbreuk vormt op het recht op privacy, slechts zijn in te zien na betaling. Normen hebben normaliter te gelden als privaatrechtelijke afspraken. Wanneer normen worden opgenomen in Uniewetgeving, zoals hier het geval is, verandert hun karakter in dat van Unierecht en zouden ze ook aan de eisen van toegankelijkheid en voorzienbaarheid moeten voldoen.[57] In Nederland noemt men dit 'het dwingend verwijzen naar normen' en moeten deze normen vrij beschikbaar worden gemaakt.[58]

De keuzes omtrent het ontwerp die niet worden gemaakt in de Verordening, worden overgelaten aan de onderhandelingsruimte tussen de Commissie en de normaliseringsorganisaties. Hoe deze ruimte wordt ingevuld, bepaalt of het ontwerp resulteert in beperkingen op het recht op privacy. Normaliseringsorganisaties staan erom bekend dat het zwaartepunt van de belangen die zij behartigen bij het bedrijfsleven ligt. Met een blik op de beoogde toekomst van het eCall-systeem, dat ook als platform dient voor commerciële diensten, ligt het voor de hand dat het oorspronkelijke ontwerp van het systeem is ingericht om een eventuele, ook commerciële, evolutie te faciliteren. Het zou tegen de huidige economische logica indruisen als dit systeem niet een continue uitwisseling van locatie- en andere gegevens mogelijk zou maken.

Echter, zo'n ruime delegatie van bevoegdheden voldoet niet aan de regels die volgen uit artikel 290 VWEU en de nadere invulling die het HvJEU hier aan heeft gegeven. Deze delegatie betreft namelijk alleen de bevoegdheid van de Commissie om niet-wetgevingshandelingen vast te stellen ter wijziging of aanvulling van niet-essentiële onderdelen van de Verordening.[59] Hoewel het onderscheid *essentieel/niet-essentieel* eerst louter een politieke kwestie was, is dit inmiddels achterhaald door rechtspraak van het HvJEU.[60] Het Hof heeft bepaald dat, wanneer het om *politieke keuzes* gaat (dat wil zeggen met uiteenlopende belangen) of wanneer de handeling dermate belangrijke inmengingen met grondrechten mogelijk maakt, tussenkomst van de Uniewetgever is vereist. Dit zijn alternatieve criteria. Het past niet binnen het onderscheid dat het Hof aanbrengt om politiek gevoelige ontwerpkwesties met grote gevolgen voor de effectieve bescherming van het recht op privacy, neer te leggen bij de Commissie, laat staan bij de normaliseringsorganisaties. Beslissingen aangaande deze *essentiële ontwerpkwesties* zijn voorbehouden aan de Uniewetgever, die op zijn beurt is gebonden aan de eisen die volgen uit het Handvest.

VI. Effectieve bescherming van het recht op privacy

Het recht op privacy van de automobilist moet effectief worden beschermd. Effectieve bescherming impliceert dat de automobilist niet onnodig wordt blootgesteld aan het risico op willekeurige inmenging in zijn recht om zich vrij van observatie in zijn auto te begeven. De bescherming van privacy wordt door verschillende factoren beïnvloed. Het recht is hier maar één van. Structurele bescherming van het recht op privacy volgde oorspronkelijk uit de moeilijkheid om tot de privésfeer door te dringen met speciale maatregelen.[61] Een andere factor is economische haalbaarheid.[62] Kosten vormen een belangrijke begrenzing voor het inzetten van surveillance-maatregelen door publieke autoriteiten. In 2010 schreef Ian Brown voor de Commissie een rapport waarin hij stelde dat het in de nabije toekomst duurder zal zijn om mensen uit te sluiten van surveillance, dan ze in te sluiten. eCall levert in zijn huidige vorm een grote bijdrage aan het verlagen van de drempel voor de staat om reisbewegingen van auto's vast te leggen, alsmede om gesprekken vast te leggen. Ten slotte, eCall kan ook voor de staat de drempel verlagen om automobilisten staande te houden.

Om te voorkomen dat het recht op privacy wordt uitgehold, moet bij de verplichtstelling van nieuwe technologieën middels EU wetgeving worden gekeken naar de *inmengingen* én het *risico op inmengingen* die de technologie in kwestie mogelijk maakt.

