The Quest for the Effective Protection of the Right to Privacy:

On the Policy and Rulemaking concerning Mandatory Internet of Things systems in the European Union

Tijmen H.A. Wisman

THIS RESEARCH WAS FORMALLY CONCLUDED ON 31st of December 2017

The painting used for the cover is a work of Miek Twerda.

VRIJE UNIVERSITEIT

The Quest for the Effective Protection of the Right to Privacy:

On the Policy and Rulemaking concerning Mandatory Internet of Things Systems in the European Union

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad Doctor aan

de Vrije Universiteit Amsterdam,

op gezag van de rector magnificus

prof.dr. V. Subramaniam,

in het openbaar te verdedigen

ten overstaan van de promotiecommissie

van de Faculteit der Rechtsgeleerdheid

op woensdag 23 januari 2019 om 15:45 uur

in de aula van de universiteit,

De Boelelaan 1105

door

Tijmen Hendrik Adriaan Wisman

geboren te Texel

promotoren: Prof. dr. A.R. Lodder

Prof. A. Murray

copromotor: mr. dr. M. van der Linden

Chapter 1

He was found by the Bureau of Statistics to be
One against whom there was no official complaint,
And all the reports on his conduct agree
That, in the modern sense of an old-fashioned word, he was a saint,
For in everything he did he served the Greater Community.
Except for the War till the day he retired
He worked in a factory and never got fired,
But satisfied his employers, Fudge Motors Inc.
Yet he wasn't a scab or odd in his views,
For his Union reports that he paid his dues,
(Our report on his Union shows it was sound)
And our Social Psychology workers found
That he was popular with his mates and liked a drink.
The Press are convinced that he bought a paper every day
And that his reactions to advertisements were normal in every way.
Policies taken out in his name prove that he was fully insured,
And his Health-card shows he was once in hospital but left it cured.
Both Producers Research and High-Grade Living declare
He was fully sensible to the advantages of the Instalment Plan
And had everything necessary to the Modern Man,
A phonograph, a radio, a car and a frigidaire.
Our researchers into Public Opinion are content
That he held the proper opinions for the time of year;
When there was peace, he was for peace: when there was war, he went.
He was married and added five children to the population,
Which our Eugenist says was the right number for a parent of his generation.
And our teachers report that he never interfered with their education.
Was he free? Was he happy? The question is absurd:
Had anything been wrong, we should certainly have heard.

The Unknown Citizen by W. H. Auden, 1939

Chapter I
Introduction

1. Research Context: The Age of Internet of Things

Everyware is the colonization of the everyday environment by ICT.[1]

The age of the Internet of Things is upon us. ICT is increasingly moving out of its conventional box and integrating seamlessly with our everyday surroundings: cars, televisions, streetlamps, electricity meters and even trees are *tagged* and connected through a variety of network technologies. Since the 1980s various visions have been developed, coined in phrases such as 'ubiquitous computing', 'Ambient Intelligence' and 'Internet of Things'.[2] The common denominator is that they seek to harness the processing power of fragmented products and connect these through network technology.

IoT Systems: What is in the name?

Kevin Ashton coined the phrase 'Internet of Things' (hereinafter IoT) and asserted that 'things' are much better at capturing data than people.[3] As an employee of Procter & Gamble, he was involved in the optimisation of supply-chain management. These 'things' record and process data on the nodes of the network informing and optimising various business processes for parties employing IoT technology. Creating an IoT requires embedding surfaces of everyday life with information processing technology.[4] The relationship between people and technology continuously becomes closer as people surround themselves by networked objects with sensors, transforming society slowly into an ever-growing sensor network. In addition to sensors, some of the systems in the IoT are equipped with features that enable their remote shutdown, also known as actuators. Generally an IoT system exhibits three features:

(1) it records and collects data[5] through sensors;

(2) it communicates this data through network technologies;

---

[1] Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (1st edition, Pearson Education 2006) 33.

[2] Kevin Ashton, 'That "Internet of Things" Thing' (RFID Journal, 22 June 2009). <http://www.rfidjournal.com/articles/view?4986> accessed 7 June 2018; Mark Weiser, *The Computer for the 21st Century* (Scientific American 1991).

[3] ibid.

[4] This key quality can be found in Thesis 3 of Greenfield's book 'Everyware': 'Everyware is information processing embedded in the objects and surfaces of everyday life'. These key qualities derive from ao Greenfield (n 1) 18.

[5] ISO/IEC 2382-1 provides that data is 'a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing'.

(3) it can allow for remote control through actuators.

Surveillance is a central quality of the IoT. The surveillance and control potential of IoT technology became all the more relevant when the European Commission decided to actively formulate and execute IoT policy.[6] It launched an Action Plan on the IoT in 2009 and has pursued the deployment of IoT systems in the home and the car. The system in the home is the smart electricity meter which measures the usage of electricity on a detailed level, once every 15 minutes, and is equipped with network technology to send this data to the meter operator. The system in the car is the eCall system, equipped with GSM and GPS, which sends a minimum set of data when the car is involved in an accident. eCall can also be used by third parties to offer private services. These systems are particularly interesting as their installation has become mandatory by European Union (hereinafter EU) law. This means citizens are no longer free to decide whether their private environment and property are equipped with these systems, which might have adverse consequences for their privacy.

Privacy is vital to a free society: being monitored implies that citizens have to fear the consequences of their registered actions and so can no longer conduct their affairs freely. In the words of Gavison, '[p]rivacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of democracy.'[7] Civil rights are at the core of constitutional democracy.[8] Although the concept of civil rights is complex and fluid their importance has been widely recognised after the atrocities of WWII leading to their codification in the Universal Declaration of Human Rights (UDHR, adopted in 1948) and the European Convention on Human Rights (ECHR, adopted in 1950).[9] Civil rights, especially the right to privacy, are often framed as opposed to public interests, but we ought not to forget that privacy is a public interest in itself.[10] The point of departure of this book is that the effective protection of the right to privacy is essential to preserve a free and just society.

The right to privacy is just one factor that curtails surveillance practices. Another factor is plain economics.[11] Costs are an important limit exerted upon public authorities concerning their use of surveillance competences. In 2010, Ian Brown made the point that in the near future it will cost more to exclude people from total surveillance than to include them.[12] The

[6] Commission, 'Internet of Things – An action plan for Europe' (Communication from the Commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions COM (2009) 278 final.

[7] Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 YaleLJ 421, 455.

[8] Constantijn AJM Kortmann, Constitutioneel Recht (Kluwer 2001) 53.

[9] The ECHR was signed and ratified by all member states of the Council of Europe.

[10] This view corresponds with John Dewey's account of civil rights. John Dewey, 'Liberalism and Civil Liberties' in Jo Ann Boydston (ed), *The Later Works, 1925-1953* (Volume II: 1935-1937, 372-375.

[11] VPRO Tegenlicht, 'Bureau voor digitale sabotage' (Interview with Eleanor Saitta: excerpt starts from 12:50, Tegenlicht 2 March 2014) https://www.vpro.nl/programmas/tegenlicht/kijk/afleveringen/2013-2014/bureau-voor-digitale-sabotage.html (from 12:50), accessed 15 August 2015.

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

design of IoT systems is crucial to the question whether these can be used for surveillance purposes. Information is the fuel for governing affairs, whether these are private or public in nature. [13] Information can be extracted from the data flows produced by IoT systems, which are inextricably linked to the extent to which certain areas of life can be subjected to governing. Since this is dependent on the design of these systems, their design is a political matter. These systems, furthermore, can be equipped with features that can be exploited for surveillance purposes. An omnipresent ICT-infrastructure through which third parties can access private information and to a degree even actively exercise control, takes away people their control over their information, their environment and ultimately their lives. If these systems become mandatory through EU legislation, this could equal forcing privacy-intrusive surveillance systems into citizens' daily lives. The subsequent blurring of the private and public sphere is considered to be a trait of totalitarian societies.[14]

IoT systems potential for surveillance and control

The enormous surveillance power that can be wielded through the IoT has been commented on by numerous authors. Bruce Schneier, has pointed out that companies such as Google originally knew only about your personal interests from computer data, but when modules on cars and home appliances become internet-enabled, i.e. when they become part of the IoT, then digital trails would also be produced by activities that originally took place offline. [15] According to Schneier, it will not take long before the whole spectrum of our activities will be registered and captured forever. Every activity that is mediated through ICT, which records and communicates data to third parties, takes away the private character of the act. The act will be registered, stored and potentially retrieved by the parties employing the technology.

Schneier's insights were hardly new. An early visionary, Mark Weiser, heralded the introduction of ubiquitous computing as a development that would bring great benefits, however, he also issued a warning regarding a number of social issues:

> 'Perhaps key among them is the privacy: hundreds of computers in every room all capable of sensing people near them and linked by high-speed networks, have the potential to make totalitarianism up to now seem like sheerest anarchy.'[16]

---

[13] David Lazer and Viktor Mayer-Schonberger, *Governance and Information Technology: From Electronic Government to Information Government* (MIT Press 2007).

[14] Hannah Arendt, *The Origins of Totalitarianism* (Schocken Books 1951). Bart Jacobs, 'Keeping our surveillance society non-totalitarian' [2009] 1(4) Amsterdam Law Forum <http://amsterdamlawforum.org/article/view/91> accessed 7 June 2018.

[15] Bruce Schneier is a security technologist. See Bruce Schneier, 'Will giving the internet eyes and ears mean the end of privacy?' (The Guardian, 16 May 2013). <http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google> accessed 7 June 2018. In 2014 Google bought Nest, a company that produces smart thermostats and smoke detectors, with in-built motion detectors and a microphone, thereby expanding their surveillance apparatus to the home.

[16] Mark Weiser, *The Computer for the 21st Century* (Scientific American 1991) 25.

American intelligence agencies see opportunities in this new network. Then director of the CIA, David Petraeus, stated in 2012 that *transformational* is an overused word, but that it applies to the effect the IoT would have on the face of surveillance. In an interview on the IoT systems in the home, he commented that the 'resultant chorus of "connected" devices will be able to be read like a book – and even remote-controlled.'[17] In a congressional testimony in 2016, the US Director of National Intelligence, James R. Clapper, gave an indication of global threats: '"smart" devices incorporated into the electric grid, vehicles – including autonomous vehicles – and household appliances' are a threat to privacy, data integrity and continuity of services. He added to this that intelligence services 'might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks for user credentials.'[18] The documents which were disclosed in the Wikileaks on Vault 7 revealed that IoT devices were not just treated as a threat by Clapper, they are also an opportunity.[19]

The belief in the transformational effect of the IoT on the face of surveillance is not limited to the confines of intelligence agencies. The German Presidency of the Council gained the support of the Commission in 2007 to set up a group at the ministerial level to discuss informally policy matters of European Home affairs.[20] This assembly was entitled the 'Future Group' and referred to itself as the 'Informal High Level Advisory Group on the Future of European Home Affairs Policy'. It was co-chaired by then VP of the Commission and brought together, ad personam, the Ministers of Interior of nine Member States, 'a common law observer (United Kingdom)' the President of the LIBE Committee of the European Parliament, as well as a representative of the Council's Secretariat General.[21] The report of the first meeting stressed that the Group created an opportunity for future presidencies and the Commission to uphold an informal dialogue prior to drafting any legislative proposals.[22] The discussions of the Group did not concern lawmaking, but the 'future objectives and priorities of European Home Affairs'.[23] In one of the concept papers drafted in pursuance of these 'fireplace-like discussions' it was revealed they actually used privacy for firewood:

---

[17] Rob Waugh, 'The CIA wants to spy on you through your TV: Agency director says it will "transform" surveillance' (Mailonline, 16 March 2012) <http://www.dailymail.co.uk/sciencetech/article-2115871/The-CIA-wants-spy-TV-Agency-director-says-net-connected-gadgets-transform-surveillance.html> accessed 7 June 2018.

[18] James R Clapper, 'Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community' (2016) Congressional Testimonies 1.

[19] Alex Hern, '"Am I at risk of being hacked?" What you need to know about the "Vault 7" documents' (The Guardian, 8 March 2017) <https://www.theguardian.com/technology/2017/mar/08/wikileaks-vault-7-cia-documents-hacked-what-you-need-to-know> accessed 7 June 2018.

[20] Future Group, 'Public Security and Technology in Europe: Moving Forward' (Concept paper on the European strategy to transform Public security organisations in a Connected World, Portugal 2007) <http://bit.ly/PqvWIJ> accessed 17 August 2012, 8.

[21] Future Group, 'Freedom, Security, Privacy – European Home Affairs in an open world' (June 2008) <www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf> accessed 7 June 2018, 3.

[22] Future Group, 'First meeting of the Future Group' (Warm-up session 20 and 21 May 2007, Eltville Germany) <http://bit.ly/VeLZf2> accessed 7 June 2018, 1.

[23] ibid.

> 'Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organizations, and create huge opportunities for more effective and productive public security efforts.'[24]

This sweeping statement is followed by an admission that 'these developments raise fundamental issues in relation to privacy and how much information about the behaviour of citizens should be shared with States and in what circumstances' and claims that citizens' expectations of privacy should be balanced 'against their expectations of proactive protection'.[25] The underlying assertion is that data generated by IoT systems will be used as a tool for mass surveillance of the citizens of all Member States. The stated main objective is 'the full interoperability of information systems and the improvement of security research'.[26] The Group recognised the importance of explaining the practical results of this policy to citizens in layman's terms; nonetheless the specific work of this group was supposed to stay confidential and '**transparency** of its work [would] be ensured by sharing information, e.g. in informal dinner of Ministers, informal Council meetings and documents to the other members of the JHA Council'.[27] The proposal served the Council of the EU in preparing the Stockholm Program on justice, freedom and security.[28] In the Stockholm Program, a five-year program of the Council of the EU containing guidelines for justice and home affairs, the paragraph that deals with the protection of citizen's rights in the information society states:

> 'The Union must secure a comprehensive strategy to protect data within the EU and in its relations with other countries. In that context, it should promote the application of the principles set out in relevant EU instruments on data protection and the 1981 Council of Europe Convention on data protection as well as promoting accession to that convention. It must also foresee and regulate the circumstances in which interference by public authorities with the exercise of these rights is justified and also apply data protection principles in the private sphere.'[29]

This program, read in conjunction with the Future Group reports, spells out an ambition to record flows of data in the private sphere through the installation of IoT systems. The assumption is that these systems will generate useful data for public authorities. This raises the question whether this assumption is reconcilable with the human rights standards in force in the EU. Enabling mass surveillance through the obligatory installation of IoT systems in the private sphere appears more suitable as an ingredient for a dystopian novel, rather than a page in a policy document of a transnational organisation which claims in its constitutional

[24] 'Public Security and Technology in Europe: Moving Forward' (n 20) 8.
[25] ibid.
[26] 'First meeting of the Future Group' (n 22) 3.
[27] ibid 1. Bold was in the original.
[28] The area of justice, freedom and security is not included in the scope of this research, but this example is to illustrate the real risk that personal data will be used to fuel the surveillance apparatus of EU Member States.
[29] Council of the European Union, 'The Stockholm Programme – An open and secure Europe serving and protecting the citizens' (2009) Brussels <https://ec.europa.eu/anti-trafficking/eu-policy/stockholm-programme-open-and-secure-europe-serving-and-protecting-citizens-0_en > accessed 7 June 2018, 18.

treaties to be founded on values such as respect for human dignity, freedom and respect for human rights.[30]

In the Commission's 2009 Action Plan on the IoT, the subheading 'Privacy and protection of personal data' is found under the heading 'Lifting the obstacles to the uptake of the Internet of Things'.[31] Respect for privacy and data protection is presented as a precondition for the social acceptance of the IoT. Positioned as 'a prerequisite for trust and acceptance of these systems' is that 'appropriate data protection measures are put in place against possible misuse and other personal data related risks'.[32] In focusing on the use of the recorded data, the silence on the recording and collection of the data itself stands out. This silence is striking since architectural choices regarding the recording and collection of data can prevent data from becoming available for practices such as data mining, as opposed to trying to regulate the use of data which does not impact the availability of the data as such, but merely the conditions under which it can be used. By framing privacy as an obstacle, the Commission positions privacy as a value opposed to its policy goals and incorrectly presents IoT policy as a zero-sum game.

In 2010, the European Parliament issued a resolution on IoT in which it took a stronger position on privacy than the Council and the Commission. It explicitly considered that concern for personal privacy 'may block applications', considering it necessary to provide public empowerment and user control mechanisms and the possibility to 'opt-out of individual IoT technologies without disabling other applications or a device as a whole'.[33] Also, it emphasised the importance of privacy and data protection in adopting a general principle which requires IoT technologies to be designed to collect and use only the minimum amount of data necessary to perform their function.[34] It follows from this resolution that citizens can opt out of certain IoT systems, which would include the features of data processing and remote control. The data processing feature should not process more data than necessary to attain the goal for which the system was installed. In 2015 a study was issued for the LIBE Committee on 'Big Data and Smart Devices and Their Impact on Privacy'.[35] This study underlined that the 'European Commission's perspective is very much commercially and economically driven, with little attention to the key legal and social challenges regarding privacy and personal data protection'.[36] Although this study recognised that IoT systems could collect data unobtrusively and that this collection could potentially lead to intrusive

[30] Article 2, Treaty on European Union (TEU) [2012] *OJ* C 326.
[31] COM (2009) 278 (n 6).
[32] ibid 6.
[33] European Parliament Resolution of 15 June 2010 on the Internet of Things 2009/2224 (INI), paras 4, 15 and 22.
[34] ibid, para 35.
[35] Gloria Gonzáles Fuster and Amandine Scherrer, 'Big Data and Smart Devices and Their Impact on Privacy', European Parliament, Directorate-General for Internal Policies, Policy Department Citizens' Rights and Constitutional Affairs.
[36] ibid, 6. Even though the position taken in this report is more critical than the Commission, it also only focusses on safeguards which follow from data protection law, even in relation to mandatory IoT systems such as smart meters.

practices such as profiling and data mining, the final recommendations do not address the recording and collection of data.[37]

Pursuing the vision of the IoT could have grave gradual consequences on citizens' sense of freedom, the diminishment of which will be felt in parallel to the realisation of being surrounded by a surveillance network. Los argues that this inability to understand what is happening around us could have a paralysing effect on people, as their sense of 'being helpless in face of the omnipresent, interconnected and internationalized surveillance' is growing.[38] This effect is also defined as the disciplinary effect of scrutiny, the central idea behind the prison-design commonly known as the panopticon. Jeremy Bentham, who is regarded as the initial designer of the panopticon, referred to it in the following words: 'a new mode of obtaining power of mind over mind, in a quantity hitherto without example.'[39]

The potential of these systems to encroach upon citizens' freedom lies also in their capacity to exercise remote control. Smart meters are often equipped with a function which allows remote shut down of the electricity supply, and eCall introduces a vulnerability in cars which can be used to shut cars down from a distance.[40] An informal network of heads of police departments responsible for implementing new technologies, instigated under the Council of the EU, published a report already in 2014 adopting the ambition to be able to 'Remote Stopping Vehicles' to deal with 'cars on the run'.[41] The description given was to work on a '*proportionate* response' based 'on a technological solution that can be a "build in standard"' for '*all cars* that enter the European market' (emphasis added).[42] The mandatory installation of IoT systems therefore creates the potential for a fundamental shift in the power relation between citizens and the state, allowing the latter to exercise power at a distance. Schermer described this as the shift from an 'architecture of observation' to an 'architecture of control'. [43] Bentham's panopticon is child's play compared to an unrestricted IoT infrastructure which creates an architecture of observations and control.[44]

[37] ibid, 13, 22

[38] M. Los, 'Looking into the future: surveillance, globalization and the totalitarian potential', in *Theorizing Surveillance: The panopticon and beyond*, ed. D. Lyon (Devon: Willan Publishing, 2006) 73.

[39] Jeremy Bentham, 'Panopticon' in Miran Bozovic (ed), The Panopticon Writings (London, Verso 1995).

[40] Boris van Zonneveld, 'Nieuwe chip maakt auto doelwit' (*Technisch Weekblad*, 29 June 2013) <https://www.technischweekblad.nl/nieuws/nieuwe-chip-maakt-auto-doelwit/item4237> accessed 13 July 2018.

[41] Council of the European Union, ENLETS Work programme 2014-2020, *Doc. 17365/13*: Brussels, 4 December 2013, 8.

[42] ENLETS Work programme 2014-2020, *Doc. 17365/13,* 8.

[43] B. Schermer, 'Surveillance and Privacy in the Ubiquitous Network Society' [2009] 1(4) Amsterdam Law Forum <http://amsterdamlawforum.org/article/view/95/159> accessed 7 June 2018, 68.

[44] Tijmen HA Wisman, 'Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things' (2013) 4(2) EJLT < http://ejlt.org/article/view/192/379> accessed 5 June 2018.

2. Applying EU law to the design of mandatory IoT systems

'*The nature of the internet is not God's will. Its nature is simply the product of the design.*'[45]

This famous quote of Lessig on the internet also rings true for IoT systems. This stands in stark contrast to the claim of amongst others – politicians, policymakers and lawyers – that current norms go against the technical imperative of big data and IoT.[46] Those who embrace this attitude mistakenly attribute consciousness to the chips, sensors and actuators, which increasingly work in harmony by the virtue of choice of human engineers and politicians. How society is constructed cannot be attributed to technology itself, it is the result of concerted choices for which those in power can be held accountable. Choices with respect to the design of IoT systems are of fundamental importance when these systems become mandatory through legislative intervention. It means that equipping ones' environment with these systems is no longer a personal matter, it becomes state policy. Decisions on the design of obligatory IoT systems should essentially reflect the answer to the question what type of society do we want to live in and what values do we want these systems to respect.

The design of IoT systems which are mandated through the power of the EU legislature illustrates the significance of Mitch Kapor phrase that 'architecture is politics'.[47] The compulsory powers of government together with the pervasive and sentient qualities of the IoT systems imposed on everyday life have the potential to create a surveillance society which strikes at the heart of citizens' freedom. The IoT vision, therefore, demands a critical attitude towards the objectives it seeks to achieve in the respective sectors it is deployed in, the justifications for obligatory installation of these IoT systems and the design of these systems.

If architecture is politics, the question arises who decides on the design of IoT systems. In this policy the Commission sets the agenda, initiates policies, brings together stakeholders in 'fora' or 'groups' and addresses them through its communications. Before it issues a legislative proposal mandating these systems it executes an impact assessment, it can defend the standard of fundamental rights adopted in its proposal in the legislative process and it plays the role of the executive in the quasi-legislative phase, in which it negotiates with the European Standardisation Organisations (ESOs). The design of an IoT system, therefore, is the result of a policy and rulemaking process in which the European Commission plays the most prominent role. Decisions on the design of IoT systems do not take place in a legal vacuum. The Commission and legislature are bound by EU law, particularly the EU Treaties, the Charter of Fundamental Rights, general principles of EU law, as well as secondary legislation, including Directive 95/46 on processing and free movement of personal data, which was replaced by the General Data Protection Regulation (GDPR) 25 May 2018.[48] The

[45] Lawrence Lessig, *Code* (Version 2.0, Basic Books, 2006) 38.

[46] Lokke Moerel, 'Big Data Protection' (Lecture, 2014) <https://pure.uvt.nl/portal/files/2837675/oratie_Lokke_Moerel.pdf> accessed 7 June 2018, 53.

[47] Jacobs (n 14) 23.

[48] TEU, Treaty on the Functioning of the European Union (TFEU) [2012] *OJ* C326; Charter of Fundamental Rights of the European Union [2010] *OJ* C83/02; Directive 95/46/EC of the European Parliament and of the

design of IoT systems must respect EU law. This means it has to meet the requirements which follow from the right to privacy and data protection legislation, in line with the case law of the Court of Justice of the EU (CJEU). Furthermore, the decisions made on the design have to respect EU law on delegated and implementing acts.

The premise of this research is that the best way to protect citizens against the IoT systems potential for surveillance and control is to not equip them with these features in the first place. Or, alternatively, if this equipping is strictly necessary for the purpose of their installation, to make sure this potential is restricted to the absolute minimum. When an IoT system, which is obligatory by virtue of EU legislation, gives rise to an interference with the right to privacy established in Article 7 of the Charter, this interference will extend to all citizens living in EU Member States. This impact on the right to privacy necessitates compliance with Article 52 of the Charter which sets strict conditions for any limitations on the exercise of the Charter's rights and freedoms. Moreover, to the extent that it processes personal data it has to comply with EU data protection legislation: Article 8 of the Charter and the GDPR. Both similarly establish requirements, which need to be interpreted and applied in order to impose practical demands on the design of IoT systems. When the installation of IoT systems is no longer voluntary, these requirements for design offer the most effective protection of the right to privacy. Some of these requirements, such as proportionality and data minimisation have a 'prohibitive potential', which means their application can prohibit the legislature from equipping these systems with unnecessary surveillance features. Pursuing the most effective protection of the right to privacy in IoT systems design is also in line with the Commission's ambition to ensure that the Charter 'is effective in practice' or is even 'as effective as possible'.[49] The Commission, furthermore, has indicated the relevance of the standards set in European Court of Human Rights (ECtHR) and CJEU case law when examining the legality of interferences with fundamental rights.[50] It remains, however, to be seen whether this prohibitive potential of privacy and data protection legislation is realised. The protection offered by the law depends to a large extent on how the law is interpreted and applied by the Commission. The battleground over the ultimate design of IoT systems is a clash between their surveillance and control potential and the prohibitive potential of privacy laws.

Illustrative for the fundamental design choices that have to be made is the choice between centralised and decentralised storage of data. In centralised storage, detailed data is stored

---

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 [1995] OJ L281/31; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] L119.

[49] Viviane Reding, 'The importance of the EU Charter of Fundamental Rights for European legislative practice'(Lecture given at the German Institute for Human Rights, Berlin, 17 September 2010) 3; Commission, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'(Communication from the Commission) COM (2010) 573 final 3.

[50] Commission 'Report on the practical operation of the methodology for a systematic and rigorous monitoring of compliance with the Charter of fundamental rights' (Report from the Commission) COM (2009) 205 final 7.

with the system operator and the citizens using the system lose informational control over their lives. In the decentralised approach, the data is stored on the system under the control of the citizen. Through aggregation it is possible for the citizen to send the data needed for purposes such as the paying for bills, without disclosing detailed data. This way the informational power resides with the owner or holder of the system. Bart Jacobs pointed out that the information processing features of IoT systems, such as smart meters and eCall, require a fundamental choice between centralised or decentralised processing. Jacobs argues that choices between centralised and decentralised processing 'will have a deep impact on the organisation of our society and in particular on the division of (political) power', therefore, 'such architectural power issues are best discussed and decided upon within political fora, such as parliaments'.[51]

The policy and rulemaking on IoT systems takes place in three phases – the pre-legislative, the legislative and the quasi-legislative phase. The first phase concerns the earliest considerations on system design and privacy and data protection legislation, which follow from the Commission's communications. Three approximate groups of acts can be distinguished here, including communications on privacy and data protection in general, on the role of data in the future economy and on particular IoT systems. Despite their non-binding nature, the Commission's soft law documents represent an official understanding of the relevant legal norms enshrined in EU law. The Commission's interpretation, therefore, feeds into its approach in moulding and upholding norms in its various roles, including when managing, supervising and implementing IoT policy which is then imposed on relevant stakeholders. They carry the implicit authority of EU-endorsed interpretation of legal norms embodied in EU legislation. The interpretation of the Commission, therefore, holds the power to set norms in its various roles within the management, supervision and implementation of the IoT-policy and impose these on other stakeholders. Therefore its interpretation shapes relationships between data controllers (e.g. public or private providers of IoT services), ESOs and data subjects. In addition to interpreting and applying data protection law, the Commission's attitude towards privacy and data protection law can be deduced from these communications. The analysis of the latter contributes to understanding of the interpretation and application of the right to privacy by the Commission at various stages.

In the second phase, the Commission usually takes the legislative initiative. Before it issues a legislative proposal the Commission executes an impact assessment in which it is supposed to assess the likelihood and the magnitude of the impact on fundamental rights. The Commission expressed the ambition to defend the standards of fundamental rights protection adopted in the proposal in the face of amendments of the co-legislators which seek to lower

[51] Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth and others (eds), *Data Protection in a Profiled World* (Springer 2010) 291.

them.[52] The EU legislature, in turn, is also bound by the Charter and human rights as the general principles of EU law.[53]

The final piece of this process is the quasi-legislative phase. This phase concerns the relation between the legislative act on the one hand and the quasi-legislative acts on the other, namely implementing or delegated acts.[54] The ground rules for the adoption of delegated or implementing acts are provided in the legislative act. These rules, therefore, are also linked to the pre-legislative and legislative phase. The legislature may only delegate decisions to the Commission with regard to the elements of the act which are understood to be 'non-essential'.[55] This is the non-delegation doctrine which imposes one of the most important limits on the legislature's competence to delegate. The decision as to what qualifies as 'essential elements' is not solely for the legislature to decide. As established by the CJEU, these must have their basis in 'objective factors amenable to judicial review'.[56] Two important factors are whether the elements require political choices regarding conflicting interests and whether the elements of the act constitute the possibility that the 'fundamental rights of the persons concerned may be interfered with to such an extent that the involvement of the European Union legislature is required.'[57] The elements of the design of an IoT system which interfere, or can be used to interfere, with fundamental rights of citizens, should be regarded as 'essential elements of design'. Here the interpretation and application of the right to privacy and data protection legislation, again, becomes pivotal to the protection offered in this phase. If these elements of the design are not recognised as essential, they become subject to the decisions of the executive, namely the Commission. The quasi-legislative phase is further complicated by the reliance of the Commission on ESOs which develop standards in which the technical rules for the design of IoT systems are established. These ESOs act on the request of the Commission and they enjoy discretion on the parts of IoT design which are not considered essential.

An analysis of these phases will provide insight into the interpretation and application of the right to privacy and data protection legislation in the policy and rulemaking process on mandatory IoT systems and provide an answer to the question whether the surveillance and control potential of these systems is successfully curbed by virtue of the Charter and the accompanying fundamental rights ambitions of the EU.

[52] The Commission expressed the ambition to take the Charter into account after the initial proposal, as well as seeing to defending the standards contained in the proposal in the face of amendments of the co-legislators which seek to lower them. COM (2010) 573 (n 51) 8.

[53] Article 51 of the Charter.

[54] Article 290-291 TFEU.

[55] Article 290 TFEU.

[56] See Chapter 2, section 4.1. C-355/10 *Parliament v Council* ECLI:EU:C:2012:516 published in the electronic Reports of Cases (Court Reports – general).

[57] ibid, para 77. Maarten den Heijer and Eljalill Tauschinsky, 'Where Human Rights Meet Administrative Law: Essential Elements and Limits to Delegation' (2013) 9 European Constitutional Law Review 513, (note) 519.

3. Research question and outline

The recognition that the impact of an IoT system on privacy depends to a large extent on the way systems are designed is key to a meaningful discussion about how to pursue IoT policy. It lifts the veil of technological determinism and places responsibility firmly with the initiator of policy, i.e. the Commission[58], as well as the EU legislature to establish rules on the designing of these systems.

Within the research context presented above, the central question this research aims to answer is:

How does the Commission interpret and apply the right to privacy in EU policy and rulemaking with regard to the IoT, in particular mandatory systems? To which extent is this interpretation in line with the case law of the CJEU and ECtHR?

Although this question focuses on the right to privacy, data protection legislation as a derivative of the right to privacy is also analysed within this thesis given the Commission's reliance on this legislation in dealing with concerns about privacy. Reflecting the subquestions of this research, the thesis is structured as follows:

1. What is the scope of the right to private life and the home as protected by the ECHR and the Charter? What requirements have to be met to interfere with this right? (Chapter 2)
2. What is the scope of the right to the protection of personal data and what requirements have to be met to interfere with this right? (Chapter 3)
3. What is the scope of the GDPR and what requirements have to be met to comply with this Regulation? (Chapter 3)
4. What is the Commission's approach to privacy and data protection legislation that follows from its communications? (Chapter 4)
5. In which stages of the legislative and rulemaking process does the Commission interpret and apply the right to privacy in IoT policy? (Chapter 4)
6. How are the right to privacy and data protection legislation interpreted and applied in the policy and rulemaking process of smart meters and is this in line with the case law of the CJEU and ECtHR? (Chapter 5)
7. How are the right to privacy and data protection legislation interpreted and applied in the policy and rulemaking process of eCall and is this in line with the case law of the CJEU and ECtHR? (Chapter 6)

4. Methodology

The methodological approach deployed in this thesis is predominantly doctrinal legal analysis. Doctrinal analysis is the starting premise for an analysis of the legal framework applicable to the issue of human rights protection in the EU vis-à-vis emerging policies and

[58] The central actor in this book is the European Commission, since it is this institution that formulates policy, sets the agenda, adopts legislative proposals and has a big role in quasi-legislation where it negotiates with European Standardisation Organisations (ESOs) about the design of systems.

rules in the area of IoT. Within the width of the doctrinal legal research, the analysis can range from the identification, description, study of the law, to its systematic analysis or attempt to find answers to stated problems.[59] While in the past significant criticisms of the doctrinal method led to a shift towards other methodologies in legal research, increasingly of an interdisciplinary nature,[60] doctrinal research has not lost its function.[61] It is a starting point for any discussion which attempts to identify, present and understand legal norms before analysing their application or significance in any given domain. Moreover, such an analysis, as this thesis seeks to show, furnishes a powerful critique: does the legal practice of the Commission live up to its stated objectives and acknowledged normative anchors?

In this light, it is crucial to undertake a review of primary and secondary sources in order to answer the research question with its sub-questions stated above.

The doctrinal analysis of primary sources of EU law will form the foundation of this study. The TEU, the TFEU, the Charter of Fundamental Rights of the EU are analysed to clarify the legal parameters within which the IoT policy in the EU are to be deployed. The provisions of the TEU inform the discussion on the role of the human rights in the EU legal order, including the sources of human rights in the EU. The analysis of TFEU provisions relevant for data protection and the adoption of quasi-legislative acts in the EU is necessary to test the approach adopted in relation to eCalls and smart meters. In this respect, the study of the Charter of Fundamental Rights as well as the relevant general principles of EU law is of great significance.

In the area of fundamental rights, case law analysis is crucial in order to interpret the norms. Indeed, case law analysis is one of the key methods of conducting doctrinal research where the legislation itself is insufficient in guiding the process of interpretation. The case law of the ECtHR and CJEU on the right to privacy and data protection legislation is also analysed from a doctrinal perspective as it should inform the Commission's fundamental rights policy. In particular the scope of the protection offered by these rights and their possible limitations should be ascertained prior to evaluating the Commission's approach towards policy and rule-making related to IoT. It is in particular important to expose and understand the relationship between and the differences in the protection offered by the right to privacy and data protection legislation. This, in turn, is revealing when assessing the consequences of the Commission's one-sided focus on data protection legislation when dealing with IoT policy at the expense of the right to privacy.

[59] Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83.

[60] See Roger Cotterrell, 'Why Must Legal Ideas be Interpreted Sociologically?'(1998) 25 Journal of Law and Society 171, 173; Jack M Balkin, 'Interdisciplinarity as Colonization' (1996) 53 Washington and Lee Law Review 949; Douglas W Vick, 'Interdisciplinarity and the Discipline of Law' (2004) 31 Journal of Law and Society 164.

[61] Rob van Gestel and Hans W Micklitz, 'Revitalizing Doctrinal Legal Research in Europe: What about Methodology?' (2011) LAW 2011/05 EUI Working Papers.

The EU secondary legislation on data protection is also of key importance. The doctrinal method is used, thus, also to analyse Directive 95/46/EC which was a pioneering piece of legislation in the area of personal data protection, one which was not, however, suitable for the era of the IoT. The current legal regime introduced in the GDPR is also discussed to question the adequacy of this legislation in protecting the right to privacy and to reveal the parameters within which IoT systems can be legally deployed.

The doctrinal research conducted here is not confined to the analysis of primary sources. It is also supported by a review of secondary sources in the area of fundamental rights in the EU, as well as the ECHR legal regime.[62] Furthermore, secondary literature review informs the analysis of the various functions of the Commission.[63] The existing scholarship on the legal aspects of IoT systems provides the basis on which this research questions the compliance of these systems with fundamental rights norms.[64]

In addition to doctrinal legal method, discourse analysis has been relied upon in analysing the position of the European Commission towards the rights to privacy and the protection of personal data.[65] In the varying range of roles mentioned above, the Commission is a prolific actor producing discourse of its own through its communications, official statements,

[62] Bernadette Rainey, Elizabeth Wicks and Clare Ovey, *Jacobs, White & Ovey: The European Convention on Human Rights* (Oxford University Press 2010); Lee A Bygrave, 'Data protection pursuant to the right to privacy in human rights treaties' (1998) 6 International Journal of Law and Information Technology 247; Paul de Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection* (Springer 2009); Tor-Inge Harbo, 'The Function of the Proportionality Principle in EU Law' (2010) 16(2) ELJ 158; Benedikt Pirker, *Proportionality Analysis and Models of Judicial Review* (Europa Law Publishing 2013); Eva Brems and Laurens Lavrysen, '"Don't Use a Sledgehammer to Crack a Nut": Less Restrictive Means in the Case Law of the European Court of Human Rights' (2015) 15 HRLRev 139; Paul Craig, *EU Administrative Law* (Oxford University Press 2006); Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014); Herke Kranenborg, 'Article 8' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart 2014) 260.

[63] Neil Nugent, *The Government and Politics of the European Union* (6th edition, Palgrave Macmillan 2006); Paul Craig and Gráinne de Búrca, *EU Law: text, cases and materials* (5th edition, Oxford University Press 2011); Harm Schepel, *The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets* (1st edition, Hart Publishing 2005); Robert Schütze, *European Constitutional Law* (2nd edition, Cambridge University Press 2016); Christian Frankel and Erik Højberg, 'The constitution of a transnational policy field: negotiating the EU internal market for products' (2007) 14(1) Journal of European Public Policy 96; Paul Craig, 'Delegated Acts, Implementing Acts and the New Comitology Regulation' (2011) 36 ELR 673; Wim JM Voermans, Josephine Hartmann and Michael Kaeding, 'The quest for legitimacy in EU secondary legislation' (2014) 2 The Theory and Practice of Legislation 5.

[64] Ian Brown, 'Britain's smart meter programme: A case study in privacy by design' (2014) 28 International Review of Law, Computers & Technology 172; Eoghan McKenna, Ian Richardson and Murray Thomson, 'Smart meter data: Balancing consumer privacy concerns with legitimate applications' (2012) 41 Energy Policy 807; Joseph Savirimuthu, 'Smart meters and the information panopticon: beyond the rhetoric of compliance' (2013) 27 International Review of Law, Computers & Technology 161; Christophe Geuens and Jos Dumortier, 'Mandatory implementation for in-vehicle eCall: Privacy compatible' (2010) 26 Computer Law & Security Review 385; Carmela Tronsoco and others, 'PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance' (2011) 8 IEEE Transactions on Dependable and Secure Computing. Jacobs (n 46).

[65] David Howarth, *Discourse* (Open University Press 2000).

recommendations, reports and action plans. This discourse in its turn shapes the understanding of policy, feeds into legislation, quasi-legislation and sees through the implementation of the law. To understand the Commission's vision of the right to privacy, a systematic analysis of the texts it produces on the IoT is necessary.

On the basis of the study conducted through the doctrinal research and discourse analysis, the final substantive chapters of this thesis analyse the compliance of the policy and rule-making in the areas of smart meters and eCall with the primary norms of EU law. Here, to a certain extent a normative approach is also deployed, as the research also addresses the issue of what the law (as well as the quasi-legislation) 'ought to be'. Fundamental rights, indeed, are seen as one of the cornerstones for undertaking a quest into what the law 'ought to be'.[66] For this purpose, a wide range of documents forming the policy and rule-making process of the assessed mandatory IoT systems will be analysed. With this in mind, the scope of the right to private life and the home is analysed next.

[66] Jan M Smits, *The Mind and Method of the Legal Academic* (Edward Elgar 2012) 70-73.

Chapter II
The right to privacy in the EU legal order

1. Introduction

'The right to privacy consists essentially in the right to live one's own life with a minimum of interference."[1]

Article 8 ECHR has been the most important and influential provision on privacy in Europe.[2] The ECHR applies to all Council of Europe member states that have ratified it. The aim of this Convention is to secure the universal and effective protection of the rights recognised in it, whereby these rights are considered instrumental to greater unity between the members of the Council of Europe.[3] Since the early 1970s, the CJEU recognised respect for human rights as an 'integral part of the general principles of Community law'.[4] The Treaty of Amsterdam established that human rights are among the founding principles of the Union.[5] The Lisbon Treaty, in its turn, established three sources of human rights in the EU, which include general principles of law Article 6(3) TEU, the Charter which acquired legally binding force and the ECHR (upon accession to the latter).[6] The right to privacy specifically has been recognised in various decisions of the CJEU as well as in Directive 95/46/EC.[7] With the entering into force of the Charter of Fundamental Rights in 2009, privacy protection was reaffirmed in EU law through Article 7 of the Charter, which is a near copy of Article 8 ECHR.[8] Article 52(3) of the Charter provides that the meaning and scope of rights enshrined therein is the same as laid down in the ECHR for corresponding rights, although this 'provision shall not prevent Union law providing more extensive protection'. The Explanations Relating to the Charter of Fundamental Rights provide that this also includes the authorised limitations (requirements for interferences) and that the legislator therefore must comply with minimally the same standards as laid down in the ECHR.[9]

---

[1] Parliamentary Assembly of the Council of Europe, *Resolution No 428 (1970) containing a declaration on mass communication media and human rights* (Part C Article 16, 23 January 1970) <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en.> accessed 7 June 2018.

[2] Article 8 ECHR was inspired by Article 12 of the Universal Declaration of Human Rights, adopted by the General Assembly of the United Nations on 10 December 1948. One important difference between the two provisions is that Article 12 UDHR includes attacks upon honour and reputation.

[3] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 1950.

[4] Case 11/70 *Internationale Handelsgesellschaft* [1970] ECR I-1125; Case 4/73 *Nold v Commission* [1974] ECR I-491.

[5] Art 1(8), *OJ* C 340/01, 10 November 1997.

[6] Robert Schütze, *EU Constitutional Law* (2nd edition, Cambridge University Press 2016).

[7] Case C-404/92 *P X v Commission* [1994] ECR I-04737. A case started by a business: Case 136/79 *National Panasonic* [1980] ECR I-02033; Recital 10 Directive 95/46/EC.

[8] The only exception is that 'correspondence' in the latter is replaced by 'communications' in the former.

[9] Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02), 32.

The ECHR was drafted against the backdrop of fear of totalitarian societies characterised by a blurring of the private and public sphere. A specific recognition of the right to respect for private life could be viewed as an extra safeguard separating these spheres. The ECHR, furthermore, was signed in the spirit of democracy and the rule of law. The ECtHR consistently held that the 'essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities'.[10] Moreover, the Court established that personal autonomy is an important principle underlying the interpretation of its guarantees. The human rights enshrined in the ECHR can be considered the most substantive part of constitutional democracy, hence their effective protection is paramount to the very protection of society itself. The right to privacy plays a pivotal role in this respect, since it facilitates the exercise of other rights crucial to democracy, such as the freedom of expression and assembly. The Convention requires an interpretation of its provisions that 'render[s] its guarantees practical and effective'[11] :

> '[…] the rights of man in Western Europe must be not just an empty confession, but a real guardian for the individual human being against a decline which might very well set in without this protection, even though the external form of democracy is preserved.'[12]

Crucial to the effectiveness of a right, thus, is the way it is interpreted and applied. This is equally true with respect to the design of IoT systems in the context of legislation mandating their installation. The EU legislation which introduces mandatory IoT systems has to meet the requirements which follow from the Charter and ECHR. The Commission plays a prominent role in the preparation and proposing of legislation. Here, the Commission's function to oversee the correct application of EU law is of crucial importance for the effective protection of the right to privacy.

The Commission's exercise of its tasks is overseen by the CJEU. The ultimate interpretative authority therefore lies with the CJEU, which in turn relies to a great extent on the case law of the ECtHR.[13] The standards developed in the case law of these two courts is also deemed relevant by the Commission for aligning the impact assessment with the standards of proportionality and necessity, so that the assessment can 'provide analyses for the later legal control'.14 In order to understand how the right to privacy should inform the Commission's actions throughout the policy and the legislative process introducing mandatory IoT systems, it is necessary to test this introduction against the right to privacy as developed in the relevant case law of both courts. The focus will be on case law regarding private life and the home.

---

[10] *Von Hannover v Germany (No 2)* App nos 20660/08 and 60641/08, (ECtHR, 7 February 2012) para 98.

[11] *Sabanchiyeva and Others v Russia* App no 38450/05 (ECtHR, 6 June 2013) para 132.

[12] Arthur H Robertson, *Collected edition of the 'travaux préparatoires' of the European Convention on Human Rights = Recueil des travaux préparatoires de la Convention Européenne des Droits de l'Homme* (Vol 1, Preparatory Commission of the Council of Europe Committee of Ministers, Consultative Assembly, 11 May-8 September 1949, The Hague, Nijhoff 1975) 66.

[13] The CJEU is held to do this on the bases of Article 52(3) of the Charter. The CJEU and ECtHR also refer to each other's case law.

[14] Commission, '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 7.

2. The scope of the right to private life and the home

IoT systems and their envisioned environment raise numerous issues with respect to the right to private life and the home. The systems discussed here are not installed covertly — their presence is known. Their installation is not targeted, but mandatory for the entire population. They process personal data; some offer or facilitate remote control over the aspects controlled by the system or the sensors it is equipped with; they are and can be used for surveillance purposes (including secret ones), whether these are private, public or hybrid in nature. Judicial considerations regarding the scope of the right to private life and additionally the right to respect for the home are, hence, relevant. Moreover, the repurposing of data acquired in one context for another has attracted significant attention of the ECtHR. Case law regarding data protection is used to gain insight into the factors relevant to the question if and to what extent the processing of personal data constitutes an interference with the right to private life. Through the principles of evolutive interpretation and effective and practical rights, the ECtHR has continuously adapted the right to private life to societal and technological changes.[15] The principle of evolutive interpretation implies that the ECHR is a living instrument and the rights therein should be interpreted in light of present-day conditions.[16] This principle has to respect the text, context, object and purpose of the ECHR, but allows taking into account changing material conditions (e.g. the introduction of the Internet) and changing moral conditions. In accordance with the aim of the Convention, 'the maintenance and further realisation of Human Rights and Fundamental Freedoms', this principle should serve the levelling up of human rights. In the light of the special character of the Convention as a treaty for the collective enforcement of human rights and fundamental freedoms, the Court has held that 'the object and purpose of the Convention as an instrument for the protection of individual human beings require that its provisions be interpreted and applied so as to make its safeguards practical and effective'.[17] The principle of practical and effective rights was not a novel invention in the ECtHR case law, but is a widely recognised principle of treaty interpretation.[18] Together these principles can prove helpful in interpreting and applying the rights enshrined in Article 8 ECtHR in relation to EU legislation mandating the installation of IoT systems.

Understanding the scope of the right to private life and the home is important in order to establish the *severity of the interference.* The courts have to find the interference sufficiently severe before judging upon the merits of the justification. Determining the scope of these rights is also important for establishing the requirements that need to be met to justify the interference.

[15] *Hatton and others v The United Kingdom* App no 36022/97 (ECtHR, 8 July 2003). Alastair Mowbray, 'The Creativity of the European Court of Human Rights' [2005] HRLRev 5:1, 57, 79.
[16] *Tyrer v UK* App no 5856/72 (ECtHR, 25 April 1978) para 31.
[17] *Soering v The United Kingdom* App no 14038/88 (ECtHR, 7 July 1989) para 87.
[18] Hanneke Senden, *Interpretation of Fundamental Rights in a Multilevel Legal System* (Intersentia 2011) 73.