54. Inmiddels zijn deze normen vernieuwd, zie link NEN.
55. Zie https://www.nen.nl/NEN-Shop/Norm/NENEN-160722011-en.htm, laatst gezien 18 februari 2016.
56. Zie overweging 26 Verordening 2015/758.
57. R.A. Hoenkamp, G.B. Huitema en A.J.C. de Moor-van Vugt, 'Law and standards: Safeguarding societal interests in smart grids', in: R. Leenes & E. Kosta (ed.), Bridging distances in technology and regulation, Oisterwijk, the Netherlands: Wolf Legal Publishers 2013, p. 117.
58. Zie https://www.nen.nl/Over-NEN/Vrij-beschikbare-normen.htm, laatst gezien 22 mei 2016.
59. Art. 290 VWEU.
60. In 2011 schreef Voermans dat wat essentieel was is 'essentially a question to which there is only a political answer'. W. Voermans, 'Delegation Is a Matter of Confidence'. European Public Law 17, no. 2 (2011): 313-330, p. 321. Hij achtte het onwaarschijnlijk dat het HvJEU een mening hierover zou formuleren. Hoewel dit in overeenstemming was met eerdere jurisprudentie, veranderde het Hof zijn koers in 2012 in de zaak C-355/10 European Parliament v. Commission.
61. Surden, Structural Rights in Privacy, SMU Law Review 2007/60, p. 1605.
62. Zie http://tegenlicht.vpro.nl/afleveringen/2013-2014/bureau-voor-digitale-sabotage.html, laatst gezien 15 augustus: interview met Eleanor Saitta vanaf 12:50.

Dit is in lijn met de impact assessment methode om onbedoelde negatieve effecten te verlichten, alsmede met de ambitie van de Commissie om de rechten in het Handvest zo effectief mogelijk te maken. Deze interpretatie wordt ondersteund door de rechtspraak van het EHRM, waarin het Hof de rechten zo uitlegt dat deze effectief en praktisch moeten zijn, in tegenstelling tot denkbeeldig en theoretisch.[63] Bij het invoeren van eCall wordt weliswaar niet beoogd om een beperking van het recht op privacy tot stand te brengen, maar door essentiele aspecten van het ontwerp niet vast te stellen in de Verordening wordt de mogelijkheid opengelaten dat het systeem kwetsbaarheden introduceert die later worden geëxploiteerd. Zodra een lidstaat op dit systeem voortbouwt, voor andere doeleinden die vallen onder de soevereiniteit van de lidstaat, kan er geen beroep meer worden gedaan op de bescherming van het EU recht. Dit blijkt onder andere uit het antwoord van het HvJEU op een prejudiciële vraag van de Raad van State waarin het Hof werd verzocht om te oordelen over de rechtmatigheid van het verwerken van vingerafdrukken van de Nederlandse bevolking. Deze vingerafdrukken waren verkregen op basis van een Europese verordening die beoogde identiteitsfraude bij de afgifte van reisdocumenten te voorkomen, maar werden in Nederlandse wetgeving ook beschikbaar gesteld voor andere doeleinden, waaronder opsporing en vervolging van strafbare feiten, en onderzoek naar handelingen die een bedreiging vormden voor de nationale veiligheid inlichtingendiensten.[64] De Raad van State verwees hierbij expliciet naar artikel 7 en 8 Handvest (recht op privacy en op bescherming van persoonsgegevens), Richtlijn 95/46 en artikel 8 EVRM, waarop het Hof kortweg reageerde dat Unierecht in dezen niet van toepassing was. Uitspraken van de WG 29 over eCall 'that any secondary use of data, e.g. for enforcement procedures related to traffic, should not be allowed as it would be contrary to the principles of the Data protection directive', getuigen van een onterecht vertrouwen in het opleggen van verboden. Dergelijke afspraken op Europees niveau bieden geen effectieve bescherming tegen *function creep* (eventueel opgelegd door de nationale wetgever).[65]