2.1 The right to private life

The right to private life was not common to constitutions in Europe before WWII, other than in some specific forms, such as the inviolability of the home and confidentiality of the mail.[19] These latter forms sought to establish certain domains free from government intervention in principle. The right to privacy as such was only recognised with the adoption of the Universal Declaration of Human Rights in 1948,[20] and two years later, in Europe, with the ECHR. Throughout the drafting history of the Convention, two umbrella terms competed for a place in Article 8, namely 'privacy' and 'private life', of which the latter prevailed. The right to private life provides a sphere to the individual, beyond the home and the envelope, in which he is protected against arbitrary interference, particularly from public authorities. In this sense, the right to private life can be seen as a substrate of the idea of the division of the public and private sphere rooted in the classical liberal tradition.[21]

The ECtHR decided that the term private life is '*not susceptible to exhaustive definition'* and this right has branched out, covering a great variety of interests ranging from identity, relationships, physical and informational self-determination, surveillance and more.[22] The right to private life has stretched beyond a restricted interpretation of what comprises the private sphere and 'the inner circle', extending to places outside the home[23] and finding articulation in the right to establish and develop relationships with other people as well as the outside world.[24] At the time of signing the ECHR, the term 'informational privacy' was inexistent. It was only coined in 1967 by Westin as the right to determine when, how and to what extent information about oneself could be communicated to others.[25] It can be argued, nevertheless, that the threat to informational privacy was the impetus for Warren and Brandeis to publish the seminal article 'The Right to Privacy' in the Harvard Law Review in 1890. It was the combination of free press and snapshot-photography that lowered the threshold for others to invade 'the sacred precincts of private and domestic life' and facilitate informational access against the will of those subjected to public scrutiny.[26] The vast majority of privacy breaches can be formulated in terms of 'the communication of information'. In 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of personal data was adopted by the Council of Europe (hereinafter 'Convention 108'), which the ECtHR started to refer to in its case law since 1993 viewing it as relevant international

[19] Oliver Diggelmann and Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right' [2014] HRLRev 441.
[20] ibid.
[21] Peter H Blok, *Het recht op privacy* (Boom Juridische uitgevers, 2002) 11.
[22] *Peck v The United Kingdom* App no 44647/98 (ECtHR, 28 January 2003) para 57.
[23] ibid.
[24] *Niemietz v Germany* App no 13710/88 (ECtHR, 16 December 1992) para 29; *Bensaid v The United Kingdom* App no 44599/98 (ECtHR, 6 February 2001) para 47. *Von Hannover* (n 10) para 95.
[25] Alan F Westin, 'Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part II, Balancing the Conflicting demands of Privacy, Disclosure and Surveillance' (1966) 66 Columbia Law Review 1205.
[26] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy', (1890) 4 Harv L Rev 193.

law.[27] The ECtHR holds that the protection of personal data is of 'fundamental importance' to the enjoyment of the right to respect for private and family life.[28] The object protected is the collection, storage and use of data that fall under the right to private life. Despite the fact that the Court deems the protection of personal data vital to the enjoyment of the right to respect for private life, it does not extend the protection of Article 8 ECHR to the processing of any personal data. This signifies a difference with EU data protection legislation, which, in principle, does apply to any processing of personal data.

The two subcategories of private life most relevant for the IoT are the right to be free from unwanted informational access (the collection, storage and use of personal information) and surveillance.[29] These two subcategories have a complex relationship and cannot be viewed in isolation. A joint analysis is merited in which the focus is on, but not limited to, the processing of personal data. The question whether the processing of personal data amounts to an interference with the right to private life, as well as the severity of this interference, depends mainly upon a number of factors: the *context of the processing*, the *nature of the data* and the *potential future violations*.[30] The last factor can be applied to interferences which do not involve the processing of personal data.

The context of the processing

The context of the processing is the most important factor when deciding whether processing of personal data interferes with the right to private life. The ECtHR assesses *inter alia* the transparency of the processing (if the person concerned was informed about the processing),[31] the status and the number of people affected by a measure entailing the processing of personal data, the relationship in which the processing takes place, the parties that process the data, whether the person whose data it concerns consented to the processing, the location where data is recorded (in a person's home as opposed to a prison cell), the purpose(s) for which the data are used, whether the data collected was minimised to what was relevant,[32] the

[27] *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997) para 95; *Gardel v France* App no 16428/05 (ECtHR, 17 December 2009) para 27.
[28] *Z v Finland* (n 27) para 95.
[29] Other subcategories that follow from the right to private life are left out of this chapter, because they bear no relevance to my research.
[30] I draw from the work of Bygrave with respect to the first two distinctions. Bygrave denotes the most important factors that determine whether the processing of personal data interfere with the right to private life (based on the case law of the ECtHR), which are also relevant to determine the extent to which they interfere: '(i) the nature of the data in question (e.g., to what extent do the data concern 'private life'?); (ii) the manner in which the data are processed (e.g., are they processed with the knowledge or consent of the data subject?) (iii) the context for the data processing (e.g., are the data found in a register that allows potentially negative assessments to be made of the data subject's character).' I will examine these categories, although I include the manner in which the data are processed alongside the context for data processing into one category: *the context of processing.* Lee A Bygrave, 'Data protection pursuant to the right to privacy' (1998) 6(3) International Journal of Law and Information Technology 247, 269.
[31] *LH v Latvia* App no 52019/07 (ECtHR, 29 April 2014) para 51.
[32] ibid, para 59.

indiscriminate nature of the retention,[33] whether the data is used for additional purposes and how these relate with the original purposes, the possible adverse consequences of this processing for the person concerned, the reasonable expectation of privacy of this person, the potential future violations of privacy the data or system recording it facilitates (this will be further discussed in the last subsection) and the scope of the processing.[34] A number of these aspects correspond to the rules laid down in Convention 108.

The scope of the processing can also have an influence on the nature of the data. The ECtHR held that there is a proportional relationship between the scope of a recording system and the amount and sensitivity of the data held.[35] This reasoning connects the *nature* of data to the *context of the processing*. The densification of personal data through the continuous interlinking and automation of databases and information networks implies that it is increasingly unlikely that processing of personal data does not raise an issue under the right to private life.[36] A parallel can be drawn with cases concerning interferences with the right to respect for the home that consist of environmental nuisances, in which the interference needs to attain a *minimum level of severity* in order to raise an issue under Article 8 ECHR.[37] Again, the point of reaching the minimum level is highly dependent on the context. A general criterion the Court uses is that the infringement needs to reach the level where the applicant is affected seriously or which impinges upon the enjoyment of the home. In a similar fashion, it can be argued that a *minimum level of severity* can be established when the processing of personal data frustrates the enjoyment of private (and possibly family) life, for which the Court deems the protection of personal data of fundamental importance.[38] The severity of the interference in turn has consequences for the requirements that need to be met to justify it.

Some of these aspects feature in situations where data is processed originally within a relationship between citizens and businesses. The Court held on several occasions that the retention of data performed in such contractual relationship does not automatically raise an issue under Article 8 ECHR. This can change when that data is used subsequently beyond the context of this relationship. In the history of ECtHR case law, there have been a few examples of using data beyond the original context. Consent, the reasonable expectation of privacy and the relationship between the party processing the data and the person whose data it concerned were also relevant aspects in these cases. In 1984, the Court held in *Malone v. The UK* that a supplier of a telephone service may, in principle, obtain metering records legitimately, with the purpose to ensure correct billing; or to investigate possible abuses of

[33] *S and Marper v The United Kingdom* App nos 30562 and 30566/04 (ECtHR, 4 December 2008).
[34] *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010).
[35] *MM v The United Kingdom* App no 24029/07 (ECtHR, 13 November 2012) para 200. It should be noted that this was in the case of a recording system for felonies and cautions, nevertheless it makes sense that this is also relevant for more trivial data. The more data there is, the more comprehensive information can be inferred from it. The Court deemed this important for the safeguards to be applied in the various stages of the subsequent processing, see section 3.1.
[36] Bart W Schermer, 'The limits of privacy in automated profiling and data mining' (2011) 27(1) Computer Law & Security Review 45, 50.
[37] *López Ostra v Spain* App no 16798/90 (ECtHR, 9 December 1994).
[38] *S and Marper* (n 33) para 103.

the service.[39] The supplier used 'a device called a meter check printer which registers the numbers dialled on a particular telephone and the time and duration of each call'.[40] The Court agreed with the UK Government that the supplier, the Home and Postal office, in principle did not interfere with the right to private life when it registered this information for legitimate purposes such as billing and fighting fraud. This shows that a systematic or permanent record is not enough for the Court to reach the conclusion that the right to private life has been violated. The Court, however, disagreed with the Government's contention that the use of this data, whatever the circumstances and purposes, could not give rise to an issue under Article 8 ECHR. The Court decided that the release of 'metering data', more commonly referred to as 'billing data', without the consent of the subscriber amounted to an interference with a right under Article 8 ECHR. This shows that certain data processing activities do not raise an issue under Article 8 ECHR, yet non-consensual processing of personal data beyond the original context does. It also shows that processing certain data raises a risk of privacy breaches at a later stage. If the billing data only consisted of the total amount of money that Malone had to pay, without exposing the more detailed information it did, then this data would have not been of interest to the police. Depending on the design of an IoT system, its installation can cause or facilitate non-consensual processing of personal data.

A comparable case is *Copland v. The UK.*[41] The applicant was an employee of Carmarthenshire College and worked closely with the Deputy Principal. All data concerning College employees' telephone, e-mail and internet usage was automatically generated, only the applicant's data were further analysed at the Deputy Principal's instigation.[42] Originally, the data collection was not for the purpose of surveillance, yet it was used for this purpose at a later stage. An interesting distinction from *Malone* was the fact that the data was not released to another party, it was not even specifically requested; it was automatically generated and thus available to the College. The Court held here that the storing of this personal data fell under the scope of Article 8(1) ECHR and found an interference with the right to private life.[43] The absence of warning that calls could be monitored was seen as relevant, though not conclusive, in determining the scope of her right to private life, leading to a conclusion that she had a *reasonable expectation as to the privacy* of her calls, e-mail and Internet usage.[44]

Sometimes, the context of the processing is related to the nature of the data. Gutwirth and De Hert demonstrate that the Court makes a distinction between 'personal data that fall within the scope of Article 8 ECHR and personal data that do not', 'data that merits protection' and 'data that does not', or 'processing of personal data that affects private life and processing of

[39] *Malone v The United Kingdom* App no 8691/79 (ECtHR, 2 August 1984) para 84.
[40] ibid, para 21.
[41] *Copland v The United Kingdom* App no 62617/00 (ECHR, 3 April 2007).
[42] ibid, para 32.
[43] ibid, para 43.
[44] ibid, para 42. A case where the person was warned led to the opposite outcome, see *Bărbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017).

personal data that does not'.[45] The case used by Gutwirth and De Hert to support the above argument is *Pierre Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium*, declared inadmissible by the European Commission of Human Rights.[46] In this case, the European Commission of Human Rights considered that the use of photographic equipment deployed by public authorities or private individuals in public spaces or premises owned by them did not interfere with the right to private life of the applicant. Crucial was the fact that the equipment did not record the visual data and the subsequent impossibility to make it available to the public or use it for other purposes than monitoring these spaces. The mere filming of a public scene is not considered to give rise to a violation under Article 8 ECHR, since any member of the public can view this event. The Court, however, held that if this scene is monitored through technological means 'private-life considerations may arise … once any systematic or permanent record comes into existence of such material from the public domain'.[47] In *Friedl,*[48] the European Commission of Human Rights found that photographs taken of a group of demonstrators by the police did not fall under the right to private life and specifically attached weight to the, albeit disputable,[49] circumstance that no further action was taken by the police to identify them.[50] Again, it was not the *nature of data* that proved decisive for the European Commission of Human Rights, but *the context of processing* or more specifically for this case, the assumed lack of processing. Both cases demonstrate that the decisive criterion in determining whether an interference of Article 8 ECHR has taken place is not the *nature* of data, but *the context of processing*.

In *Amann* the ECtHR held the *nature of data* as irrelevant to the question whether an interference had taken place.[51] The Court decided that the storage and release of personal information in a secret police file, or on a card by public authorities, constituted an interference with the right to respect for private life, irrespective of the question whether the data were sensitive, or whether the applicant was inconvenienced in any way.[52] This line of reasoning has been explicitly adopted by the CJEU, which extended the protection to the

[45] These are the quotation marks from the original chapter: Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection* (Springer 2009) 24-26. Raphaël Gellert and Serge Gutwirth, *Beyond accountability, the return to privacy* (Palgrave Macmillan 2012) 9.

[46] *Pierre Herbecq and the Association 'Ligue des droits de l'homme' v Belgium* App nos 32200/96 and 32201/96 (Commission Decision, 14 January 1998).

[47] *PG and JH v The United Kingdom* App no 44787/98 (ECtHR, 25 September 2001) para 57.

[48] *Friedl v Austria (*1996) 21 EHRR 83 (Commission Decision).

[49] Upon closer reading of the case this fact seems highly disputable, since their identities had already been taken down in the streets, before being photographed at the station (para 7). Furthermore, the police themselves indicated that the photographs were taken for possible prosecution (para 8).

[50] Orla Lynskey, 'Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order' (2014) 63(3) ICLQ 569, 584.

[51] *Amann v Switzerland* App no 27798/95 (ECtHR, 16 February 2000).

[52] Respectively *Leander v Sweden* App no 9248/81 (ECtHR, 26 March 1987) para 48 and *Amann v Switzerland* (n 51) para 70.

communication of salaries to a public authority.[53] These cases necessitate the conclusion that the courts do not exclude any kind of data *a priori* and that the context of the processing is the primary criterion. The recording, collection and storage of data can fall under the scope of the right to private life depending on the context. The nature of data is only of secondary importance.

Nature of data

Convention 108 already recognised a division between sensitive and non-sensitive data, which was also reaffirmed in EU data protection legislation. Amongst the 'special categories of data' ranking under Article 6 Convention 108 are data revealing racial origin, political opinions, religious or other beliefs, data concerning health or sexual life and relating to criminal convictions. The GDPR added to this ethnical origin, trade union membership, genetic and biometric data for the unique identification of a natural person.[54] The ECtHR makes distinctions on the *nature* of data and holds that some are more sensitive than others.[55] It has accorded a special status to medical data and held its protection crucial to preserving confidence in the medical profession and health services.[56] According to the ECtHR, the respect for the confidentiality of medical data is 'a vital principle in the legal systems' of the signatories of the Convention.[57] It has made a further distinction with regard to data concerning a person's HIV-status which it considered to be particularly sensitive.[58]

The nature of data is also a criterion employed in the area of surveillance. Visual and acoustic surveillance measures are distinguished by the Strasbourg Court from other surveillance measures, such as data collected through metering or GPS. According to the Court, the nature of visual and/or acoustical surveillance is more likely to interfere with the right to respect for private life, which is more inclined to reveal information about conduct, opinions and feelings.[59] The ECtHR made this distinction between GPS and methods of acoustical or visual surveillance in *Uzun*, claiming the latter two are more susceptible to infringe a person's privacy. Although the *type of data* can provide an indication of the severity of a breach, it is not decisive for the *nature of the information* extracted from it. For instance, a

[53] Joined cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-04989, para 75. This case is also interesting because theCJEU reads Article 7 and 8 of the Charter in conjunction and formulates 'the right to respect for private life with regard to the processing of personal data'.

[54] Article 9 GDPR.

[55] *S. and Marper* (n 33) paras 75 and 78, the already mentioned distinction between DNA and fingerprints, the Court held that a HIV-infection is of a highly intimate and sensitive nature.

[56] *Z v Finland* (n 27) para 95.

[57] *LH v Latvia* (n 31) para 56. The Court referred to the ECHR.

[58] *Z v Finland* (n 27) para 96.

[59] *Uzun v Germany* (n 34) paras 52, 65, 66.

person's habit of visiting prostitutes might be less easy to extract from the content of their communications than from their location data.[60]

The CJEU originally followed the ECtHR in this distinction. In *Digital Rights Ireland*, it held that metadata 'does not permit the acquisition of knowledge of the content of the electronic communications as such', leading to the conclusion that the interference constituted by their retention did not 'adversely affect the essence of those rights' under Article 7 of the Charter.[61] This paved the way for its judgment in *Schrems*, where the CJEU held that the US legislation 'permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter'.[62] Although the CJEU's argument includes the nature of the data (content), the main distinction between *Digital Rights Ireland* and *Schrems* is that the US legislation allowed *access on a generalised basis*, i.e. the context of the processing. It is the access on a generalised basis, which, according to the CJEU, hampers the essence of the right to private life. This is also in line with the much recited mantra of the ECtHR that the essential object of the right to private life is to protect the individual against arbitrary interferences by public authorities. It is not the nature of the data that determines whether the essence of the right to private life is at stake, but whether this data is processed (recorded, collected, accessed and used) in an arbitrary fashion.

In a recent case of *Tele2 Sverige*, the CJEU, following the position of AG Saugmandsgaard, held that metadata are 'no less sensitive, having regard to the right to privacy, than the actual content of communications'.[63] AG Saugmandsgaard even argued that metadata allows:

> '(t)o identify individuals opposed to the policies of the incumbent government. Again, analysing the content of communications would require considerable resources, whereas, by using communications data it would be possible to identify all individuals on the distribution list of emails criticising government policy….the risks associated with access to communications data (or 'metadata') may be as great or even greater than those arising from access to communications … 'metadata' facilitate the almost instantaneous cataloguing of entire populations, something which the content of communications does not.'[64]

An extra dimension on the nature of the data transpires in this passage. It does not focus on *the type* (audio, visual, numerical, text etc.), but on *the format* of data, which the AG links to the question of how it *facilitates further processing*. The AG views the ease with which

[60] Other authors also disagree with this distinction, see Paul de Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in David Wright and Paul de Hert (eds), *Privacy Impact Assessment* (Part of the Law, Governance and Technology Series vol 6, Springer 2012) 60. Daniel Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press 2011) 158-159. Solove points out that IP addresses can reveal very intimate information about a person.

[61] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] OJ C175/6, paras 54 and 39.

[62] Case C-362/14 *Schrems* EU:C:2015:650, para 94.

[63] Joined cases C-203/15 and C-698/15 *Tele2 Sverige* EU:C:2016:970, para 99.

[64] Joined cases C-203/15 and C-698/15 *Tele2 Sverige* EU:C:2016:970, Opinion of AG Saugmansgaard, paras 258-259.

metadata can be used to catalogue an entire population as relevant to the severity and the magnitude of the interference it facilitates. In its judgment, the CJEU adopted a similar line of reasoning concluding that the retention of metadata allowed the establishment of profiles of individuals, producing information as sensitive as the content of communications.[65] Through this recognition, the CJEU implicitly acknowledged that the nature of the information which can be inferred from data is a relevant factor. In conclusion, the CJEU recognised and acknowledged a new dimension of the nature of data, which might in turn inspire the ECtHR.

The susceptibility of data to infringe on a person's privacy, thus, requires attention for the type of data, the format of the data and the *nature of the information* that can be inferred from it.

Potential future violations[66]

The ECtHR makes another interesting distinction based on the envisioned use of data in the future. It held that DNA and cellular samples, compared to fingerprints, hold 'stronger potential for future use' and that the question of interference, thus, should be examined separately.[67] This factor bears resemblance to the *surveillance and control potential* of IoT systems. The ECtHR established in *Marper* that individual concern about the way certain data might be used in view of the rapid pace of technological developments can be 'legitimate and relevant to a determination of the issue of whether there has been an interference'.[68] Although this concerned information technology and genetics, there is no reason why *potential future violations* would be limited to a combination of these categories. Moreover, whilst this judgment concerned the use of *data* by public authorities, the same considerations can apply to the assessment of *systems* or *particular aspects of systems* that can potentially be used for purposes of surveillance. The CJEU has taken *potential future violations* of fundamental rights into account when assessing the legality of an injunction of a filtering system that would enable the monitoring of online communications.[69] An evolutive interpretation, respecting the principle of effectiveness and practical rights, necessitates a critical assessment of potential future privacy violations facilitated by mandatory IoT systems in tomorrow's networked society. Alternatively, the effective protection of the right to private life could be slowly undermined by erecting an information society in which it is impossible for citizens to live without constantly being monitored.

The installation of IoT systems can result in overt surveillance performed by the parties responsible for the roll-out (either private or public), at least as far as citizens are properly informed. The same systems can be used for covert surveillance purposes. There are already

[65] *Tele2 Sverige* (n 63) para 101.
[66] This subsection draws from this article: Tijmen HA Wisman, 'eCall and the Quest for Effective Protection of the Right to Privacy' (2016) 2 European Data Protection Law Review 59.
[67] *S and Marper* (n 33) para 69.
[68] ibid, para 71.
[69] C-70/10 *Scarlet Extended* [2011] ECR I-11959, para 52.

practices in which the law effectively facilitates the use of data generated by IoT systems in large profiling practices of the state, such as the System Risk Indication in the Netherlands.[70] In addition, a communication from the Commission on a European cloud that can be used for big data mining operations, exposes the will to use certain types of data obtained through the deployment of IoT systems for public purposes.[71] This envisioned secondary use implies a collective concern about the mass-interference with the right to private life raised by the perspective of mandatory installation of these systems. In its case law, the ECtHR and CJEU view the further processing of personal data by public authorities to be an interference with the right to private life.[72]

The above also reveals an interesting quantum-feature in IoT systems or the *surveillance and control potential*: it is uncertain whether these systems will be used to perform surveillance-functions. This potential is of vital importance to the impact assessment, the legal basis on which they should be adopted, the essential elements that the legislative act should contain, the legal safeguards which should be adopted in the legislative act and prior to this the very question whether or not their mandatory installation can be justified in the first place. Even if all legal procedural requirements were met, the adoption of legislation forcing the installation of IoT systems with intrusive potential would amount to the mandatory roll-out of surveillance equipment which would affect virtually all EU citizens. When the impact assessment exposes the presence of this potential, the Commission should also assess whether this potential can be negated by laying down requirements rendering it impossible for this system to perform this function. These requirements concern essential elements which should be adopted in the legislative act, because they are the preserve of the EU legislature.[73]

The importance of the above can be illustrated by the hypothetical case where a Member State would exploit the vulnerabilities in the design of an IoT system to place citizens under surveillance. The question that would then arise is whether EU law (the Charter and data protection legislation) offers protection to these citizens. Recent case law indicates a negative answer to this question. In *Willems* 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 the 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:

[70] Article 62 -65 Wet structuur uitvoeringsorganisatie werk en inkomen, Staatsblad 2013, 405.

[71] Commission, 'Towards a thriving data-driven economy' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2014) 442 final.

[72] *Malone v The United Kingdom* (n 39); *Copland v The United Kingdom*(n 41); *Digital Rights Ireland* (n 61); *Schrems* (n 62).

[73] Chapter 4, section 4.1.

> '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.'[74]

At the core of this question was whether EU legislation prevented the repurposing of collected biometric data on the basis of EU law.[75] These new purposes consisted of the identification of victims of disasters and accidents, the detection and prosecution of criminal offences, and the conduct of investigations of acts constituting a threat to state security. The CJEU decided that the EU legislation was not applicable because the stated purposes were matters of national interest. The Court failed to pay attention to such considerations as the collection of the data on the basis of an EU Regulation and the existence of CoE Convention 108 regulating the use of data. It also failed to note that the use for these new purposes went against the original purpose specified, thereby rendering compliance with the right to data protection largely meaningless. The CJEU declared data protection legislation and the CFEU inapplicable in the face of Member States' reliance on EU legislation to expand their surveillance apparatus under a pretext of national security.

The application of this, arguably flawed,[76] logic to the repurposing of IoT systems for national interests such as fighting crime, terrorism or even tax fraud would make it clear that the fundamental rights protection by the EU leaves the citizens of Member States empty handed against *potential future violations* facilitated by EU introduced IoT systems. Even when the EU legislature lays down obligations to process personal data only for the handling of emergencies, once national legislation establishes a national interest purpose, these 'obligations' become obsolete. In practice, this means that the safeguards which legitimise the adoption of legislation on EU level, can later be discarded at national level. *Willems* shows that once the EU legislation mandating the installation of IoT systems with surveillance features is in place, these features are practically immune to the regime of fundamental rights protection in the EU. This normative gap allows for 'deliberate state misappropriation of systems introduced under EU law for domestic surveillance purposes'.[77] This underlines the fact that a carefully executed Commission impact assessment seeking to prevent the adoption of these features in IoT systems is the only effective remedy against overzealous Member States seeking to utilise their surveillance and control potential.

---

[74] Joined Cases C-446/12 to C-449/12 *Willems* EU:C:2015:238, para 43.

[75] A salient detail is that the central storage of this biometric data itself already constituted an interference with the right to private life that went beyond what was strictly necessary for the purpose of the collection, which was the prevention of lookalike fraud. This purpose can also be obtained by storing the biometric data on the passport or travel document itself, instead of storing it on a central server, which places the biometric data outside the control of the holder of the document without a legitimate reason.

[76] See Steve Peers, 'Biometric data and data protection law: the CJEU loses the plot' (*EU Law Analysis*, 17 April 2015) <http://eulawanalysis.blogspot.se/2015/04/biometric-data-and-data-protection-law.html> accessed 7 August 2015; Tijmen HA Wisman, 'Giving Member States the Prints and Data Protection the Finger' (2015) 3 EDPL 245.

[77] This is a quote from the comments of Andrew Murray on this paragraph.

Just as legislation might pose a menace of surveillance, the existence of administrative practices in which a variety of data sets are combined in order to create profiles of *risk citizens*, also poses a menace of surveillance. This becomes particularly acute if the installation of IoT systems in the private surroundings of citizens can lead to the collection of information related to a person or a family's indoor activities, which are subsequently accessible by third parties.

2.2 The home

In most Western societies, the right to inviolability of the home has a long history of constitutional protection. The home is the designated place where people ought to be free from interference and can develop their own views of life, practice their own religion and share their own thoughts without having to fear possible adverse consequences in the future. This freedom is essential in a constitutional democracy, since it provides space in which the citizen can develop moral autonomy, a central requirement of democracy.[78] 'The home', albeit in one version 'the house',[79] was present in all drafts of the Convention, which shows the widespread consensus in Europe on the importance of this category.

The right to respect for the home is deemed an essential right for citizens in a free society and the ECtHR considers it 'pertinent to their own personal security and well-being'.[80] The classic breach of this right is when government officials gain physical entry to the home. Although the right to property was, after many discussions in the Consultative Assembly, intentionally left out of Article 8 ECHR, it found its way back through the case law of the Court, that is to say that property rights regarding the home are protected to the extent that they overlap with the protection offered by Article 8 ECHR. The ECtHR has held that 'the loss of one's home is the most extreme form of interference with the right to respect for the home'.[81]

There is an extensive body of case law which recognises that the scope of the right to respect for the home covers the physical area as well as the quiet enjoyment thereof.[82] This implies that infringements of this right are not limited to physical breaches, but also extend to non-physical phenomena like pollution, noise, smells, etc. The Court deems these phenomena to be detrimental to the 'quality of the private life' and 'the scope for enjoying the amenities of the home'.[83] Although there is not a right to a clean and quiet environment formulated as such, the Court acknowledges that these conditions are important for the enjoyment of the home. There is, as formerly discussed, a *minimum level of severity*, which needs to be

[78] Ruth E Gavison, 'Privacy and the Limits of Law' (1980) 89(3) YaleLG 421, 455.
[79] Diggelmann and Cleis (n 19) 16.
[80] *Gillow v The United Kingdom* App no 9063/80 (ECtHR, 24 November 1986) para 55.
[81] *Buckland v The United Kingdom* App no 40060/08 (ECtHR, 18 September 2012) para 65.
[82] *Moreno Gómez v Spain* App no 4143/02 (ECtHR, 16 November 2004) para 53.
[83] *Powell and Rayner v The United Kingdom* App no 9310/81 (ECtHR, 21 February 1990) para 40.

attained in order to raise an issue under Article 8 ECHR.[84] The breach has to be serious enough, for which evidence can be produced by inter alia expert reports (e.g. doctors for health-issues or professors in applied physics for noise).

On the one hand, the collection of data or possibilities for remote shutting on or off certain IoT systems does not compare to government official gaining physical entry to a house and search it. On the other hand, public authorities knocking on the door would be more indicative of their intentions in contrast to the seamless way these parties can search the lives of citizens through these networked systems. Furthermore, the installation of an IoT system is permanent, the data it may collect might be highly detailed and the information that can be inferred from it can be sensitive and have highly adverse consequences for the person or family concerned. Therefore, the security and well-being of the person in the home can be adversely affected by an IoT system and protection against this falls under the scope of the right to respect for the home.

This right protects against measures and regulation by the government, e.g. regulation that allows air traffic that causes noise pollution violating the right to respect for the home.[85] It can also have a horizontal effect against a commercial enterprise in the direct proximity of the house that causes environmental pollution, nuisance or health problems.[86] When the right to respect for the home is invoked against other individuals or corporations, the interference is attributed to the failure of public authorities to take action to end third-party breaches, the so-called positive obligations addressed in the next section.[87]

2.3 Positive obligation to protect rights in Article 8 ECHR

Adding to the complexity of the ECtHR's case law, but also to the protection offered by Article 8 ECHR, is the distinction between positive and negative obligations:

> 'while the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this negative undertaking, there may be positive obligations inherent in an effective respect for the rights enshrined in the Convention. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.'[88]

In other words, in finding a positive obligation the Court does not hold an activity of the state to violate a Convention right; it is rather the inaction which constitutes the violation. Since there is no consensus among the Contracting States about what 'respect' entails, states have a wide margin of appreciation in deciding what is required from the state to respect the right

[84] *Lars and Astrid Fägerskiöld v Sweden* App no 37664/04 (ECtHR, 26 February 2008).
[85] *Hatton and others* (n 15).
[86] *López Ostra v Spain* (n 37).
[87] *Moreno Gómez v Spain* (n 82) para 57.
[88] *Van Kück v Germany* App no 35968/97 (ECtHR, 12 September 2003) para 70.

concerned in the application.[89] The complexity of this issue lies in determining when a state oversteps the margin of appreciation.

The Courts review is divided into two stages. First, the Court will assess if the grounds invoked by the state to justify its inaction are relevant. The second part is more substantial and involves the assessment of the 'appropriateness of the state's attitude'.[90] The outcome of this assessment is highly dependent upon the severity of the interference with the right to private life or the home, against which the applicant did not enjoy effective protection from the state. The Court seeks to strike a fair balance between the competing right to private life and the opposing interests, whether these are public (e.g. the interests of the community) or private (e.g. the interests of the employer).

The Court has formulated a non-exhaustive list of positive obligations that concern the right of transsexuals to have their sexual identity corrected (or 'gender reassignment' as the Court eloquently phrases this), the obligation for a state to provide an effective remedy against criminal acts committed on the internet causing great dangers for minors' physical and moral welfare, access to personal information that relates to 'private and family life' kept by public authorities and protection from pollution and other environmental nuisances.[91]

Positive obligations may consist of legal rules, but can also entail practical measures. The failure of the state can thus lie in its omission to take either legal or practical measures, where one can subsume the other.[92] Positive obligations may be either *procedural* or *substantive*. Procedural obligations see to the requirement of efficient remedies, e.g. access to a domestic court. Substantive obligations see to 'the basic measures needed for full employment of the rights guaranteed'.[93] The notion of these basic measures corresponds to the notion *of the essential elements of design* of an IoT system and can provide another legal basis for the duty for the EU legislature to impose these.[94] The concept of positive obligations in the case law of the ECtHR provides further support to demand a pro-active approach from the Commission towards incorporating the right to privacy in the design of IoT systems. The Court held that the positive obligation must not impose an impossible or disproportionate burden on state authorities or legislators.[95] The Court, however, is not easily convinced that this burden is indeed disproportionate.[96]

[89] Ursula Kilkelly, *The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention of Human Rights* (Human Rights Handbook, No. 1, Council of Europe 2003).
[90] ibid.
[91] *Christine Goodwin v The United Kingdom* App no 28957/95 (ECtHR, 11 July 2002); *KU v Finland* App no 2872/02 (ECtHR, 2 December 2008); *Gaskin v The United Kingdom* App no 10454/83 (ECtHR, 7 July 1989); *López Ostra v Spain* (n 37).
[92] Kilkelly (n 89) 7.
[93] Kilkelly (n 89) 16.
[94] For a discussion on *essential elements of design* see Chapter 4, section 4.1.
[95] *KU v Finland* (n 91) para 48.
[96] *Christine Goodwin v The United Kingdom* (n 91).

Positive obligations also allow the Court to regulate horizontal relationships. The responsibility of a state to intervene may arise when it fails 'to regulate private industry in a manner securing proper respect for the rights enshrined in Article 8 of the Convention'.[97] The Court does need to pay regard to not overstepping its competence and therefore it has to assess carefully whether it has the legal basis to intervene. It must be shown that the infringing behaviour of the private party can be attributed to the failure of the state to act or to the state tolerating it.[98] According to the ECHR handbook on positive obligations, this means in practical terms that 'the state has been unable legally or materially to prevent the violation of the right by individuals, and otherwise because this has not made it possible for the perpetrators to be punished'.[99] There can be an obligation for the state to regulate private industry and to take adequate measures to secure the applicants' rights. In addition to the basic measures mentioned in the previous paragraph, this could prove relevant with respect to the EU legislature failing to determine the essential elements in the legislative act and allowing a margin of discretion to ESOs resulting potentially in significant interferences with EU citizens' right to respect for private life and the home.

Positive obligations ultimately aim at the effective application of the Convention and the effectiveness of the rights it provides.[100] This ambition is best captured in the *Airey* judgment: 'the Convention is intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective'.[101] The ambition of the Commission to make the rights in the Charter as effective as possible, as discussed in Chapter 4, echoes the principle of effectiveness of the ECtHR.[102] Moreover, this doctrine can also be linked to Article 16 TFEU, which provides that the EP and the Council have to lay down rules relating to the protection of individuals with regard to the processing of personal data. According to Hijmans, data protection legislation 'is indispensable to ensure the individual has a right which has meaning in practice'.[103] The importance of the clarification and specification on the application of core data protection principles to IoT systems for effective protection of the right to private life also weighs in on the question whether the EP and the Council have a duty to lay down rules on data protection in the legislative act introducing IoT systems. Another consideration here is that an omission on the part of the EU legislator will result in a very difficult position for the Commission when requesting ESOs to draw up a standard. Given these considerations, it is fair to conclude that the EP and the Council do have a duty to lay down detailed rules in the legislative act. Once the EU accedes to the ECHR the

[97] *Hatton and others* (n 15) para 119.

[98] Jean-François Akandji-Kombe, *Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention of Human Rights* (Human Rights Handbooks, No 7, Council of Europe 2007) 14.

[99] ibid.

[100] ibid 9.

[101] ibid 10. *Airey v Ireland* App no 6289/73 (ECtHR, 9 October 1979) para 24.

[102] 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'. See *Sabanchiyeva and Others v Russia* (n 11) para 132.

[103] Hielke Hijmans, *The European Union as Guardian of Internet Privacy* (Springer 2016) 266.

doctrine of positive obligations could become one of the ways to hold the EU institutions accountable for developing IoT policy and legislation that has a negative impact on effective protection of the right to privacy. It could be used to put pressure on the European Commission to support the EU legislature through the development of effective and practical safeguards in the impact assessment that guarantee the avoidance or mitigation of privacy interferences by IoT systems. The subsequent adoption of these essential elements of design in the legislative act by the Council and EP (among others on the basis of Article 16 TFEU) and the duty of the Commission to respect these elements in relation to their cooperation with ESOs would greatly contribute to the effective protection of the right to privacy.

Unlike smartphones, the IoT systems discussed here are not the result of market forces. These systems have marinated in years of lobbying, workshops, conferences, passionate speeches in parliament, until they grew into an EU policy and slowly matured into legislation. In short, their deployment is the result of the initiative and interference of EU institutions. By virtue of Article 52(3) of the Charter, a positive obligation, thus, rests with the European Commission and the EU legislature respectively to develop essential elements of design and to adopt these in the legislation introducing these systems. [104] These elements can set the parameters within which the ESOs develop the design of such systems respecting the right to privacy. This is in line with an interpretation of Article 8 ECHR, which effectively protects and safeguards the right to private life and the home. This positive obligation also echoes the ambitions of the EU to make the Charter rights as effective as possible, especially in the legislative process.

2.4 Reflections on implications for IoT systems

The primary anticipated interference consists in the mandatory installation of these systems into an individual's private environment, most importantly his home. The secondary anticipated interference with the right to private life facilitated by IoT systems is the processing of personal data against the will or without the knowledge of the person(s) whose data it concerns. Although this processing does not concern acoustical or visual categories of data, the nature of the information that can be inferred from it is likely to be intimate. This is, amongst others, due to the place where the device is installed, the systematic nature of the processing and the activities it concerns. The degree of intimacy depends to a great extent on the level of detail of the activities monitored. The severity of the interference it amounts to also depends on the context in which this personal data is processed. Processing enables the operators of these systems, and public authorities in their wake, to monitor activities within the home and the car. The third anticipated interference is a function which allows these systems (the smart meter, or the object they are latched onto (eCall and the car)) to be remotely shut down. The fourth anticipated interference consists of the potential sensors on the device that may be remotely turned on or off.

[104] Chapter 4, section 3.1 and 4.1.

The mandatory installation of IoT systems, which record, collect, store and use data generated in the course of a person's everyday activity, results in the non-consensual, involuntarily monitoring of a person's activity through the collection of data and additionally might allow remote control over certain aspects of a person's environment. This constitutes an interference with the right to private life and the home. Although it is not possible yet to draw precise conclusions about the severity of the interference, some general observations can be made. It is in the nature of the IoT that these systems will affect virtually everybody within the EU. The relationship in which they are installed is one in which the provider of the system is dominant, oligopolistic and in a position to impose his rules. The processing can take place without consent. The location where the systems are installed will vary from personal (car) to very personal (home). The subsequent recording of personal data will, although depending on the granularity of the data, be of an intimate nature; similar to the nature of the activities they facilitate interference with, for purposes that can be of both private and public. If IoT systems process data related to activity within the home, the right to respect for the home becomes relevant and an assessment has to be made to what extent this processing is detrimental to the 'quality of the private life' and 'the scope for enjoying the amenities of the home'.[105] This also depends on the secondary use made of this data or the secondary use that can be foreseen. The processing can have adverse consequences for the persons concerned and the systems might facilitate future violations of privacy in foreseen and unforeseen ways. The possibility that the IoT system facilitates remote control over a certain aspect of a person's life constitutes a grave interference with the right to private life. The potential for sensors to be remotely turned on exposes citizens to another grave interference with their right to private life. This may concern a microphone as will be discussed in Chapter 6. The installation and use of such a device usually requires a court order prior to its installation.

The considerations of the ECtHR in *Marper* about the future use of data are relevant for the mandatory installation of systems that can be used for other (future) purposes than they were originally installed for. This can be linked to the communications of the Commission on thriving data-driven economies, the central tenet of which is the multi-purpose facet of data, facilitated by the *interoperability* of data and IoT systems.[106] The possibility for secondary use opens a window of unforeseen processing, which results in a loss of control over the data by the person concerned and thus a loss of control over the aspect of his life covered by that data. In *Malone* and *Copland*, the use of personal data without consent and beyond the original context resulted in an interference with the right to private life. These cases point towards the underlying rationale of data protection: the idea that within a normal relationship data can be collected within reasonable boundaries, without constituting a breach of privacy, as long as they are only used within this relationship for agreed purposes that do not go against the data subject's reasonable expectation of privacy. However, the one bullet point on virtually every presentation on the advantages of the IoT is *interoperability*. The interoperable character of data enables their use beyond the original context. It could be seen

[105] *Powell and Rayner v The United Kingdom* (n 83) para 40.
[106] COM (2014) 442 (n 71). See Chapter 4, section 2.2.

as the standardisation of data, enabling communication in a network that spans the country, continent or world and providing the raw material for big data analysis, supposedly gaining immense value compared to data that can only be used within a singular context. The perspective and likelihood of these data being used beyond beyond their stated purposes should be involved in the impacts assessment of the Commission and feed back into the essential design choices to be made by the EU legislature.

Another category has to be distinguished from the conventional use of a system. IoT systems can also introduce vulnerabilities, which upon exploitation can cause the system to perform different functions than they were originally installed for, also known as *function creep*. These different functions can give rise to new interferences.[107] This means that legislation mandating the installation of an IoT system should be judged beyond the merits of its stated purpose. When the EU legislature uses its power to mandate the installation of these potentially intrusive systems it holds the responsibility to make sure that these systems do not introduce unnecessary risks into the lives of citizens. This responsibility is also confirmed by the fact that the impact assessment of the Commission aims to assess (unintended) negative impacts.[108] The system's design follows from the legislative act that introduced it. It should be scrutinised in the pre-legislative phase for potential vulnerabilities it brings into people's lives, as well as an assessment of the question whether this vulnerability can be avoided. If the answer is negative, the existence of these vulnerabilities should be taken into account in answering the question whether the mandatory installation of the system can be justified under the case law of the ECtHR and CJEU.

The effective protection of fundamental rights, the stated ambition of the European Commission, clearly resonates with the principle of effective and practical rights of the ECtHR. The ECtHR has linked this principle in the past to the concept of positive obligations and found that Article 8 ECHR might require from states the adoption of measures designed to secure respect for private life. This principle can be linked also to the consideration of the Strasbourg Court 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'.[109] This is in line with the approach advocated by the European Commission in the Impact Assessment Guidelines: unintended negative impacts *include* risks of interferences with fundamental rights. The principle of effectiveness, the assessment of foreseeable future use of functions provided by IoT systems and the concept of positive obligations, all point towards an obligation for the EU legislature to critically assess the design of these systems and adopt requirements in the legislative acts to ensure the effective protection of the right to private life. This obligation, moreover, would necessitate an assessment of the mandatory character of the installation of IoT systems and its possible justifications in light of the aim it serves. If the EU legislature cannot guarantee such

[107] Such as the microphone installed with the eCall system that could be used to eavesdrop on conversations in the car.
[108] Chapter 4, section 3.1.
[109] *S and Marper* (n 33) para 71.

requirements, the obligation for these systems should be reconsidered.[110] A deep and thorough understanding of the voluminous case law of the ECtHR and CJEU is a prerequisite for a proper execution of the impact assessment and decisions on the essential elements throughout the legislative process.

3. Requirements for interference with the right to privacy

After the interference with the right to privacy is established, the courts move to the question whether the interference is justified. Although the wording of the ECHR and the Charter differ, they come down to the same requirements to justify interferences with the right to privacy.[111] As noted above, by virtue of Article 52(3), Charter rights corresponding to ECHR rights should have the same scope and meaning, which includes the requirements that have to be met for an interference to be justified.[112] First, the interference has to be in accordance with the law, second it must be necessary (under the ECHR 'in a democratic society') and it must serve a legitimate aim. The necessity and legitimate aim are discussed in the same section, because the necessity of the measure is linked to the aim it serves. According to the Charter, the interference has to respect the essence of the right, a concept which only recurs occasionally in ECtHR case law. The application of these requirements in practice is gleaned from an analysis of case law with an emphasis on cases concerning surveillance and data protection. The nature of the interference, its extent and severity play an important role in the determination of the level of requirements that need to be met.

3.1 'In accordance with the law'

The first element to consider after establishing the interference is whether the latter is in accordance with the law. This is also referred to as the legality requirement or the rule of law test.[113] The test is not merely about the basis in domestic law 'but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention'.[114] The ECtHR leaves a broad margin of appreciation to the national courts in interpreting domestic law.[115] The basis in national law does not have to be statutory, but can be fulfilled by case law of national courts (even in Continental legal systems), delegated measures and even unwritten law. The ECtHR understands the law in a 'substantive', as opposed to 'formal' sense.[116] There are three sub-criteria for the *quality of*

[110] This last paragraph is inspired on Wisman (n 66).
[111] Compare Article 8(2) ECHR and Article 52(1) CFEU.
[112] Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02), C 303/33 (Article 52). Albeit it uses slightly different wording 'authorised limitations'.
[113] Kilkelly (n 89) 25.
[114] *Malone v The United Kingdom* (n 39) para 67.
[115] Steven Greer, *The exceptions to Article 8-11 of the European Convention on Human Rights* (Council of Europe Publishing 1997) 10.
[116] *Huvig v France* App no 11105/84 (ECtHR, 24 April 1990) para 28.

the law: the law should be *accessible*, *foreseeable* and it should provide *adequate safeguards* against arbitrary interferences with the substantive rights.[117]

Accessibility & Foreseeability

The Court has held that for a law to qualify as adequately accessible 'the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case'.[118] For a law to be *accessible* it has to be either published, or made available to those it affects. The accessibility of an 'order' from the Russian government that described the technical requirement of interception equipment that needed to be installed by communications service providers, was considered problematic, since it was published in the official magazine of the Ministry of Communications that was only distributed through subscription.[119] Accessibility with respect to IoT legislation can be problematic, because the actual functioning of IoT systems is described in standards, which are written in a technical language difficult or impossible to grasp for laymen. Moreover, these standards are not published and can only be accessed after paying considerable sums of money to the standardisation organisation.

For the law to be *foreseeable* citizens should be able to foresee with a reasonable degree of certainty the consequences which a given action may entail.[120] The law, therefore, must determine 'with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities'.[121] The law should provide for the limits on the exercise of power, an idea that closely corresponds to checks and balances in constitutional law. The overarching goal of this requirement is to provide adequate protection for the individual against arbitrary interference.[122] The level of precision that has to be met depends on the subject matter, 'the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed'.[123] For instance, the Court considered telephone tapping to be a *serious* interference that requires a law that is 'particularly precise'.[124] Clear and detailed rules were deemed essential especially in the light of the continuously increasing sophistication of technology.[125] The Court, thus, indirectly established a relationship between the refinement of the technology (assuming this covers the possibilities it offers) and the quality of the law, more specifically how accurate the competences of public authorities with regard to these possibilities are laid down in law. In cases concerning secret surveillance, the ECtHR particularly holds that the requirement of

[117] Greer (n 115) 9.
[118] *Sunday Times v The United Kingdom* App no 6538/74 (ECtHR, 26 April 1979) para 49.
[119] *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) para 242.
[120] *Margareta and Roger Andersson v Sweden* App no 12963/87 (ECtHR, 25 February 1992) para 75.
[121] *MM v The United Kingdom* (n 35) para 194.
[122] *Malone v The United Kingdom* (n 39).
[123] For the subject matter, see *Malone v The United Kingdom* (n 39) para 68; *Vogt v Germany* App no 17851/91 (ECtHR, 26 September 1995).
[124] *Huvig v France* (n 116) para 32.
[125] ibid; Greer (n 115) 11.

foreseeability should be applied with rigour.[126] The logic behind this is that secret surveillance carries a greater risk of abuse and therefore a certain level of transparency about the conditions under which this surveillance may take place is crucial. Obviously, the requirement of foreseeability should not result in prior knowledge of a suspect that his communication is tapped. The law, however, must provide an adequate indication in which circumstances in general and under which conditions public authorities are allowed to resort to 'this secret and potentially dangerous interference with the right to respect for private life and correspondence'.[127] The Court argued that because secret surveillance measures are:

> 'not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of unfettered power. Consequently the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.'[128]

This reiterates the earlier notion that the level of precision required depends on the subject matter. Foreseeability demands *limits* to be set with regard to the conditions under which certain designated parties may deploy certain measures. Clearly defined *limits* are an expression of *precision* and *clarity*, as opposed to arbitrariness.[129] The data processed by IoT systems can be used for secret surveillance and some IoT systems are equipped with sensors that can be remotely activated to facilitate secret surveillance. Secret surveillance will not be the original purpose for the installation of these systems. Nevertheless, their potential usefulness for this purpose should have consequences for the *essential elements of system design* adopted in the legislative act, discussed further in Chapter 4.

The principle of legal certainty requires that rules, which give rise to measures that adversely affect the rights and freedoms of designated persons, 'must be clear and precise so that he may know without ambiguity what his rights and obligations are and may take steps accordingly.'[130] With respect to mandatory IoT systems, the awareness of how they adversely affect citizens' freedoms and rights requires knowledge of their surveillance and control potential. Unawareness of this potential means the EU legislator misses essential information

[126] France was in violation of Article 8 since it did not specify the categories of persons liable to have their phone tapped, or the nature of the offences that warranted tapping. Bernadette Rainey, Elizabeth Wicks and Clare Ovey, *Jacobs, White & Ovey: The European Convention on Human Rights* (Oxford University Press 2010) 368; *Huvig v. France* (n 116) para 34.

[127] *Malone v The United Kingdom* (n 39) para 67.

[128] ibid, para 68.

[129] It should be noted that the protection of this requirement has been substantially diminished with respect to 'national security' by the acceptance of the ECtHR of overly broad categories of people and crimes that are liable to have surveillance measure executed against them e.g. whenever an international phone call is made. See Sarah J Eskens, 'Ongerichte interceptie, of het verwerven van bulk-communicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden' (2015) 85 Computerrecht 125. Also see Benjamin J Goold, 'Liberty and others v The United Kingdom: a new chance for another missed opportunity' (2009) PublL 5-14.