De enige oplossing die bijdraagt aan een effectieve bescherming van het recht op privacy is om deze zorgen omtrent privacy mee te nemen vanaf het begin van het ontwerp van een systeem en de eisen aan het ontwerp een centrale plaats te geven in de wetgeving die het systeem introduceert. Op deze manier kan een systeem worden ontwikkeld dat het recht op privacy optimaal respecteert. Het is bewezen dat het mogelijk is om privacy succesvol in systeemontwerpen te integreren zonder aan de functionaliteit hiervan in te boeten.[66] In het kader van eCall had het scannen van eCall voor mobiele netwerken in de Verordening moeten zijn vastgelegd. Het risico op gebruik van de microfoon had ook door een slim ontwerp kunnen worden voorkomen, bijvoorbeeld door de stroomtoevoer van de microfoon standaard te onderbreken en een mechanisme aan te brengen waardoor de 'onderbreker' pas fysiek wordt verwijderd als een ongeluk plaatsvindt of eventueel wanneer de bestuurder een manuele handeling uitvoert.[67] Het maken van keuzes hieromtrent vormen een zeer complexe aangelegenheid op het snijvlak van recht en technologie, waarvoor de Commissie niet goed is toegerust. Beslissingen van een dergelijk groot publiek belang, met mogelijk controversiële gevolgen, dienen voorbehouden te blijven aan de wetgever en niet uitbesteed te worden aan normaliseringsorganisaties. Dat hiervoor wel is gekozen lijkt eerder te zijn ingegeven door een afwezigheid van kennis bij de wetgever over de mogelijk negatieve gevolgen van eCall, dan het resultaat van een goed geïnformeerde keuze.

VII. Conclusie

De benadering die de Commissie heeft gekozen in het wetgevingstraject rond eCall geeft blijk van een eenzijdige focus op het gegevensbeschermingsrecht. Dit volgt onder meer uit het feit dat er alleen is gekeken naar vragen omtrent hoe gegevensverwerkingen dienen plaats te vinden. Meer fundamentele vragen aangaande de noodzaak van verplichte installatie van eCall en de noodzaak voor het systeem om persoonsgegevens te verwerken, zijn onterecht buiten beschouwing gelaten. De eenzijdige focus op gegevensbescherming heeft als voordeel dat commerciële ambities van de betrokken belanghebbenden bij de TPS eCall ruim baan krijgen, maar de keerzijde is dat zorgen omtrent privacy nauwelijks worden geadresseerd. Gegevensbeschermingsrecht is maar deels geschikt om de impact van technologie op het recht op privacy te toetsen, omdat het beperkter is in zijn reikwijdte. Dat een belangrijk gedeelte buiten de reikwijdte van het gegevensbeschermingsrecht valt, resulteert in het geval van eCall erin dat een serie kwetsbaarheden door derden kunnen worden geëxploiteerd. Daarmee leidt deze maatregel die de veiligheid van automobilisten in exceptionele situaties probeert te vergroten, tot een standaard onveilige situatie in de auto.

Snijvlak van recht en technologie.

Effectieve bescherming van het recht op privacy begint bij het ontwerp van ICT-systemen. Voordat de Uniewetgever de installatie van ICT-systemen in de persoonlijke omgeving van Unieburgers verplicht stelt, moet hij eerst zorgvuldig kijken naar de

63. 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'. ECtHR, Sabanchiyeva and Others v. Russia, application no. 38450/05, 6 juni 2013, § 132.
64. Zie Steve Peers, http://eulawanalysis.blogspot.se/2015/04/biometric-data-and-data-protection-law.html, laatst gezien 7 augustus 2015. T.H.A. Wisman, Giving Member States the Prints and Data Protection the Finger, [2015] 3 EDPL, p. 245-248.
65. Article 29 Working Party, Working document on data protection and privacy implications in eCall initiative: 1609/06/EN WP 125, 26 september 2006, p. 3.
66. C. Raab, 'Effects of surveillance on civil liberties and fundamental rights in Europe', in Surveillance in Europe, ed. R. Kreissl, D. Wright (Routledge: 2015), p. 261-262.
67. Straaljagers op vliegdekschepen werk(t)en met een soortgelijk mechanisme door metalen pinnen die de stroomtoevoer naar raketten onderbraken, zodat technische staf handelingen aan een vliegtuig kon uitvoeren, zonder het risico dat door een fout in het stroomcircuit een raket zou worden afgevuurd.

mogelijke negatieve gevolgen hiervan voor het recht op privacy en hoe deze kunnen worden voorkomen door het stellen van ontwerpeisen aan dergelijke systemen. De impact assessment kan een belangrijke rol spelen bij het detecteren van mogelijke negatieve gevolgen en het formuleren van essentiële ontwerpkeuzes. Nu keuzes hieromtrent een politiek controversiële aangelegenheid vormen, dienen deze keuzes te worden opgenomen in de wetgevingshandeling zelf. Hierdoor worden ook de regels omtrent delegatie gerespecteerd.

eCall moet niet op zichzelf worden bekeken, maar worden gezien als een volgende stap in de richting van een surveillancesysteem dat langzaamaan in alle aspecten van de privésfeer doordringt. De meest effectieve bescherming van het recht op privacy bestaat in de burger de vrije keuze te geven over de installatie van dit soort technologie in de privésfeer.