[130] Case 169/80 *Administration des Douanes v Gondrand Frères and Garancini* [1981] ECR I-1931, para 17; Case C-70/10 *Scarlet Extended* [2011] ECR I-11959, Opinion of AG Cruz Villalón, para 67.

when it takes decisions with respect to legislation mandating IoT systems. This lack of awareness of their intrusive potential also implies citizens do not receive this essential information when these systems are installed their private environment. After acceptance, the installation cannot be reversed.[131]

Adequate safeguards

The aim of safeguards is to protect citizens against the arbitrary use of power. It consists of the expression of the conditions and boundaries under which this power can be exercised. *Adequate safeguards* are especially relevant in the intersection of surveillance and data protection, since core data protection principles also provide safeguards through *inter alia* limiting data processing operations and creating transparency with respect to the parties allowed to process certain data. Safeguards can consist of restricting the kind of information that can be recorded, the nature of the offences that allow the competent authorities to engage in surveillance, the categories of persons against whom these measures may be taken, the parties that conduct the surveillance and the procedures that should be followed. Another safeguard deemed indispensable by the ECtHR is effective supervision of the authorities that engage in surveillance activities. For this supervision to be effective, it has to be independent, impartial and established in proper procedures.[132] Normally this should be guaranteed by judicial control, but the ECtHR has held in the past that other independent bodies can also suffice.[133]

What safeguards apply depends on the competences employed and the nature of the interference they allow. In *Uzun,* the ECtHR held that less strict safeguards applied to surveillance measures conducted through the use of GPS and that the minimum safeguards the applicant claimed were lacking, were not relevant to this particular measure.[134] Instead of these minimum safeguards, the Court applies the more general principles on adequate protection against arbitrary interference under reference to § 63, in which the requirement is spelled out that the 'Court must be satisfied that there exist adequate and effective guarantees against abuse.'[135] The Court elaborates that this depends on all the circumstances of the case and some more abstract considerations, in effect demanding no specific procedural safeguards in statute law in the context of surveillance measures other than visual and audio. Anyone paying attention to 'Frequent locations' on their iPhone understands the enormous amount of information that can be inferred from movement patterns: your home, your office, friend's homes, to other places you visit. It is also in line with the more recent case law of the

[131] An example of this are smart meters in the Netherlands, which can still be refused, although in practice the network operators put pressure on people with a number of fallacious arguments to accept the installation. People are not informed about the fact that the data collected by the smart meter may be used for other (government) purposes.

[132] *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000) para 55.

[133] *Klass and others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 56.

[134] *Uzun v Germany* (n 34) para 66.

[135] *Uzun v Germany* (n 34) para 63.

CJEU, discussed in section 2.1, confirming that the nature of the interference cannot solely be determined through the type of data (visual, audio, location), but also depends on other factors, such as the scope of the collection and how the data is used.[136]

Because part of these safeguards have to be expressed in statute law and provide information regarding the circumstances under which surveillance measures may be conducted, they enable the individual to foresee to a certain degree when they can be subjected to these. Adequate safeguards can be linked, therefore, to the requirement of foreseeability.[137] This is exemplified in *S and Marper v The United Kingdom* where the Court notes in relation to 'in accordance with the law' that it is essential to have detailed rules that govern the scope and application of measures:

> 'minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.'[138]

The ECtHR continues that in this case this relates to the broader question of whether the interference was necessary in a democratic society. Furthermore, it uses the data protection principles in force to substantiate the requirement of adequate safeguards. The next quote also confirms the link with foreseeability, because these safeguards have to be clearly indicated in the law regulating the discretion of the authorities:

> '… At each stage, appropriate and adequate safeguards which reflect the principles elaborated in applicable data protection instruments and prevent arbitrary and disproportionate interference with Article 8 rights must be in place'.[139]

In the context of data processing, these stages originally consist of the collection, use and storage.[140] The CJEU has, referring to ECtHR case law, adopted similar considerations:

> '…the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data … The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data…'[141]

---

[136] See section 2.1.

[137] They are also held relevant to the formal part of the proportionality test, to be discussed in the next section. The CJEU also held that the presence of safeguards can alleviate the disproportionality of the interference, see *Digital Rights Ireland* (n 61) para 54.

[138] *S and Marper* (n 33) para 99.

[139] *MM v The United Kingdom* (n 35) para 195; *S and Marper* (n 33).

[140] *MM v The United Kingdom* (n 35) para 196. When legislation mandates IoT systems, the generation of data also has to be considered.

[141] *Digital Rights Ireland* (n 61) para 54 and 55.

All these considerations relate to cases in which the collection of the data served to combat crime. In the context of IoT systems, the best way to protect people against the arbitrary use of their personal data is to avoid or minimise the collection of personal data altogether. This is also in line with the Commission's own view towards the methodology it employs in the *impact assessment*: to avoid or mitigate the violation of a fundamental right, e.g. through *effective safeguards that mitigate the negative impact on a fundamental right*.[142] Although the data collected by these systems might be considered trivial at first sight, the scope of the systems will create greater amounts of data and the data will become more sensitive if they are processed without restrictions. This is why adequate safeguards should be adopted at all the stages of the processing of the data, starting with their recording.[143] Although data in IoT systems will not be processed for secret surveillance purposes, according to the policy and laws introducing them, *ex post* legislation on the national level can enable public authorities to use the data collected by these systems for such purposes (comparable to the metering in *Malone*). The sensitivity of the data and the interference it may cause is increased also due to the societal context in which the collection is foreseen. The IoT vision, in which the use of data for a multitude of purposes is foreseen as opposed to the stated purpose(s) in the legislation introducing IoT systems, pursues the radical transformation of the nature of the initial interference caused by their mandatory installation. The adoption of effective safeguards, which require these systems to be designed in a way which avoids or mitigates the violation of the right to privacy, prevents or reduces their potential to transform.

3.2 The element of 'necessity', testing proportionality

The ECtHR has held that 'necessary' is not synonymous with 'indispensable', 'absolutely necessary', and 'strictly necessary', nor is it flexible like 'ordinary', 'admissible', 'useful', 'reasonable' or 'desirable'.[144] Necessity is assessed by means of a proportionality test, which is a construct of several subtests that play a varying role depending on the particular case. The aim of the proportionality test is to guide the assessment of the relation between the measure and the goal pursued. Proportionality as a principle is widely adopted in European systems of law, most importantly by the CoE and the EU. According to some, the widespread adoption of this principle 'transcends the barriers of contextuality erected between them', there are however reasons to doubt this view.[145] Proportionality is a relational concept. The proportionality of a measure can only be assessed in relation to the goal pursued, therefore, a clear formulation of the latter is of the utmost importance. Unlike proportionality in the context of the ECHR, the principle is established within several sources of EU law. The proportionality principle features outside the scope of fundamental rights in relation to EU

[142] Commission, 'Operational Guidance on Taking Account of Fundamental Rights in Commission Impact Assessments'(Commission Staff Working Paper) SEC(2011) 567 final 11-18.
[143] *MM v The United Kingdom* (n 35) para 200.
[144] *Handyside v The United Kingdom* App no 5493/72 (ECtHR, 7 December 1976) para 48.
[145] Tor-Inge Harbo, 'The Function of the Proportionality Principle in EU Law' (2010) 16(2) ELJ 158, 159.

competences.[146] According to Article 5(4) TEU, 'under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.' The measures adopted by the EU should also be reconciled with fundamental rights and in this context the review of proportionality is of a different nature.[147] The aim of Article 5(4) TEU is to channel the actions of the Union and to prevent it from crossing the boundaries of Member States' competence. Here, the principle of proportionality guides the relationship between the EU and Member States and functions as a general principle of action by the Union. In the context of Article 52(1) of the Charter, proportionality is a condition for the legitimacy of the limitation on the exercise of a fundamental right.[148] According to AG Villalón, the tests may follow the same course, but differ in the stringency with which they are executed; proportionality in the Charter is tested more stringently.[149]

The two courts have a different rationale: the ECtHR is guided by the protection of human rights, while the CJEU must balance a diverse set of general interests. These interests would include the economic integration through the establishment of the single market as well as the protection of human rights, but it is widely perceived that the centre of gravity resides with the former. Further differences in the contextuality follow from the formulation of the ECtHR that an interference has to be 'necessary in a democratic society', whilst the Charter merely requires that the 'limitation' is necessary.[150]

Legitimate aims and General interests

The necessity of a measure can only be judged in relation to the aim it serves. The interests that can justify interferences are very broad. Article 8 ECHR is unique in mentioning the economic well-being of the country. Sometimes the Court takes little effort in accurately assessing the legitimacy of the aim and consequently allows interferences with human rights serving interests that do not merit protection under the Convention.[151] These atypical rulings only emphasise the importance of the relation between the legitimate aim and interferences with fundamental rights. The concept of the public interest should follow 'from normative ideas about the relationship between the individual and society, the importance of rights in structuring this relationship, and so forth'.[152]

The CJEU is not primarily concerned with the relationship between the individual and society, but it is increasingly called upon to decide on fundamental rights, which is a broader

[146] Case C-331/88 *Fedesa* [1990] ECR I-4057.
[147] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* EU:C:2013:845, Opinion of AG Villalón, para 89.
[148] ibid, para 133.
[149] ibid, para 89.
[150] The choice for 'limitation' instead of 'interference' can also be viewed as using different words to cover up their meaning.
[151] This was aptly proven in *Otto-Preminger-Institut v Austria* App no 13470/8 (ECtHR, 20 September 1994) para 52.
[152] Stavros Tsakyrakis, 'Proportionality: An assault on human rights?' (2009) 7(3) ICON 468, 482.

notion than human rights, in relation to measures of EU institutions or Member States. It could be said that the CJEU operates with an 'integrationist bias'.[153] Its judgments are marked by the goal of economic integration. Pursuant to the Charter, measures can be adopted that 'genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.[154] The notion of 'general interests' in Article 52(1) of the Charter is an open category which covers a wide range of issues varying from the area of freedom, security and justice to the internal market.[155] One important difference between the goals as set in the ECHR and the Charter is that the former has a closed formulation, whereas the latter is open. The limitation according to the logic of the Charter has to meet genuinely *objectives of general interest* recognised by the Union or the need to protect the rights and freedoms of others. This can be relevant for the adoption of Union legislation that aims to utilise IoT systems prior deployed through EU legislation, since this open formulation implies that further use of systems could be based on any objective as long as this 'genuinely' meets a general interest of the Union.

The introduction of the Charter, with its broad spectrum of fundamental rights ranging from property rights to the rights to conduct business, increases the number of rights that the right to privacy has to compete with. Even though the ECtHR has also held applications by corporations to be admissible, these were always applications where the rationale of human rights was followed. Under the Charter, the CJEU accords these rights to businesses and does not shy away from balancing these rights against human rights of citizens.[156] Even worse, it has accorded fundamental rights to public authorities and held they can invoke these against citizens.[157] This introduces an entire new prospect for human rights violations, which are euphemistically dubbed 'limitations' in Article 52(1), justified by the protection of fundamental rights of businesses and government. This approach by the Court undercuts the special status of human rights and throws them on one big pile together with policy interests and business interests. This means that powerful well-organised interests can use the court system in Europe to erode the protection of human rights through invoking rights originally adopted to protect citizens' interests.[158] This is a radical departure from the human rights system under the ECtHR. Moreover, it is in conflict with the Charter, in particular with Article 52(3) mentioned above.[159] According to the explanations of the Charter, this includes the authorised limitations, which 'means in particular that the legislator, in laying down

[153] Benedikt Pirker, *Proportionality Analysis and Models of Judicial Review*, (Europa Law Publishing 2013) ch 6, 36.

[154] Article 52(1) of the Charter.

[155] In the Explanations of the Charter (n 9) the following list can be found: Article 3 and 4 TEU. Article 35(3), 36, 346 TFEU.

[156] *Scarlet Extended* (n 69).

[157] Case C-73/16 *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy* ECLI:EU:C:2017:253, Opinion of AG Kokott. See also Stéphanie Mihail and Tijmen HA Wisman, 'The Right to Privacy with Respect to the Processing of Personal Data in the Context of Controlling Tax Fraud', (2017) 3(2) EDPL 265.

[158] ibid 271.

[159] It should be noted that the economic well-being of the country is a legitimate aim under Article 8(2) ECHR, nevertheless this does not grant an opposing right to businesses as such.

limitations to those rights, must comply with the same standards as are fixed by the detailed limitation arrangements laid down in the ECHR'.[160] Allowing fundamental rights of businesses, or even public authorities, to compete with human rights of citizens lowers the standards of protection under the Charter as compared to the ECHR. The CJEU, as well as the EU legislature, should uphold the principle that these interests cannot directly compete with the rights enshrined in the ECHR.[161] Institutional practice deviates from this normative assumption. This levelling of interests goes against the very system of the ECHR.

Proportionality testing

The proportionality test is formulated by the courts often as a balancing of the rights of the individual and the interests of the state or the EU. In this balancing exercise, the (estimated) positive effects of a measure have to be weighed against the negative effects. In the field of IoT systems this is especially complex, because these systems can be used for secondary purposes (purpose or function creep), which can deliver a negative as well as a positive effect. However, in the face of human rights obligations, the primary purpose of which is to protect people against government interference, the negative effects of secondary interferences weigh heavier. Such a balancing exercise is a precarious matter, because there is no manual for the judge instructing how to weigh the opposing interests and, unlike Themis, the judge cannot rely on a pair of scales as an objective instrument. The balancing exercise, therefore, carries the risk of subjectivity, which is ironically what the proportionality test seeks to counter. Practice shows that this risk manifests in cases of the ECtHR, as well as the CJEU. Both are inconsistent in their application of the proportionality test. Nevertheless, the proportionality test has the potential to help to secure legitimacy of judicial decisions and to prevent making arbitrary decisions.[162] Proportionality testing can also help to secure the legitimacy of legislation mandating the installation of IoT systems.

Within the confines of legal doctrine there seems to be consensus about a steady formula in which the proportionality test is divided into three subtests — suitability, necessity and

[160] 'Explanations Relating to the Charter of Fundamental Rights' (2007/C 303/33).

[161] This does reveal the danger of the CJEU positioning preliminary questions in the key of the right to the protection of personal data, which is not covered by Article 52(3) of the Charter and therefore can compete under the Charter with business interests. The ECtHR has held that Article 8 of the Charter is inspired on Article 8 ECHR and Convention 108 and implicitly argued that it corresponds to Article 8 ECHR, when it wrote that Article 11 of the Charter, similarly 'is said to correspond to Article 10 of the Convention.' See *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* App no 931/13 (ECtHR, 27 June 2017) para 58. Interestingly, in the explanations of the Charter which lists the right 'which may at the present stage, without precluding developments in the law, legislation and the Treaties, be regarded as corresponding to rights in the ECHR', does not mention Article 8 of the Charter. The question, which is beyond the scope of this thesis, is whether 'law' includes case law of the ECtHR and additionally, if not, whether the autonomous interpretation of the ECtHR could change this and of course what the implications are for the way Article 8 of the Charter should be interpreted.

[162] Harbo (n 145).

proportionality stricto sensu — which should be performed in this order.[163] The logic behind this is that even if a measure is suitable and does not go beyond what is necessary to attain the goal, the measure can still be excessive in relation to its purpose. In practice, the courts rarely adhere to this formula. Nevertheless, for the sake of structure this division will be used in the following section.[164]

The ECtHR uses the proportionality test to assess whether the interference with the right to private life is 'necessary in a democratic society'. Although the phrase 'in a democratic society' does not play a major role, it can function as a guiding principle of interpretation.[165] The Court has not been generous in its elaborations on what it views as the core values of a *democratic society*.[166] The rule of law, tolerance and broadmindedness are some of the values it explicitly mentioned. Moreover, it has held that the purpose of the Convention is to 'maintain and promote the ideals and values of a democratic society'.[167] The Court does not view democracy simply as the rule of the majority, as it states that it 'does not simply mean that the views of a majority must always prevail: a balance must be achieved which ensures the fair and proper treatment of minorities and avoids any abuse of a dominant position'.[168]

The first and most basic subtest is in assessing whether the measure or legislation in question is *suitable* or *appropriate*, the latter frequently found in the wording that measures *should be appropriate for attaining the objective pursued*.[169] In some cases, the Court explicitly held that '*relevant'* only covers the suitability test and that '*sufficient* 'implies the necessity test (the second subtest).[170] In most cases, however, it does not make this distinction. When the CJEU applies this test in the context of Article 5(4) TEU to review legislative choices of economic, political or social nature, requiring complex assessments and evaluations, it grants the EU legislature broad discretion.[171] In order for the CJEU to find an action of the legislature to be in breach of this principle there is a heavy burden of proof that the measure 'manifestly goes beyond what is necessary to attain that objective'.[172] Rephrased in the context of data processing, the question could be turned to the suitability or appropriateness of the data processed to achieve the stated purpose.

The second subtest of the proportionality test is *necessity*, which raises the question whether there are less restrictive means to realise the aim. This test implies that the state must be able

[163] Norbert Reich, 'How proportionate is the proportionality principle' (The Reach of Free Movement conference, Oslo, 18-19 May 2011); Robert Alexy, 'Constitutional Rights, Balancing,and Rationality' (2003) 16 (2) Ratio Juris 131.

[164] Robert Alexy (n 162) 135; Dimitrios Kyritsis, 'Whatever Works: Proportionality as a Constitutional Doctrine' (2014) 34(2) OJLS 395, 396; Pirker (n 153).

[165] Janneke Gerards, *EVRM algemene beginselen* (SDU Uitgevers 2011) 151.

[166] Greer (n 115) 15

[167] *Soering* (n 17) para 67; Kilkelly (n 89) 31.

[168] *Gough v The United Kingdom* App no 49327/11 (ECtHR, 28 October 2014) para 168.

[169] Case C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-1106, para 74.

[170] *Margareta and Roger Andersson v Sweden* (n 120) para 96.

[171] Case C-491/01 *British American Tobacco (Investments) and Imperial Tobacco* [2002] ECR I-11453, para 123.

[172] Joined cases 453/03, C-11/04, C-12/04 and C-194/04, *ABNA and Others* [2005] ECR I-10423, para 83.

to prove that the interference was kept to a minimum to attain the legitimate goal it pursues and should be rooted in facts, because it is objectively possible to establish that a less restrictive mean realises the goal with equal efficacy.[173] This test therefore enables primary decision-makers to advance the right without detriment to the competing principle or right.[174] It is unusual for the ECtHR to execute this part of the test, which shows a preference for the balancing test.[175] Nonetheless, there have been some instances in which the Court held that 'the possibility of recourse to an alternative measure that would cause less damage to the fundamental right in issue whilst fulfilling the same aim must be ruled out', or alternatively that 'less intrusive methods of surveillance had previously not proved successful'.[176] There were some rare exceptions where the ECtHR took the opposite position, but these seem to be the odd ones out in the case law on proportionality.[177] Alternatively, if other states present evidence that there are less far reaching alternatives, the table might be turned.[178] When the interference with the right to privacy consists of data processing, this subtest can help to establish whether more data is processed than necessary to achieve the aim of the processing operation, in line with the principle of data minimisation. If so, this is a strong indication that the processing is not proportionate. With regard to the retention of data, the Court has held that '[t]he core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage'.[179] Another consideration here was the consistent application of these principles within the police sector of the Contracting States.

It is argued that the necessity test is performed more thoroughly when the margin of appreciation is narrow.[180] The CJEU seems to have a stronger focus on this part of the proportionality test.[181] There is an argument to be made against courts applying this test, because it could lead to judges taking decisions reserved for legislators. The European Commission and the EU legislature, however, are supposed to execute this test in the context of IoT policy and legislation. A failure to consider duly the alternatives to a restrictive measure on their part could be a reason for a judge to strike a measure down for being

[173] Rainey, Wicks and Ovey (n 126) 10.

[174] Eva Brems and Laurens Lavrysen, '"Don't Use a Sledgehammer to Crack a Nut": Less Restrictive Means in the Case Law of the European Court of Human Rights' [2015] 15/1 HRLRev 139, 143.

[175] Pirker (n 153) 199.

[176] *Nada v Switzerland* App no 10593/08 (ECtHR, 12 September 2012) para 183; *Glor v Switzerland* App no 13444/04 (ECtHR, 30 April 2009) para 94; *Sabanchiyeva and Others v Russia* (n 11) para 145; *Uzun v Germany* (n 34) para 80. Similar formulations exist where the state is expected to investigate whether 'less severe measures' are sufficient, see for an example *Kharin v Russia* App no 37345/03 (ECtHR, 3 February 2011) para 40.

[177] *Tre Traktörer Aktiebolag v Sweden* App no 10873/84 (ECtHR, 7 July 1989) para 62. In this specific case the Court held that despite the fact that the state could have taken less severe measures to pursue its goal, it still struck a fair balance.

[178] Gerards (n 165) 153.

[179] *S and Marper* (n 33) para 107.

[180] Gerards (n 165) 154. The margin of appreciation will be discussed under the subsection 'Margin of appreciation'.

[181] Paul Craig, *EU Administrative Law* (Oxford University Press 2006) ch 17; Pirker (n 153) ch 6.

disproportionate. If the impact on the right is considered to fall below the minimum level of severity, and the interference is with the periphery of the right rather than its core, an omission of the necessity test could be accepted by a court.[182] An important advantage of this 'less restrictive means test' is that it allows to 'smoke out unacceptable motives'.[183] The legislator can formulate one aim, which is legitimate in itself to override rights, whilst the design of the system in fact serves another aim which remains hidden. By restricting the functions of IoT systems to what is necessary for their officially stated reasons, the risk of abuse of mandating the installation of these systems is prevented, or at least minimised. The necessity test or less restrictive means test, therefore, is a requirement fit to address and prevent IoT systems' potential for future privacy violations.

In most instances, the ECtHR takes all factors into account before it executes a balancing test, which is the third subtest. Despite the right to private life handbook referring to the *fair balance* test as the proportionality test 'at its simplest', this can actually be viewed as the most complex, or perhaps opaque, part of the test.[184] To systematise this test the Court relies on a number of factors, the most important of which are *the interest* to be protected from the interference, *the nature* of the interference and *the pressing social need* for the interference to take place.[185] In assessing whether a pressing social need is present, the ECtHR focuses on particular facts and circumstances of the case and country, plus it has to be convinced there has been an acceptable assessment of the relevant facts at issue.[186] In short, the pressing social need should be objectively verifiable. Sometimes, the ECtHR initially skips the second subtest of necessity, but then complements the balancing test with the necessity-test and argues that the availability of alternative solutions is only one of the factors in the assessment of the question whether a measure strikes a fair balance.[187] In complex cases involving the assessment of surveillance legislation particularly, the Court can link the question of *foreseeability* to whether it is *necessary in democratic society*.[188] Setting clear rules on the conditions on the deployment of surveillance measures and the efficient safeguards on their appropriate use contributes to a system that keeps the power of the government in check and is more likely to limit its use to when it is necessary.

A similar approach can be discerned in the case law of the CJEU. This court does not explicitly mention the requirement of foreseeability, nor the necessity in democratic society, instead it uses the term 'proportionality'; the logic is similar nonetheless. In *Digital Rights Ireland*, Directive 2006/24/EC, the Data Retention Directive, was annulled. Both the Court and the AG Villalón made numerous observations hinting at the *quality of the law*, even if

[182] Brems and Lavrysen (n 174) 11-12.
[183] ibid 9.
[184] Kilkelly (n 89) 31.
[185] Kilkelly (n 89) 32.
[186] Greer (n 115) 14.
[187] Pirker (n 153) 227; *James and Others v The United Kingdom* App no 8793/79 (ECtHR, 21 February 1986) para 51.
[188] *Klass and others v Federal Republic of Germany* (n 133) paras 59 and 60; *Roman Zakharov v Russia* (n 119) para 236.

only the latter explicitly recognised its relevance. The Court found a general absence of limits in the directive and a lack of an objective criterion to determine those limits to the retention of data resulting in the indiscriminate retention of all traffic and location data of practically the entire European population lacking any relationship with the directive's objective. There were no substantive or procedural conditions established for the competent national authorities to gain access and subsequently use the data. [189] Moreover, no objective criteria were established to limit the persons authorised to access and use the data to what is strictly necessary in the fight against serious crime. Neither was there an obligation for Member States to adopt an objective criterion to determine the limits for national authorities to access such data.[190] The CJEU held that Directive 2006/24/EC does not establish 'clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Article 7 and 8 of the Charter', whereby the EU legislature overstepped the boundaries imposed by the proportionality principle.[191] In *Scarlet Extended*, the CJEU deviated from the AG's opinion in a similar fashion as in *Digital Rights Ireland*, which indicates a preference for skipping the legality-test. Instead of finding incompatibility of the demand for a filtering system with the law, the CJEU commenced with the balancing exercise. It found that the injunction to install this system did not strike a *fair balance* between, on the one hand, the intellectual property rights of the copyright holders and, on the other, the freedom to conduct a business enjoyed by the ISPs and the right to protection of personal data of ISP customers.[192] This case shows how the Charter is invoked to transform business interests into 'fundamental rights'.

Scholars such as Habermas criticise the balancing exercise as it levels human rights and the pursuit of the public interest, questioning the protection of rights based on policy arguments.[193] This criticism fits the shift of the balancing exercise in the EU *acquis* where strong, well-organised, corporate interests are allowed to compete with fragile, scattered parties representing human rights.[194] The image of a balance unjustly positions human rights on an equal footing with other societal interests. This ignores the fact that these rights lie at the heart of Western constitutional democracies. The core of the ECHR, as laid down in Article 1, is the obligation for States to respect and secure to everyone within their jurisdiction the rights and freedoms defined in Section I of the Convention. The rights in the ECHR take priority over the policy goals, which Greer termed 'the priority to rights' principle.[195] The case law of the ECtHR diverges on this point: there are cases in which the higher status of human rights are recognised; on the other hand, there have been occasions where the Court treated the rights and exceptions as equal by expressing the need to balance

[189] *Digital Rights Ireland Ltd v Minister for Communication et al* (n 61) paras 56-61.
[190] ibid, para 60.
[191] ibid, paras 65 and 69.
[192] *Scarlet Extended* (n 69).
[193] Jürgen Habermas, *Between facts and norms* (Cambridge 1996), 256-259.
[194] Lawrence Lessig, *Code* (Version 2, Basic Books 2006) 200-201.
[195] Steven Greer, '"Balancing" and the European Court of Human Rights: a Contribution to the Habermas-Alexy Debate' (2004) 63(2) CLJ 412, 417.

them.[196] Moreover, the balancing exercise is often executed as a contest between the rights of the individual affected by the measure and the interest of the community as a whole,[197] which calibrates the scales in a manner favourable to shifting the centre of gravity from human rights towards the public interest.[198] The ECtHR has formulated a number of general principles in relation to the right to privacy, but these do not transcend the level of the individual, unlike the right to freedom of expression where the Court has expressly linked this right to its role in democratic society. An increasing number of authors take the view that privacy should be viewed as a societal interest.[199] The right to privacy facilitates the exercise other civil rights (freedom of expression, association, religion) without fearing possible repercussions by a suppressive government or other antagonists. Moreover, the aim of IoT systems is to be used by everybody, which supports a reading of the right at issue to transcend to the level of societal interests. The final objection against the balancing metaphor is that a gain on one side of the scales results in a loss on the other side. This ignores the fact that, especially in the context of system-design, it is possible to make choices that respect the right to privacy, whilst preserving the functionality of the system.[200]

Margin of appreciation

In the case law of the ECtHR, the proportionality test cannot be viewed in isolation from the *margin of appreciation*. In the course of time, the margin of appreciation developed into its current function 'as a general doctrine of discretion in the implementation of proportionality review'.[201] According to the case law, it is first and foremost up to the national authorities to execute the proportionality test: they are in a better position to assess the particularities of a situation, although, the Court holds the privilege to execute the final test which 'constitutes the most important yardstick for evaluating whether the national authorities have overstepped the margin of appreciation.'[202] Whether the margin of appreciation allowed to the state is *narrow* or *wide* depends on the circumstances, the subject matter and the background of the case. Again, context is everything.[203] If the margin is narrow, chances are higher that the Court will find a violation of the right at issue, if it is wide it is more likely that the

[196] Greer (n 115) 15.

[197] *Hatton and others v The United Kingdom* (n 15) para 129.

[198] Başak Çali, 'Balancing Human Rights? Methodological Problems with Weights, Scales and Proportions' (2007) 29 (1) HumRtsQ 251, 259.

[199] Priscilla M Regan, 'Privacy and the common good: revisited' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy* (Cambridge University Press 2015); Kirsty Hughes, 'The social value of privacy, the value of privacy to society and human rights discourse' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy* (Cambridge University Press 2015).

[200] Charles Raab, 'Effects of surveillance on civil liberties and fundamental rights in Europe', in David Wright and Reinhard Kreissl (eds), *Surveillance in Europe* (Routledge 2015) 261-262.

[201] Julian Rivers, 'Proportionality and discretion in international and European law' in Nicholas Tsagourias (ed) *Transnational Constitutionalism* (Cambridge University Press 2014) 126.

[202] Yukata Arai, 'The Margin of Appreciation Doctrine in the Jurisprudence of Article 8 of the European Convention on Human Rights' (1998) 16(1) NQHR 41, 43.

[203] Kilkelly (n 89) 32

Contracting State will be acquitted.[204] The Court has found several factors to be relevant in determining the margin of appreciation. These include 'the nature of the Convention right in issue, its importance for the individual, the nature of the activities restricted,[205] as well as the nature of the aim pursued by the restriction',[206] the nature of the measure and how far this intrudes into the life of the applicant, the *pressing social need* that it seeks to address, the level of consent between Contracting States on the subject matter (which is linked to some extent to social acceptance of a phenomenon) and the technical complexity of the matter.[207]

With regard to *the nature of the right*, the Court has held that the margin will be narrower if the right at stake is 'crucial to the individual's effective enjoyment of intimate or key rights'.[208] The more important and fundamental the right at issue, the narrower the margin of appreciation for a state will be; this applies to negative as well as positive obligations.[209] There is 'an inverse relationship between the importance of the right to privacy in question on the one hand and the permissible intensity of the State's interference on the other hand.'[210] The importance of the right to respect for the home for applicants was held to be 'pertinent to their own personal security and well-being'. This has a narrowing effect on the margin of appreciation granted to the government.[211] The Court held that if the right at stake is 'crucial to the individual's effective enjoyment of intimate or key rights' the margin tends to be narrower.[212]

The *importance for the individual* is another relevant factor. Article 8 is held to concern rights of central importance to an 'individual's identity, self-determination, physical and moral integrity, maintenance of relationships with others and a settled and secure place in the community …. the scope of the margin of appreciation depends on the context of the case, with particular significance attaching to the extent of the intrusion into the personal sphere of

[204] *Lautsi v Italy* App no 30814/06 (ECtHR, 18 March 2011), Dissenting opinion of Judge Malinverni, joined by Judge Kalaydjieva.

[205] Sexual activities are deemed one of the most intimate aspects of private life. See *Dudgeon v The United Kingdom* App no 7525/76 (ECtHR, 22 October 1981) para 52.

[206] The Court grants a wide margin of appreciation to the legislature in social and economic policies, such as housing. The Court explicitly limited this to the right to property under Article 1 of Protocol No. 1, 'not Article 8 which concerns rights of central importance to the individual's identity, self-determination, physical and moral integrity, maintenance of relationships with other and a settled and secure place in the community'. When these type of policies interfere with the rights protected under Article 8 ECHR the margin of appreciation will depend on the extent of the intrusion into the personal sphere. See *Connors v The United Kingdom* App no 66746/01 (ECtHR, 27 May 2004) para 82.

[207] *Christine Goodwin v The United Kingdom* (n 91) para 92; Pirker (n 153) 9.

[208] *MK v France* App no 19522/09 (ECtHR, 18 April 2013) para 31; *Connors v the United Kingdom* (n 206) para 82; *S and Marper* (n 33) para 102.

[209] *X and Y v The Netherlands* App no 8978/80 (ECtHR, 26 March 1985); *KU v Finland* (n 91) para 43

[210] *Hatton and others v The United Kingdom* (n 15) Joint dissenting opinion of judges Costa, Ress, Türmen, Zupančič and Steiner, para 10.

[211] *Gillow v The United Kingdom* (n 80) para 55.

[212] *Connors v The United Kingdom* (n 206) para 82.

the applicant.'[213] Following the earlier finding, the *importance for society* is also relevant in the context of EU-wide deployment of IoT systems.

This rather long list can result in conflicting answers with regard to the state's wide or narrow margin of appreciation. With the risk of becoming repetitive, which view prevails in the end depends upon the context.[214] The scope of the margin of appreciation of Contracting States is inversely proportional to the extent they intrude upon the personal sphere of the applicant. This criterion provides an additional ground for interpretation of the significance of the context for the importance of the right for the individual. When the Court held that the right to respect for the home is pertinent to the *personal security and well-being* of the applicants, it continued by stating that the 'importance of such a right to the individual must be taken into account in determining the scope of the margin of appreciation allowed to the Government'.[215] This implies that when the EU legislature mandates IoT systems for the home it has to pay particular attention to the proportionality of this measure, which is linked intrinsically to the design. Jacobs, White and Ovey also note that if 'a particularly important facet of an individual's existence or identity is in issue under Article 8, the Strasbourg Court will be less likely to accept that a Contracting Party should be afforded a broad discretion'.[216] Since the design of an IoT system and its mandatory installation pose a risk of subjecting citizens' lives to a complex public-private surveillance assemblage, the margin of appreciation granted to the legislature with respect to the design of this system should be narrow.

On the one hand, the ECtHR has held that the legislature has a wide margin of appreciation in implementing social and economic policies; on the other, it recognised that 'the scope of this margin depends on such factors as the nature and seriousness of the interests at stake and the gravity of the interference'.[217] *Hatton v. UK* concerned pollution caused by the nearby presence of an airport. The Court held in first instance that Article 8 required the State to 'minimise, as far as possible, the interference with these rights, by trying to find alternative solutions and by generally seeking to achieve their aims in the least onerous ways as regards human rights.'[218] The means by which this needed to be pursued was through 'a proper and complete investigation and study with the aim of finding the best possible solutions'.[219] The Grand Chamber reversed this decision and granted a wide margin of appreciation to the UK. The prudence of the Grand Chamber was fuelled by the consideration that environmental human rights only remotely fall under the scope of Article 8.[220] The processing of personal

[213] ibid
[214] *Hatton and others v The United Kingdom* (n 15) para 103.
[215] *Gillow v The United Kingdom* (n 80) para 55.
[216] Rainey, Wicks and Ovey (n 126) 327.
[217] *Peck* (n 22) para 77.
[218] *Hatton and Others v The United Kingdom* App no 36022/97 (ECtHR 2 October 2001) para 97.
[219] ibid, para 86.
[220] *Hatton and others* (n 15) para 96. This was only after the case was referred to the Grand Chamber. It should be noted that five judges argued in their dissenting opinion that this approach to environmental human rights meant a step backwards from the case-law developed up to that point, because it 'gives precedence to economic considerations over basic health conditions'.

data by ICT-systems forced in the private sphere, however, does directly fall under the scope of the right to private life. The approach in the first *Hatton* case is, therefore, more appropriate in the context of IoT systems, since it held 'that States are required to minimise, as far as possible, the interference with these rights, by trying to find alternative solutions and by generally seeking to achieve their aims in the least onerous way as regards human rights'.[221] Using EU legislation to deploy, or even make the installation of IoT systems mandatory, places the burden of responsibility on the EU institutions to see to the minimisation of the interference(s) following from this installation.[222] The impact assessment of the Commission could be a good starting point to fulfil this duty.

3.3 'Essence' of the right to privacy

'The very essence of the European Convention on Human Rights is respect for human dignity and human freedom.'[223]

While it is impossible to give a definition of the essence of the right to privacy, getting to grips with this notion is valuable in terms of determining the limits of the legislature's discretion. The mere notion of the essence of the right recognises that some part of it cannot be entrusted to Themis scales. The limitation of rights must not 'restrict the exercise of the right in such a way or to such an extent that the very essence of the right is impaired'.[224] The Court has stressed on numerous occasions that the essential object of the right to private life is to protect the individual from arbitrary interference by public authorities.[225] It could be argued, therefore, that the essence of this right, as well as the right to respect for the home, could be at risk once measures are adopted that facilitate or constitute arbitrary interferences.

To assess whether this is the case it is necessary to delve a bit deeper into the meaning of arbitrariness. Arbitrariness is typically void of reason. When measures are adopted without rational selectivity with respect to conditions under which they are employed, be it to everybody or always, or even worse, always to everybody, a suspicion of severe arbitrariness and an attack on the core of privacy is raised. The case law of the courts and the requirements developed in it always demand from the state to restrict their power based on rational, knowable categories.

Instead of taking the arbitrariness of the interference as the starting point, it is also possible to take a step back. Privacy, in its classic sense as the right to be left alone, is a state of non-interference.[226] The adoption of measures entailing a standard interference with the right to

[221] *Hatton and Others* (n 218) para 86.
[222] This is also consistent with other case law from the ECtHR. See *López Ostra v Spain* (n 37) para 55.
[223] *Pretty v The United Kingdom* App no 2346/02 (ECtHR, 29 April 2002) para 61.
[224] *Mikulová v Slovakia* App no 64001/00 (ECtHR, 6 December 2005) para 52; *Gobec v Slovenia* App no 7233/04 (ECtHR, 3 October 2013) para 159.
[225] To put it in less distant terms, what the right to privacy seeks to secure is protection of the individual from being left to the tender mercy of collective powers that seek to control his life for their own goals.
[226] Warren and Brandeis (n 26).

privacy of everybody, e.g. through the massive collection of detailed data, could, in combination with other factors, amount to the impairment of the core of the right to privacy.

The Court did elaborate on various occasions on key or intimate rights under Article 8, which could be an indication for their importance for the essence of the right to privacy. The case law suggests that the more intimate the part of the life that is interfered with, the more serious the reasons must be for such interference.[227] This indicates that the nature of the activity restricted is relevant. Respect for the home is considered an essential right, vital to personal security and the well-being of the individual and measures that interfere with this respect for the home could also be said to impair personal security and well-being.

The CJEU has discussed the practice that hampered the essence of the right to private life directly, when it had to examine the US legislation sanctioning surveillance practices of US agencies exposed by the Snowden revelations (see section 2.1). The CJEU held that the essence of the fundamental right to private life was compromised due the legislation permitting the access to the contents of communications on a generalised basis. Although the CJEU limited this judgment to the contents of communications, in line with *Digital Rights Ireland*, the AG departed from this line of reasoning in *Tele2 Sverige* by holding that metadata are more sensitive, given their suitability for automatic processing.[228] The original element in the AG's approach was the emphasis on the nature of the information that could be inferred from these data (see section 2.1) central to the question on the severity of the interference with the right to privacy, as opposed to an emphasis on the nature of the data retained. The Court in this case first agreed, referring to the opinion of the AG, that data does provide the means to establish profiles of people and that this information is as sensitive as the contents of communication. A few paragraphs further, however, the Court tied itself in a knot by noting that data retention legislation did not affect the essence of Article 7 and 8 of the Charter, simply because 'it does not permit retention of the content of a communication'.[229] Metadata can be processed more effectively, analysed automatically and all this against far lower costs, providing the intelligence community the means to spy on an entire population.[230] The NSA General Counsel Stewart Baker stated that 'metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.'[231] When David Cole confronted his opponent, General Michael Hayden (former director of the NSA and the CIA), with this quote he replied 'absolutely correct' and raised the stakes: 'We kill people based on metadata.'[232] This is only to illustrate

[227] *Pretty v The United Kingdom* (n 223) para 59.

[228] Here the AG drew from the report of the United Nations High Commissioner for Human Rights (Human Rights Council) on the right to privacy in the digital age, 30 June 2014, A/HRC/27/37, para 19.

[229] *Tele2 Sverige* (n 63) paras 99 and 101.

[230] This was already convincingly argued by Patrick Breyer in 2005: Partrick Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) 11(3) ELR 365, 370-371.

[231] Alan Rusbridger, 'The Snowden Leaks and the Public' (NYR, 21 November 2013) http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/> accessed 17 June 2014.

[232] David Cole, 'We Kill People Based on Metadata' (NYR Dailey, 10 May 2014) <http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/> accessed 17 June

that the retention and use of data cannot be judged based on their nature, which the CJEU and the ECtHR both mistakenly did in the past. Instead, it must be judged on the nature of the information that can be inferred from it. It is this factor, together with the context of the processing as well as the future use of these data and systems that should be decisive in establishing whether it interferes with the essence of the right to privacy.

Among other factors relevant for determining whether an EU measure impaired the essence of the right, the CJEU takes into account whether these measures were applied based on *individual conduct* and under *exceptional circumstances* referred to in the law establishing the measure.[233] This is yet another indication that mass surveillance measures, such as data retention, are irreconcilable with the essence of the right to private life, because they affect everybody on an unconditional basis. Such inference follows from the rationale of human rights more generally and Article 8(2) ECHR particularly which provides that the interference is the *exception.*[234] This requirement was also confirmed by the CJEU in *Tele2 Sverige*, where it held that a legal basis which allows restrictions on the scope of a fundamental right should be interpreted strictly and cannot allow the exception to become the rule.[235] This requirement supports a powerful plea against measures recording and retaining data indiscriminately.

In sum, there are a number of factors connected to legislation mandating the roll-out of IoT systems which have to be taken into account when answering the question whether this legislation impairs the essence of the right to private life or creates a risk thereto. These include the place of installation of IoT systems, the nature of the data they record and the nature of the information that can be inferred from it, the context of the processing, the near-continental scale on which the roll-out of these systems is foreseen (status and number of people affected) and the activities they facilitate interference with.

3.4 Implications and conclusions for EU law mandating IoT systems

There are a number of implications following from these requirements, which are particularly important for the notice of the Commission officials involved in the pre-legislative process.

2014. It should be noted that there is fierce criticism against this practice, not only because of the dehumanisation of killing another person, the lack of judicial scrutiny, the collateral damage involved in these strikes etcetera; but also on the very practical ground that the conclusion that a person should be killed based on metadata analysis is often wrong.

[233] Case C-601/15 *PPU – N* ECLI:EU:C:2016:84, para 52.

[234] Italics added by author. The word 'except' is not found in art 52 of the Charter. This can be viewed as an omission that is repaired by art 52(3) which provides that rights in the Charter corresponding to the ones in the ECHR, shall have the same meaning and scope. This position is also adopted by the ECtHR. See eg *KU v Finland* (n 91) para 49. The Court takes the position that the right to privacy in the context of telecommunications and Internet services 'cannot be absolute and must yield *on occasion* to other legitimate imperatives', clearly underlining the incidental nature of the interference.

[235] *Tele2 Sverige* (n 63) para 89.

First, EU legislation authorising the obligatory installation of IoT systems has to include provisions on functionalities that (potentially) interfere with the right to privacy. Secondly, this law needs to be accessible. This will not raise a problem if the functionalities are established in EU law which is published in the Official Journal of the EU. This requirement will not be met, however, when these functions are determined in a later stadium in standards which require a fee to be accessed. Thirdly, the law must be foreseeable. It follows from the demand of foreseeability in conjunction with adequate safeguards, that the modalities of the functions which interfere with the right to private life are defined in the law. Since the installation of IoT systems is an initiative of the EU, especially in the light of their surveillance potential, the required level of precision with which the functions are indicated should be high.

With regard to the necessity and proportionality of the measure, the requirements can be broken down in the three subtests of proportionality. First of all, when an IoT system is made mandatory it has to be *suitable* to realise the aim it serves. This test usually does not raise problems. Second, the installation of the IoT system must be *necessary* to achieve this aim. Due to the specific context, in which the EU institutions take the initiative to make these systems mandatory or semi-mandatory (hard or impossible to escape their installation in the long run) through EU law, there is an extra important obligation on the EU legislature to investigate the options of designing these systems in a manner that would avoid or minimise the interferences with the rights enshrined in Article 8 ECHR.[236] If it is impossible to design the system in a way that does not interfere, or risks to interfere, with the right to privacy, proportionality in the strict sense has to be tested by balancing the interests at stake against the right to privacy. In this balancing exercise, particular attention should be paid to the *interest to be protected from interference, the nature of the interference* and *the pressing social need*.[237] The nature of the interference has an effect on the interests requiring protection. Here, it is necessary to determine the functions of the IoT system and how they may facilitate the interests of parties that may gain access to the system. To make an adequate assessment of the affected rights, the potential secondary use of the IoT system – inter alia its data-processing as well as its remote control features – should be thoroughly reviewed.

In the reports written under auspices of the European Commission, as well as the various communications and other acts it has adopted on the IoT, privacy is placed always on par with some general interests of the EU, most notoriously security and/or economic interests. Although not outspoken, the position implicitly adopted by the various authors and the Commission is one of hard-core utilitarianism, where the harm done to individuals can always be justified when this is outweighed by the benefits to society. This harm may consist in subjecting individuals to the continuous recording of certain aspects of their lives. The mandatory installation of IoT systems could force people into a state where they can practically no longer choose to spend their time in their private environment *offline*, that is to say unmonitored and unrecorded. The harm that may follow from such measures is that

[236] *Hatton and others v The United Kingdom* (n 15) para 97.
[237] Kilkelly (n 89) 32.

people may feel continuously monitored, resulting in a 'chilling effect' and turn their private environment into a modern panopticon.[238] The recording of data can produce a disciplining effect, because the perspective that this data might be mined at a later stage through secret algorithms puts citizens in a position in which they always need to fear scrutiny. In the panopticon, the prisoner did know what behaviour was undesirable. In modern society there is uncertainty about what behaviour might offset an action from the state.[239] The mere possibility of surveillance will already have a disciplining effect. This position is irreconcilable with the priority of rights-principle that follows from the ECHR as well as the proclaimed founding values of the EU enshrined in Article 2 TEU: respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights. Therefore, a lack of concrete demands on these systems allowing them to maintain their *panoptic potential* creates the risk that citizens' private environment is turned into an experimental prison complex.[240]

It is apt here to refer to the near prophetic dissenting opinion of Justice Brandeis in the first wire-tapping case before the Supreme Court in the US, in which the majority of the Court held that wiretapping was not protected by the Fourth Amendment:

> 'Moreover, "in the application of a constitution, our contemplation cannot be only of what has been, but of what may be." The progress of science in furnishing the government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions…. Can it be that the Constitution affords no protection against such invasions of individual security?'[241]

What Justice Brandeis predicted here, in 1928, is the potential of science in refurbishing our homes in ways that they become animated and able to spy on its inhabitants. This Orwellian panorama has materialised in more or less sophistication in modern society. IoT systems furnish the private environment of citizens with senses and thus erode their personal security.

4. Conclusion

The material scope of Article 8 ECHR and Article 7 of the Charter is broad, non-exhaustive and technology-neutral. The right to privacy in Europe is polymorphous and adaptable to the most challenging of circumstances. The roots of this right lie in the protection of the individual against abuse of power by public authorities to provide a maximum of freedom by keeping interference with his life to the minimum necessary. Autonomy is an important

[238] Jeremy Bentham, 'Panopticon' in Miran Bozovic (ed), *The Panopticon Writings* (London, Verso 1995).
[239] Michel Foucault, *Discipline and Punishment* (Translation copyright 1977 by Alan Sherdan, 2nd edition, Random House inc 1995) 200-203.
[240] ibid 203.
[241] *Olmstead v United States* 277 US 438 (1928) 474-475.

principle underlying the interpretation of its guarantees. The introduction of ICT in the arsenal of the state was met with creative interpretation, capturing the collection, storage and use of personal data under the scope of the right to private life and protecting citizens against the repurposing of data acquired by commercial parties pursuant to a contract. The ECtHR has formulated positive obligations for the state to intervene in affairs between private parties when there is a risk that the enjoyment and effective protection of the right to private life is substantially undermined. The nature of the interference and the interest protected, as well as the practical possibility for imposing a positive obligation are relevant here. The aim of the Convention is to secure human rights, including Article 8 ECHR (and Article 7 of the Charter in its slipstream) effectively. It should be interpreted, thus, in a way that renders its protection practical and effective.

The rights under Article 8 ECHR are always deemed important for the individual, yet are never linked to society more widely. Numerous authors take the position that the right to privacy serves society at large.[242] This also follows from the constitutive function the right to privacy fulfils with respect to other civil rights, such as freedom of expression and assembly. This constitutive function is recognised by the CJEU to serve society and democracy.[243] Acknowledging the fact that the right to privacy is a societal value becomes particularly important when it has to be interpreted and applied to the deployment of ICT-systems which affect every single citizen and thus society at large. This is an important observation that should inform the strictness with which the right to privacy should be interpreted and applied in the course of IoT policy and the legislative process.

The mere forced installation of an IoT system into the private sphere or private property of a citizen amounts to an interference under Article 8 ECHR and Article 7 of the Charter. The severity of this interference depends among others on what data is collected, its granularity, the ability of the system to allow control over or monitoring of the private environment and the ability to exercise remote control. Although such legislation forcing ICT-systems into citizens' lives on this scale is unprecedented, the right to private life and the home offer suitable requirements to inform decision-making with respect to system design.

The right to privacy should already be taken into account in the first elaborations on system design. The *potential future privacy violations* facilitated by IoT systems once they have become mandatory by law, is a phenomenon that is hard to remedy through reliance on EU law.[244] Taking the right to privacy as the starting point enables effective contemplation on the functions necessary to serve the stated aim of the system. It facilitates taking advantage of the 'less restrictive means test' by allowing to 'smoke out unacceptable motives' guiding the system's design.[245] The proportionality test requires the European Commission and the EU legislature to consider alternatives of system design where the right to respect for private life and the home is not interfered with, or the interference is minimised. By restricting the

[242] Regan and Hughes (n 199)
[243] *Digital Rights Ireland* (n 61).
[244] *Willems* (n 74).
[245] Brems and Lavrysen (n 174) 9.

functions of IoT systems to what is necessary for their officially stated reasons, *potential future privacy violations* can be nipped in the bud. If the interference cannot be avoided, the proportionality test provides an instrument to weigh the positive effects against the negative. In deciding the outcome the intensity of the measure and the existence of less infringing alternatives need to be taken into account.

Depending on the severity of the interference, certain requirements have to be met. The demand for a basis in the law goes beyond a simple legal positivist approach and the presence of a law is not enough to turn a practice legal. The three quality-of-law criteria add extra demands, most important of which are *foreseeability* and *adequate safeguards*. The former should enable the citizen to foresee the consequences of the installation of the IoT system for his right to privacy. Adequate safeguards pertain to procedural fairness. These should protect the individual against abuses of power by the state and its public authorities. The requirement of adequate safeguards can be linked to one of the aims of the Commission's fundamental rights impact assessment, which is to identify *effective safeguards that could mitigate the negative impact on a fundamental right*.[246] Moreover, a duty for the EU legislator can be derived from the case law of the ECtHR to execute a proper and complete investigation to achieve the aims of the IoT systems in the 'the least onerous ways as regards human rights.'[247] This duty follows from the Charter which interlocks with the case law of the ECtHR.[248]

IoT systems that interfere or introduce substantial risks to interferences with the right to privacy, most notably by storing data centrally, create the technical infrastructure to conduct surveillance in a generalised manner. Leaving this potential unaddressed in the legislative act creates the risk that the essence of the right to privacy will be compromised in the quasi-legislative phase. Generalised interferences with the right to privacy belong to the realm of authoritarian regimes and have no place in the EU legal order with its evolved commitment to human rights protection.

[246] SEC (2011) 567 (n 142) 18

[247] *Hatton and Others v The United Kingdom* (n 218) para 97. *López Ostra v Spain* (n 37) para 55.

[248] Article 52(3) of the Charter. This is further reinforced by the Commission's own duties in the legislative process, see Chapter 4, section 3.

Chapter III
Data protection in the EU legal order

1. Introduction

Data protection is a relatively young right, which gradually originated in the seventies in Germany, Sweden and France. [1] In the German federal state of Hesse an act was adopted in 1970 under the name 'Datenschutz'.[2] Illustrative for this early adoption and the rationale of data protection is that Hesse was in fact heavily promoting the automatic processing of personal data by public authorities.[3] After the OECD issued its Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data in 1980, the Council of Europe followed its lead in 1981 after years of preparation with the adoption of Convention 108.[4] There is no doubt that, under the legal framework introduced by the CoE, data protection was inspired by concerns over the right to privacy, but also the wish to legitimise the processing of personal data. Data protection matured into a body of rules with its own scope, principles, limitations, duties and enforcement mechanisms. The complexity of data protection and its scope is conditioned among others by the multiplicity of sources regulating this issue. In the European context, the most known legal instruments dealing with data protection are the ECHR (on a case-to-case bases), Convention 108, Directive 95/46/EC (hereinafter 'Directive 95/46/EC'),[5] General Data Protection Regulation (hereinafter 'GDPR')[6] and Article 8 of the Charter which creates

[1] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 21.

[2] ibid.

[3] Hessische Staatskanzlei (1970) 41 Gesetz- und Verordnungsblatt für das Land Hessen, Teil I 625.
Original text can be found at starweb.hessen.de/cache/GVBL/1970/00041.pdf. Perhaps parallel is the claim of privacy scholar David Wright that Australia, Canada, Ireland, New Zealand, the UK and the US have the most experience with Privacy Impact Assessments. Coincidentally or not five out of six of these countries belong to the Five Eyes, an alliance of national intelligence agencies responsible for global privacy breaches on an unprecedented scale. For the claim on the PIA and these countries see
David Wright, 'Making Privacy Impact Assessment More Effective' (2013) 29 The Information Society 307, 307.

[4] 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No 108' (Strasbourg, 28 January 1981).

[5] 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 [1995] OJ L281/31.The other directive that is 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 (Directive on privacy and electronic communications) [2002]OJ L201/37 is not included in this chapter. The focus of this thesis is on the design of IoT systems.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] L119.

a fundamental right to the protection of personal data.[7] This chapter examines the sources, which are most relevant to IoT policy, including Directive 95/46, the GDPR and Article 8 of the Charter.[8]

The Commission has proclaimed that individuals have the right to enjoy effective control over their personal information in the new digital environment, positioning data protection as the legal tool for attaining such control.[9] Moreover, in the Action Plan on the Internet of Things the Commission vows to monitor the application of data protection legislation without mentioning the right to privacy.[10] The underlying rationale seems to be that data protection legislation is adequate in dealing with privacy concerns raised by the IoT vision. The relationship between the right to privacy and data protection legislation is unclear. This is relevant, because if the two were synonymous, then the Commission's focus on data protection would not raise a problem. However, if the scope and limitation requirements of the two differ, the singular focus of the Commission on data protection results in negligence of its task as the guardian of fundamental rights.

The aim of this chapter is to establish the scope of the Directive 95/46/EC, the relevant changes introduced by the GDPR and the fundamental right to the protection of personal data under Article 8 of the Charter.[11] In addition, it will examine the subject and the mechanism of protection and limitations established in these instruments. Furthermore, the chapter explores the essence of Article 8 of the Charter, which is the right to the protection of personal data. This discussion is necessary to determine the legislative requirements to be taken into account by the Commission in the preparatory phase of legislation that mandates the installation of IoT systems, drafting legislative proposals and the legislation-making process including the delegated acts. Attention will be given also to the relationship between data protection legislation and the right to privacy in the case law of the CJEU.[12] The ultimate goal is to reach an informed conclusion about the distinctions in the requirements following from data protection legislation, as opposed to the right to privacy.

[7] This has, arguably, lead to the 'constitutionalisation' of data protection, see Paul de Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection* (Springer 2009).

[8] Article 8 of the Charter contains the right to the protection of personal data. When I will refer to data protection under the EU directives I will refer to it as secondary rules on data protection or secondary data protection legislation. When I refer to the Charter as well as the directives I refer to data protection legislation.

[9] Commission, 'Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century' COM (2012) 9 final 2.

[10] Commission, 'Internet of Things – An action plan for Europe' (Communication from the Commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions COM (2009) 278 final.

[11] I will refer to the Directive 95/46/EC and the GDPR as 'secondary data protection legislation'.

[12] This will be discussed in section 2.2 and 2.3

2. The legal regime of Directive 95/46/EC and the GDPR

Data protection is regulated in a number of directives and regulations, the most relevant of which are Directive 95/46 and the GDPR as noted above. The ambivalent aim of Directive 95/46 is captured in the following paragraphs of its first Article:[13]

> '1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.'

This is preceded by the first recital which emphasises the importance of eliminating 'the barriers which divide Europe' in order to obtain economic and social progress, improving living conditions of its people, 'preserving and strengthening peace and liberty and promoting democracy on the basis of fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms'. The language of Directive 95/46 reflects the intention of the legislature to reconcile the objectives of the EU (then EC) to realise the internal market by removing national obstacles to the free flow of personal data and at the same time to offer some degree of protection for the fundamental rights and freedoms of natural persons, in particular their right to privacy.[14] The phrasing implies an intention to strike a balance between the interests of personal data processing parties and the interest of data subjects to have their fundamental rights respected. The CJEU confirmed this in a number of cases in which it held that the objective of the Directive is 'maintaining a balance between the free movement of personal data and the protection of private life'.[15] Data protection within the EU legal order, therefore, can be understood as a balancing exercise between conflicting interests.[16] The metaphor of 'balancing' places fundamental rights on par with the interests of parties seeking to process personal data. The legal basis for Directive 95/46, Article 100a TEC,[17] suggested that market interests prevail over fundamental rights. The means by which the Directive seeks to establish an internal market for the processing of personal data is by

[13] This recurs in slightly different wording in the GDPR.

[14] Although it could be argued that the initial idea behind data protection was to regulate cross-border flows of personal data, the CJEU has repeatedly held that the applicability of the directive does not depend on a direct link with the exercise of the fundamental freedoms and that the essential objective of the directive is 'approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislations'. In defense of this position it pointed out that the wording of Article 3(1) of the Directive, which sets out the scope, does not make the application of its rules dependent on the cross-border element. Case C-195/06 *Österreichischer Rundfunk (ORF)* [2007] ECR I-08817, paras 42 and 43.

[15] Case C-101/01 *Lindqvist* [2003] ECR I-12971, para 97. Repeated in Joined cases C-468/10 and C-469/10 *Asnef* [2011] ECR I-12181, para 34. See also Recital 5 Directive 95/46 and Recital 6 GDPR.

[16] Now officially recognised under Recital 4 GDPR.

[17] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47, art 114.

harmonising its protection in all Member States, so that fundamental rights cannot be invoked by public or private actors to restrict the cross-border processing of personal data.[18] Article 100a TEC (currently Art 114 TFEU) is a legal basis for adopting measures which aim to facilitate the establishment and functioning of the internal market.[19] Data protection legislation and the internal market considerations coincide. This logic was already evident under the OECD guidelines and copied in the Convention 108.[20] This demonstrates that the centre of gravity of the Directive is towards the economic dimension, rather than the human rights dimension. This was confirmed by the CJEU, which held that the Directive has as 'its principal aim to ensure the free movement of personal data'.[21] The primary aim of the Directive is therefore economic in nature, despite the grandiloquent wording of the second recital: '[w]hereas data processing systems are designed to serve man…' The question at stake is: which man?[22]

At the time the Directive was adopted there was no legal basis available to the EU legislator that was tailored more to data protection. The post-Lisbon TFEU has provided a new legal basis in this area, which has been used in the adoption of the GDPR. Article 16 TFEU provides that the Council and the EP acting through the ordinary legislative procedure can adopt legislation in the field of data protection. In combination with the adoption of the right to the protection of personal data as a fundamental right, it could be argued that using Article 16 as a legal basis suggest that the primary aim has shifted to the protection of this fundamental right. The first provision of the GDPR, however, continues to place the protection of personal data and the free movement of personal data on par.[23] The first recital provides that the protection of natural persons in relation to the processing of personal data is a fundamental right under the Charter, but the overall structure of the GDPR is similar to the Directive. What might be termed as the 'prohibitive potential' of data protection law, thus, has not changed fundamentally. On the contrary, there is evidence that the GDPR provides more elbowroom for governments seeking to expand their informational power.[24]

Data protection legislation is used to facilitate and legitimise the processing of personal data, under a given set of rules and safeguards, providing subjective rights to individuals and setting up an independent watchdog monitoring the application of these rules. Although this is an important function of data protection legislation, it disregards the individual who might not wish his data to be recorded in the first place, let alone collected and 'protected' by a

[18] Recital 8 and 9 of Directive 95/46/EC. The level of harmonisation which the Directive aims to establish is a contested issue. The eighth recital expresses the goal of 'equivalent' protection and the tenth complements this aim by stating that the approximation of laws must not result in any lessening of protection 'but must, on the contrary, seek to ensure a high level of protection in the Community'. The CJEU has held repeatedly that the aim of the Directive is not minimal harmonisation, but harmonisation which is 'generally complete'. Case C-524/06 *Huber* [2008] ECR I-09705, para 51; Case C-101/01 *Lindqvist* (n 15) para 96.

[19] Case C-376/98 *Germany* v *Parliament and Council (Tobacco Advertising I)* [2000] ECR I-8419.

[20] Fuster (n 1).

[21] *Österreichischer Rundfunk* (n 14) para 70.

[22] In the GDPR the legislature replaced the word 'man' for 'mankind'.

[23] Article 1 GDPR.

[24] This will be further discussed in section 2.3.

party which is supposed to be entrusted with his personal data. It is here that the first and most fundamental objection is raised to the contention that data protection is suitable to protect the right to privacy: the privacy of the individual is best served when he is left with the choice whether personal data is recorded and collected[25] in the first place, before it is stored and used by one or more parties he is forced to trust with the control over his data.

Whether Convention 108, and Directive 95/46 which was inspired by it, have ever sought to protect this particular interest of the individual is subject to debate. European institutions took an interest in adopting data protection legislation, because there was a need to regulate the processing of personal data through the use of computers. Both legal instruments were heavily inspired by the 'Fair Information Practice Principles', developed in 1973 by a US government advisory committee and primarily aimed at facilitating data processing.[26] Although the Convention and the Directive may have placed greater emphasis on the right of the individual in comparison with the US, both instruments assist the parties seeking to process personal data for their own purposes, i.e. in the interest of data controllers.[27] To quote the highly crystalized thoughts of Gloria Gonzáles Fuster on this matter:

> '…. [Convention 108] incorporated the 'data protection' terminology while redefining its meaning. It designated 'data protection' as corresponding to the respect of rights and fundamental freedoms, in particular the right to privacy,[28] and concretized it in rules profoundly indebted to the 'fair information practices' doctrine. Thus, it inscribed in international law, and indirectly in the national legal orders of the many countries party to the Convention, the idea that 'data protection' serves privacy, and contributed to the understanding of this idiom has carried a permissive dimension. In 1995, Directive 95/46/EC imported into EU law, directly from Convention 108, the formula according to which 'data protection' serves privacy.[29]'

Compared to the scope of the right to privacy, the following observations can be made. On the one hand, the secondary rules on data protection are only applicable to the *processing of personal data* and, therefore, are much narrower than the right to privacy. On the other hand, data protection is broader, because it covers the processing of personal data that does not, or not yet, constitute an interference with the right to private life and, hence, falls outside of the scope of Article 7 of the Charter. The following sections will focus on the most relevant and

[25] It should be noted that the term collection suggests that the data is already there. When I use the term 'collection', this also implies the recording of the data. Yet, it is important to keep in mind that the first step to the interference with the right to private life is the recording of data, because data by its nature is susceptible for collection. With the risk of becoming repetitive: if there is no data, there is nothing to collect. Therefore not *recording* data is the best way to preserve privacy. The ultimate PET to implement in an IoT system is to avoid the recording of personal data.

[26] The term itself was inspired on the Code of Fair Labor Practices. The equivalence, according to the inventors of the name, between the terms (personal) 'information' and 'labor' can be read as an indication that the underlying ratio is to permit the processing of information and not to prohibit it.

[27] Fuster (n 1) 78.

[28] Original fn is number 37: 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No 108 (Strasbourg, 28 January 1981), art 1.'

[29] Original fn is number 38: 'Art. 1(1) of Directive 95/46/EC.'

problematic aspects in relation to the design of IoT systems: the processing of personal data, the data protection principles, the grounds for processing and the rights granted to the data subject. Section 2.5 considers the shifting of the centre of gravity from the right to privacy under Directive 95/46/EC to the right to the protection of personal data under the GDPR. In the final section, the differences between the scope and requirements of the right to privacy and secondary data protection legislation are established and the implications for IoT systems discussed.

2.1 The processing of personal data

Since processing consists of basically any possible action regarding data the main criterion to decide if processing falls under the material scope of the Directive and GDPR is whether the data qualify as *personal*. It should be noted that the Directive was drafted at a time when the IoT was non-existent, but the freshly adopted GDPR did not alter the definition. Both provide that processing 'means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation…..'.[30] This wording implies that the data are already there. Although it can be argued that 'recording' (and even 'collection') implies that data are generated, data protection legislation intends to be applied in a way that the necessity of the initial recording of personal data is not questioned. This is the first phase of data processing which needs to be questioned to realise an IoT system according to the concept of Privacy-by-Design.

Personal data 'means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[31] The notion of personal data can be broken down into four elements: 'any information', 'relating to', 'an identified or identifiable', 'natural person'.[32] The element that raises the most questions is 'identified or identifiable'. If the information relates to an identified person, it is clear that this is personal data. If the person is only identifiable, the question is whether the person is directly or indirectly identifiable. An example of an identifier that allows direct identification is an identification number. Recital 26 provides that for the question whether a person is identifiable 'account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'. Article 29 WP indicated that the key question is

[30] Article 4(2) GDPR.

[31] Article 4(1) GDPR.

[32] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (Adopted on 20th June 01248/07/EN WP 136, The Article 29 Working Party 2007) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 6 June 2018.

whether it is possible to uniquely single a person out, even if the name is not known.[33] Consequently, it qualifies IP addresses as personal data when dealt with by ISPs[34] and search engines.[35] The CJEU explicitly subscribed to this view, when it confirmed in *Scarlet Extended* that IP addresses were personal data for ISPs. This judgment hinged on the fact that IP addresses could be linked to individuals by ISPs. The CJEU held that these addresses 'are protected personal data, because they allow those users to be precisely identified'; by ISPs that is, which know what address belongs to which name.[36] In a later case of *Breyer*, the question was more complicated as the party receiving the IP addresses was an 'online media service provider', which did not have direct access to the information linking individuals to IP addresses.[37] Here, the Court held relevant that 'legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider'.[38] Indirect identification can be realised when multiple pieces of information are combined to narrow them down to one person. Each of these pieces of information might not be traceable to a particular individual, yet with a combination of these pieces, identification becomes possible. MIT researchers conducted investigations into mobile phone data and credit card data, which showed that with respectively three and four data points they could single out 95% of the individuals out of a crowd of over a million.[39] It might be unjustified to completely exclude such data from the scope of data protection regulation.[40] Anonymisation should, therefore, be critically reviewed. Whether a person is identifiable is highly circumstantial and with the offset of *big data*, where numerous data sets are combined, anonymisation becomes increasingly difficult.

2.2 Data protection principles

The data protection principles have a long history starting in the OECD Guidelines and recurring in each piece of data protection legislation adopted after that in the EU. A number

[33] Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising' (Adopted on 22 June 2010 00909/10/EN WP 171, The Article 29 Working Party 2010) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 6 June 2018.

[34] By which they presumably mean *access providers*.

[35] Article 29 Data Protection Working Party, 'Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)' (adopted on 15 May 2008 00989/08/EN WP150, The Article 29 Working Party 2008) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp150_en.pdf> accessed 6 June 2018, 6.The criterion of singling out has been included in Recital 26 of the GDPR as one of the means to be used to identify a natural person.

[36] Case C-70/10 *Scarlet Extended* [2011] ECR I-11959, para 51.

[37] Case C-582/14 *Breyer* ECLI:EU:C:2016:779.

[38] ibid, para 47. The CJEU referred to this as an 'objective criterion' as opposed to a 'relative criterion'.

[39] See Yves-Alexandre de Montjoye and others, 'Unique in the Crowd: The privacy bounds of human mobility' (2013) 3 Scientific Reports <doi:10.1038/srep01376> accessed 1 October 2015 and Lenny Hardesty, 'Privacy challenges Analysis: It's surprisingly easy to identify individuals from credit-card metadata' <http://news.mit.edu/2015/identify-from-credit-card-metadata-0129> accessed 15 October 2015.

[40] Chapter 4, section 2.2.

of these principles have, in relation to IoT systems, a prohibitive potential. This means that in their interpretation and application they can stop the EU legislature from equipping IoT systems with surveillance features, consisting in the processing of personal data, which are not strictly necessary. This section limits itself to the principles with a prohibitive potential: [41]

> '(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

When the controller has a ground to process the data, this processing has to comply with the 'Principles relating to data quality' under the Directive, which were renamed 'Principles relating to processing of personal data' under the GDPR. These are the most substantive principles within data protection law, which, similar to the grounds for processing, were given direct effect in the CJEU's case law.[42] The relevance of this lies in the fact that citizens in EU countries can directly invoke these principles before a national court and that direct effect accorded to them indicates that these criteria are clear, unconditional, contain no reservation on the part of the Member State and are not dependent on any national implementing measure. The principles under subparagraph (a) and (b) reflect the privacy principles of the OECD.[43] All three coincide with the basic principles for quality of data enshrined in Article 5 of Convention 108.

The *'fairness'* principle implies transparency of the processing and that the interests of the data subject and the controller need to be balanced.[44] '*Lawfulness'* implies that data processing which falls under the scope of other laws must also adhere to these, such as Article 8 ECHR.[45] The purpose specification principle is one of the cornerstones of data protection.[46] Specifying the purpose is important to comply with a number of other rules. The specified purpose reappears in the obligation of the controller to inform the data subject on the purpose of the processing and with regard to the controllers' obligation to notify the

[41] The principles of 'accuracy', 'storage limitation' and integrity and 'integrity and confidentiality' are not discussed, because they see to the processing of data after the initial recording and collection of personal data by the IoT system.

[42] *Österreichischer Rundfunk* (n 14)

[43] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980.

[44] Paul de Hert and Serge Gutwirth, 'Consent, Proportionality and Collective Power' in Serge Gutwirth and others (eds), *Reinventing Data Protection* (Springer 2009), 162.

[45] This means, amongst others, that a data processing operations which fall under the scope of Article 8 ECHR must also meet the requirements as set out in its second paragraph.

[46] Serge Gutwirth, *Privacyvrijheid! De vrijheid om zichzelf te zijn* (Rathenau 1998) 114.

supervisory authority of the processing (replaced in the GDPR by a record of the processing in which the purpose is one of the things to be registered). The purpose can be retrieved by the data subject when he exercises his access right, as well as his right to object to data processed by the controller for the purpose of direct marketing. This list is not exhaustive, but shows the centrality of the principle. The specification of the purpose has to be understood in the light of the processing operation, and provides transparency to the data subject regarding the scope of the processing.[47] The controller has to be explicit in its wording, which means the purposes have to be clear and expressed in an intelligible form.[48] These requirements serve transparency. The last requirement of purpose specification is legitimacy. According to the Article 29 WP this means it has to be in accordance with the law in the broadest sense.[49] The purpose specification principle, furthermore is central to the application of a number of data protection principles, since these cannot be tested without articulating the purpose. The counterpart of the purpose specification principle of the right to privacy is the requirement to pursue a legitimate aim. Since this requirement is met with relative ease, purpose specification, and thus secondary data protection legislation, sets higher standards regarding the qualification of the aim the interference serves. After the initial collection of the data, the specified purpose becomes important in the determination whether *further processing* of data is compatible with the original purpose. This concept of 'compatible use' in conjunction with the purpose specification principle is referred to in the Article 29 WP as *purpose limitation*.[50] Respecting the purpose limitation principle serves the protection of individuals against secondary use of data, as confirmed by the Article 29 Working Party:

> 'It should be kept in mind that processing of personal data has an impact on individuals' fundamental rights in terms of privacy and data protection. This impact on the rights of individuals must necessarily be accompanied by a limitation of the use that can be made of the data, and therefore by a limitation of purpose. An erosion of the purpose limitation principle would consequently result in the erosion of all related data protection principles.'[51]

When further processing is compatible with the original purpose, the controller does not need the consent of the data subject for this operation. This notion conflicts with the idea of informational self-determination, understood as the idea of informational autonomy with

[47] The purpose and the identity of the controller are communicated to the data subject on the basis of Article 10 Directive 95/46/EC.

[48] Article 29 Data Protection Working Party, 'Opinion 03/2013 on purpose limitation'(Adopted on 2 April 2013 00569/13/EN WP 203, The Article 29 Working Party 2013) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf > accessed 6 June 2018 17

[49] ibid 20.

[50] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (adopted on 9 April 2014 844/14/EN WP 217, The Article 29 Working Party 2014) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 6 June 2018, 11. In her opinion in Case C-275/06 *Promusicae* [2008] ECR I-00271 AG Kokott found that the requirement of foreseeability has found 'particular expression' in the principle of *purpose limitation* as laid down in Article 8(2) of the Charter. Article 8(2) does not contain the concept of compatible use, only purpose specification.

[51] WP 203 (n 48) 14-15.

limited statutory exceptions and provides a margin of discretion to the controller. Article 6(4) GDPR provides the following key considerations in the assessment of the compatibility:[52]

> (a) 'any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
>
> (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
>
> (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
>
> (d) the possible consequences of the intended further processing for data subjects;
>
> (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.'

The aim of these considerations is to give a measure of flexibility to the data controller to further process data, whilst still protecting the privacy interests of the data subject. However, the principle of further processing also introduces further uncertainty with respect to the control of the data subject. A wide application of this principle would clearly water down the very controls that data protection law introduces through the principle of purpose specification. Purpose limitation can be seen as a specific expression of the requirement of *foreseeability*.[53] Foreseeability in the context of the ECHR requires clear and precise criteria for the government to resort to surveillance measures in order to prevent their arbitrary application. The purpose, in the form of 'nature of the offences', is only one of the categories expressed in ECtHR case law.[54] Foreseeability also limits the categories of people liable to have a surveillance measure deployed against them. Data protection law generally does not differentiate between the categories of people who can have their data processed. Data protection law facilitates indiscriminate processing of data by administrations as well as businesses, as long as the processing complies with the rules provided by the GDPR. The purpose limitation principle does impose stricter rules on the breadth of the purpose formulation in comparison with the right to private life. In practice, however, purposes are formulated broader than the law allows.[55] Purpose limitation can also be weakened by formulating a wide range of purposes. Another significant difference is that purpose limitation is applied by the controller as opposed to the legislator. It only takes one look into privacy policies on the web to see how poor they perform this task. The baroque complexity

[52] These were inspired on the key considerations provided for in the WP 203 Opinion, but also the Dutch delegation appears to have had a say in this. These considerations are similar to the ones provided for in the Dutch data protection law (Article 9(2) Wet bescherming persoonsgegevens), the implementation of Directive 95/46/EC.

[53] Case C-275/06 *Promusicae* [2008] ECR I-00271, Opinion of AG Kokott, para 53.

[54] See Chapter 2, section 3.1

[55] There are countless (tech)companies that formulate purposes such as ' to improve users experience' or 'marketing purposes'. These purposes, in exactly these words, are indicated as too broad by the Article 29 Working Party in their opinion on purpose limitation (*WP 203*). It therefore seems that this rule is ill-enforced.

in which controllers express their privacy policies, often following the advice of their lawyers, has been found to create 'consensual exhaustion, laxity and apathy'.[56]

The third principle limits the amount and kind of data the controller is allowed to process: it has to be adequate, relevant and necessary in relation to the purpose. Under Directive 95/46, the data had to be 'not excessive', which was replaced by 'necessary' in the GDPR. The gradual adoption of the aforementioned principle of *data minimisation* in the vocabulary of the CJEU, the Commission, EDPS and Article 29 WP,[57] as well as by numerous authors, showed an increasing acceptance of this principle.[58] This was consolidated finally in the GDPR where the principle of data minimisation was awarded a place amongst the other core data protection principles.[59] Despite the weakening of the wording in the final version, the aim of data minimisation is still straightforward: to process the minimum amount of data in order to achieve the purpose.

The high frequency with which the proportionality principle recurs in the Directive raises questions about the way it should be applied, in particular whether a strict or a loose approach should be adopted. Whether these principles taken together will curb the surveillance potential of IoT systems introduced through EU law depends on the way they are applied. Gellert and Gutwirth argue that, contrary to the strong normative test of the ECHR, the 'nature, content, and meaning of the proportionality test embedded in Art. 6.1(a) and 6.1(c) is still very much disputed.'[60] These principles are not interpreted and applied in a vacuum, and given that they express the proportionality principle, the same factors taken into account by the CJEU and ECtHR when they interpret this principle should be leading in their interpretation of data protection legislation.

The CJEU held on numerous occasions that the provisions of Directive 95/46, governing processing of personal data jeopardising the right to privacy, must be interpreted in the light

[56] Lee A Bygrave and Dag Wiese Schartum, *Consent, Proportionality and Collective Power*, 161 in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009).

[57] Commission, 'Delivering an area of freedom, security and justice for Europe's citizens: Action Plan Implementing the Stockholm Programme' (Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2010) 171 final.

[58] Article 29 Data Protection Working Party, 'Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector' (Adopted on 27 February 2014 536/14/EN WP 211, The Article 29 Working Party 2014) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf > accessed 6 June 2018, 16.

[59] This principle was formulated stronger at first: 'personal data must be adequate, relevant, and limited to the minimum necessary in relation the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data.' This formulation expresses a view on data protection that can also in a specific application amount to data avoidance. The final formulation deviates: 'adequate, relevant, and limited to what is necessary in relation the purposes for which they are processed ('data minimisation').

[60] Raphaël Gellert and Serge Gutwirth, 'The legal construction of privacy and data protection' (2013) 29 Computer Law & Security Review 528.

of fundamental rights.[61] This was relevant for the way Article 13 of the Directive should be applied, which allows member states to adopt legislative measures that restrict the scope of Article 6(1) Directive 95/46 to safeguard a number of public interests similar to the ones mentioned in Article 8(2) ECHR, which can be viewed as its privacy-counterpart.[62] A measure which consists of the processing of personal data for these purposes which interferes with the right to private life must still adhere to the demands set out in Article 8(2) ECHR. The CJEU held that the applicability of Article 8 (2) required the national courts to view whether the aim pursued could not be attained by processing less data, thereby applying a strict proportionality test in order to find the least infringing alternative.[63] The CJEU held that if the national court found that the national legislation was incompatible with the second paragraph of Article 8, this automatically implied that it could not satisfy the demand of proportionality as laid down in Article 6(1)(c) and 7 (c) or (e) of Directive 95/46/EC(§ 91), thereby implicitly arguing that the proportionality test that follows from the ECHR is similar to the one that follows from Directive 95/46/EC and emphasising the importance of executing the necessity subtest, i.e. finding the least infringing alternative.[64] This interpretation implies that the government cannot make exceptions through data protection law to the requirement to limit the processing of personal data to the minimum necessary to attain a specific objective, because this is one of the requirements provided in the ECHR; neither the Member State legislature, nor the EU is allowed to make exceptions to these requirements. The context in which the installation of IoT systems is mandated, by EU law and in the private sphere of the data subject, calls for a strict application of the proportionality principle.

When the protection offered by the GDPR coincides with the protection that follows from Article 8 ECHR and Article 7 of the Charter, the case law of both the CJEU and the ECtHR should be followed, meaning that the proportionality-test must be calibrated in accordance with the factors established by both of them.[65] Moreover, in further case law the Court established that Member States should not interpret secondary legislation in conflict with the fundamental rights protected by the EU legal order, an instruction which extends to the work of the Commission.[66] In the context of legislation which introduces mandatory IoT systems, this case law holds particular importance for the execution of the data protection impact assessment and the subsequent choices the legislature needs to make with respect to the design of the system. These design choices must follow from the assessment of the necessity

[61] *Österreichischer Rundfunk* (n 14) para 68. Repeated in Case C-131/12 *Google Spain* EU:C:2014:317, [2014], para 68; Case C- 362/14 *Schrems* EU:C:2015:627, [2015], Opinion of AG Bot, para 99.

[62] On a sidenote, Article 13 holds that these measures must be necessary to safeguard these interests, implicitly demanding that they must be proportionate.

[63] *Österreichischer Rundfunk* (n 14) para 88. Other authors also argue that the principle of proportionality and its three sub-principles – suitability, necessity and proportionality in a narrow sense (stricto sensu) – correspond closely to the principles of data protection law. Bygrave and Schartum (n 56) 162.

[64] This reasoning implies that the Court holds the right to privacy to be the root of Directive 95/46/EC. The criteria from Article 6 also serve to further calibrate the balancing exercise from Article 7(f). This can be found in *Google Spain* (n 61) para 93.

[65] Chapter 3, section 2.3 and section 3.2.

[66] *Schrems* (n 61) para 100; Joined cases C-411/10 and C-493/10 *N S and Others* [2011] ECR I-13905, para 77 and the case-law cited (including *Lindqvist* (n 15) para 87).

of the initial recording and collection of personal data, since this marks the starting point of the interference with the rights protected under Article 8 ECHR and Article 7 of the Charter. Secondary data protection law contains substantive principles forming an expression of some of the requirements to lawfully limit the right to privacy, but there are important differences. There is no need for a basis in the law, and the requirement of foreseeability is only reflected to a very limited extent. There are requirements of proportionality and necessity, and even stricter requirements for specifying the purpose, but there is no such thing as the assessment of a 'pressing social need'. The more value-laden categories like the *interest to be protected from the interference* and *the nature of the interference,* which play a role in the case law of the ECtHR, are not explicated in data protection law. These can and should, however, resurface when data protection law is interpreted and applied in line with the case law of the ECtHR and CJEU on the right to privacy.

The case law of the courts may hint towards a strict proportionality test, nevertheless there is reason to be sceptical about the willingness of controllers to take this view to the heart. The controller is the party which determines the means and the purposes of the processing of personal data, has the responsibility to bring this processing in line with the aforementioned principles. Loose appliance of these principles will result in wider freedom for the controller to process personal data. The application of these principles does not happen in isolation, but within a socio-economic context, which provides multiple markets for personal data. Given this monetary value of data in today's data driven economy, controllers have a strong incentive to apply these principles loosely, or even disregard them completely.[67] Controllers tend to apply them as guidelines or soft law in the spirit of commerce, rather than strict rules in the spirit of human rights. Supervisory authorities of Member States are responsible for monitoring and enforcing the application of data protection law on their respective territories. Data protection regulation can be viewed as a particular modus of co-regulation, which works fine when the stakes are low. If data protection requirements which correspond to the requirements from the right to privacy are loosely applied within the standard setting process of IoT systems, they can legitimise design choices which (risk to) interfere with the right to private life.

In addition, data protection laws are generally not well-known by the parties executing their provisions.[68] This tendency of controllers is similar to the non-compliance bias of ESOs towards data protection.[69] Data protection legislation does not apply to ESOs directly and the Commission does not seek to remedy this legal vacuum in relation to ESOs.[70] Instead it merely considers the need for rules to be taken into account.[71]

[67] Deborah A DeMott, 'Organizational Incentives to Care about the Law' (1997) 60 (4) Law and Contemporary Problems 39. For a bit more tendentious account on the corporate mindset see the documentary: Big Picture Media Corporation, 'The Corporation' (2003).
[68] Bygrave and Schartum (n 56).
[69] See Chapter 4, section 4.3.
[70] Chapter 4, section 4.3.
[71] Commission, 'Promoting data protection by privacy-enhancing technologies (PETs)' (Communication from the Commission to the European Parliament and the Council) COM (2007) 228 final 7.

2.3 Grounds for processing

The controller has to establish on what ground(s) data will be processed. This is also referred to as the principle of lawfulness and can be viewed as data protection's counterpart for the legal basis required for interferences with qualified human rights.[72] This is referred to in Directive 95/46 as 'Criteria for making the processing legitimate'. Under the GDPR it is listed as the 'Lawfulness of processing'. There are six grounds listed in Article 6:

a) 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

These grounds provide a legitimate basis for the processing of personal data and have direct effect under the Directive.[73] This implies that citizens of Member States can rely on them directly before a national court. It also implies that the content of these provisions can be determined with sufficient precision. There is no hierarchy among the grounds and the order is therefore not to be considered an indication for this.

The use of the term 'necessary' implies that the processing should be proportionate in relation to the ground. The CJEU determined that the purpose of the concept 'necessary' in relation to the public interest is to 'delimit precisely one of the situations in which the processing is lawful'.[74] The Article 29 WP refers to the case law of the ECtHR for guidance on the concept of 'necessary', discussed in the previous chapter.[75] The only ground where the necessity requirement is missing is the data subject's unambiguously given consent, which is irrelevant in the context of mandatory IoT systems. Although it could be argued that this means that the demands that follow from necessity do not have to be met when consent is given, data processing also has to comply with other relevant laws, such as Article 8 ECHR. Of course, not all processing of personal data raises an issue under Article 8 ECHR, but it is likely that

[72] It does not provide the quality of law-requirements of accessibility and foreseeability, which return in the next section on principles related to data quality.
[73] This can be concluded from *Asnef* (n 15), in which the Court held that 7(f) has direct effect.
[74] *Huber* (n 18) para 52.
[75] WP 217 (n 50) 11.

disproportionate processing of personal data will do so, because the disproportionality will make it less likely that the processing can be legitimised.

The grounds that can be invoked will depend on the party determining the purposes and means of the processing. The GDPR provides that 'where the purpose and means of such processing are determined by Union or Member State law, the controller or the specific criteria for nomination may be provided for by Union or Member State law'.[76] Processing for compliance with a legal obligation or for a task carried out in the public interest should be laid down in Member State or Union law.[77] It would be logical if this is the law introducing the IoT systems. If these systems provide the possibility to process data for interests of private parties, such as third party service providers, the processing can take place on a contract or in the legitimate interest of the controller or third party. The latter is a complex and controversial ground, since it enables the fundamental right of the data subject to be outweighed by the interest of the controller. The ground is formulated in a way that the interest of the controller is taken as the rule and a possible invocation of a fundamental right as the exception. This shows how the human rights rationale — in which the respect for the right is the rule and the interference is the exception — is turned upside-down in data protection legislation. In practice, this means that a company's interest to process personal data for profit can be accorded more weight than a person's right to privacy.[78] The GDPR even made it explicit that the 'processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest'.[79] An example of the exception can be found in the case of *Google Spain*:

> 'Application of Article 7(f) thus necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter.'[80]

The outcome of the balancing exercise depends on the weight accorded to the opposing interests, which Article 29 WP ranged from insignificant to compelling.[81] Taking into account the significance of the rights arising from the right to privacy, the balancing test should be informed by the case law of the ECtHR. Very similar to this are the 'key factors' as set out by Article 29 WP, which are the following: the controller's legitimate interest, the impact on data subjects, the provisional balance and additional safeguards applied by the controller. On the one side of the balance, there is the legitimate interest of the data controller. The weight accorded to this interest depends on the nature of this interest (whether it falls under the exercise of a right and the type of right), is the processing necessary and proportionate and whether there is a public interest served with the processing.[82] This is

[76] Article 4(7) GDPR.
[77] Article 6(3) GDPR.
[78] Federico Ferretti, 'Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?' (2014) 51 CMLRev 843.
[79] Recital 47 GDPR.
[80] *Google Spain* (n 61) para 74.
[81] WP 217 (n 50) 34-36.
[82] WP 217 (n 50) 30.

similar to the requirements for an interference with the right to privacy. On the other side of the balance is the impact on the data subject. The potential effects of the processing, the risks for the data subject associated with the processing (including their likelihood and severity when materialised), the nature of data, the way they are processed, the reasonable expectations of the data subject and the status of the data controller and the data subject are all to be taken into account when assessing the impact. [83] This is similar to the factors relevant to establish the severity of the interference with the right to privacy. Under 'additional safeguards applied by the controller', safeguards from within and outside the Directive are mentioned, such as:

- 'technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individual ("functional separation" as is often the case in a research context)
- Extensive use of anonymisation techniques
- Aggregation of data
- Privacy-enhancing technologies, privacy by design, privacy and data protection impact assessment
- General and unconditional right to opt-out.'[84]

When this ground is used to legitimise the processing of data by an IoT system, the existence of additional safeguards and the extent to which the controller utilises them, as well as the existence of privacy-friendly alternatives to a chosen design, are all relevant for the balancing test. The subtest of necessity from case law regarding the right to private life, in other words the requirement for the least infringing alternative in privacy case law, finds its counterpart at this point in data protection law.

The radical reframing of purpose limitation under the GDPR

In the trilogue between the Council, European Parliament and the Commission, the Dutch delegation pushed for a few significant changes in the text of the GDPR. These allow the EU and national legislators to adopt laws which 'adapt' the substantive rules provided by the GDPR. Article 6(3) provides a non-exhaustive list of these rules, amongst which rank 'general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures'.[85] This discretion is, therefore, sweeping. According to the last sentence of Art 6(3):

[83] ibid 36-41.This shows an interesting similarity with the Commission's impact assessment in which the likelihood and magnitude (instead of severity) of the impact are used to establish its importance.
[84] ibid 42.
[85] Ard van der Steur, then Minister of Justice and Security, told this in a letter to Dutch parliament. Tweede Kamer, Kamerstukken II [2015-2016] 32 761 no 91, 2.

> 'The Union or the Member State shall meet an objective of public interest and be proportionate to the legitimate aim pursued.'

The contrast is evident. Article 6(3) provides the power to the legislator to 'adapt' the rules of the GDPR. The Dutch government has already uttered the ambition to base laws on a broad, rather than a narrow notion of purpose limitation, to adopt framework legislation allowing collaborations between public authorities transcending single policy areas, involving parties concerned with administrative law, criminal law and private parties such as companies.[86] If such an approach results in a wide consolidation of informational power held by the government, purpose limitation is transformed into something it was never meant to be. Purpose limitation is not a standalone principle, but relates to principles of constitutional and administrative law, such as foreseeability and abuse of competence (détournement de pouvoir).

Furthermore, Recital 50 and Article 6(4) of the GDPR allow for Member States to adopt legislation enabling further *systematic* processing of personal data incompatible with the original purpose. Under Directive 95/46/EC, this was only possible in exceptional cases and on the basis of a law.[87] Recital 50 provides that such processing can also be done by a controller in 'individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority' and this 'should be regarded as being in the legitimate interest pursued by the controller.' This creates a legal basis for private as well as public data controllers to further process data and send this to public authorities. It also bears resemblance to the discussions in the *Future Group*, in which the digital trails created by citizens were foreseen as valuable input for 'more effective and productive public security efforts.'[88] This, therefore, signals a radical reframing of the purpose limitation principle, which could allow for extensive use of informational powers of the state in the fields of criminal as well as administrative law.[89]

It is unsurprising that this addition was brought to the fore by the Dutch delegation, as often when the Dutch data protection authority establishes breaches of the data protection legislation by the government, the response is to propose new legislation to remedy the situation.[90] This extreme positivist approach is characteristic of the attitude of governments towards data protection regulation as an instrument to remove the obstacles on the way

[86] Werkgroep Verkenning Kaderwet Gegevensuitwisseling, 'Kennis delen geeft kracht Naar een betere èn zorgvuldigere gegevensuitwisseling in samenwerkingsverbanden'(Rapport van de Werkgroep Verkenning kaderwet Gegevensuitwisseling, Den Haag, 5 December 2014) 24.

[87] Article 13 Directive 95/46. See for an explanation of this in the Netherlands: Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens, 2010, p. 68.

[88] Future Group, 'Public Security, Privacy and Technology in Europe: Moving Forwards, (Portugal 2007) <http://bit.ly/PqvWIJ> accessed 7 June 2018 8.

[89] In the Netherlands public authorities already undertake profiling operations against entire neighbourhoods to prevent and combat unlawful use of public funds and public services, not complying with labor law and combating tax and security fraud. There are plans in the making for adopting legislation which will allow for even more extensive and invasive profiling.

[90] Ger Homburg and others, *ANPR: toepassingen en ontwikkelingen* (WODC 2016) 3-4.

towards realising regulatory goals. In this view, the substantive protection provided by the law can also be taken away by the law. Such state of affairs disregards the values that the law intends to protect and demonstrates that governments are infected with a trite pragmatism, which is at odds with at least one of the rationales for human and fundamental rights — to impose substantive limits on government power.

The new legal framework under the GDPR could prove invaluable to US tech giants, which can now sell their services to Member States' governments, where this was prohibited prior to the GDPR. Without making any claim on the motives of the Dutch delegation in Brussels, it is noteworthy that already in 2005 the US ambassador speculated that the Netherlands could possibly assist the US in relaxing the regulatory restraints imposed by the EU in favour of US businesses:

> 'Because the Netherlands has one of the highest broadband penetrations in Europe, emerging research efforts in the areas of nanotechnology, life sciences, and other IT-related areas, and a new tax treaty, the country offers U.S. companies an important gateway into Europe. If consulted early and regularly, the Netherlands can also be an important ally in navigating the EU's regulatory environment and removing obstacles.
>
> The key to maximizing Dutch effectiveness is to involve them early through high-level consultations and exchanges. Dutch pragmatism and our similar world-views make the Netherlands fertile ground for initiatives others in Europe might be reluctant, at least initially, to embrace.'[91]

The workings of Article 8 ECHR and 7 of the Charter, however, remain unaffected by this Faustian facelift of data protection law. A broad interpretation of purpose limitation can easily escalate to government powers being formulated in a manner conflicting with rules of foreseeability, proportionality and the essence of the right to privacy. Governments building informational muscles are not indemnified against these important requirements, although it remains to be seen how this tension will develop in the case law of the courts.

2.4 The rights of the data subject

There are a number of rights the Directive and GDPR provide to the data subject. Subjective rights only become relevant once personal data are recorded and collected by a third party. Two new rights famously added by the GDPR are the right to be forgotten and the right to data portability.

These rights do not prevent the recording of personal data, however, they can contribute to making processing operations transparent. First of all, the data subject has a right to access his data. This right consists of a right to know if data is processed and if so what data is processed and from what source, for what purpose(s), the categories of data concerned, the

[91] Embassy The Hague, Ambassador's Parting Thoughts on Taking the Dutch, (22-08-2005) <http://213.251.145.96/cable/2005/08/GUARDIANUK-38987.html> accessed 7 June 2018.

recipients or categories of recipients to whom the data is disclosed and the logic involved in the processing, at least when this generates automated decisions that produce legal effects. Furthermore, this entails the right to obtain rectification, erasure or blocking of the processing of data if this processing violates the rules as laid down in the Directive (Article 12(b)). In the GDPR these rights are divided in three separate rights.

If the ground of the processing is found in the necessity to carry out a task of public interest or for the purpose of the legitimate interests for the controller or by the third party or parties to whom the data is disclosed (respectively Article 7 (e) and (f) Directive 95/46 and Article 6(1) (e) and (f) GDPR), the data subject has a right to object (Article 14 Directive 95/46 and Article 22 GDPR). The grounds on which the data subject can object have to be legitimate and compelling and relate to his particular situation. An exemplary case is *Google Spain*, in which the CJEU held that the specific circumstances of the applicant justified that the links which led to this information had to be removed from the list of search results. It found that data processing, even when it is initially lawful, later can violate the principles enshrined in 6(1)(c) to (e) Directive 95/46 when it is no longer necessary for the purposes for which they were initially processed. The CJEU established that the data subject has a right to stop Google Spain from linking information concerning him to his name and held that for this right it is not relevant whether this information causes prejudice to him.[92]

The subjective rights function only after the initial collection of personal data. These, therefore, will not contribute to a design of an IoT system which avoids or minimises the initial recording of personal data. Hardcoding these rights into an IoT system can, nevertheless, contribute to transparency for the data subject about the data that is processed.

2.5 The GDPR: changing anchors

The Commission structurally confuses the source of data protection legislation. There are a number of instances in which this confusion can be discerned. For instance:

> 'The Directive enshrines two of the oldest and equally important ambitions of the European integration process the protection of fundamental rights and freedom of individuals and *in particular the fundamental right to data protection*[93], on the one hand, and the achievement of the internal market — the free flow of personal data in this case — on the other.'[94]

Article 1(1) of Directive 95/46/EC provides that 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their *right to privacy* with respect to the processing of personal data'.[95] Article 1(2) GDPR provides that the regulation 'protects the fundamental rights and freedoms of natural persons, and in particular

[92] *Google Spain* (n 61) para 96.
[93] Italics added by author. Notice that Article 1 explicitly mentions privacy.
[94] Commission, 'a comprehensive approach on personal data protection in the European Union' COM (2010) 609 final 2.
[95] Italics added by author.

their *right to the protection of personal data*'.[96] There is no referral to the right to privacy in the GDPR. This raises the question whether this change of anchor is merely theoretical, or could it be that this change will have practical consequences.

In 2010, the Commission stated in a Communication its confusion of history in bold:

> 'The objective of the rules in the current EU data protection instruments is **to protect the fundamental rights of natural persons and in particular their right to protection of personal data**, in line with the EU Charter of Fundamental Rights[97].'[98]

In the 2012 Communication on safeguarding privacy in a connected world the Commission, again, makes the safeguarding of the right to personal data protection the focal point.

> 'The EU's 1995 Directive, the central legislative instrument for the protection of personal data in Europe, was a milestone in the history of data protection. Its objectives, to ensure a functioning Single Market and effective protection of the fundamental rights and freedoms of individuals, remain valid. However, it was adopted 17 years ago when the internet was in its infancy. In today's new, challenging digital environment, existing rules provide neither the degree of harmonization required, nor the necessary efficiency to ensure *the right to personal data protection*.'[99]

In a press release on fundamental rights, it even makes the implicit claim that the right to the protection of personal data is part of Europe's constitutional heritage.[100] The right to the protection of personal data was widely considered a constitutional novelty and therefore it would have made much more sense to refer instead to the right to privacy. The Commission also refers to the Stockholm Programme and the Stockholm Action Plan[101] noting the ambition to 'ensure that the fundamental right to data protection is consistently applied'. As noted earlier in Chapter 1, the Stockholm Programme provided that the Union:

[96] Italics added by author.

[97] *Lindqvist* (n 15) paras 96, 97. and Case C-275/06 *Promusicae* [2008] ECR I-00271. See also the jurisprudence of the European Court of Human Rights, eg in cases: *S and Marper v. The United Kingdom* App nos 30562/04 and 30566/04 (ECHR 4 December 2008); *Rotaru v Romania* App no 28341/95 (ECHR 4 May 2000) para 55.

[98] COM (2010) 609 (n 94) 5.

[99] COM (2012) 9 (n 9) 3. Italics added by author.

[100] European Commission, 'Fundamental Rights: Importance of EU Charter grows as citizens stand to benefit' (Press Release, Brussels, 14 April 2014) <http://europa.eu/rapid/press-release_IP-14-422_en.html> accessed 19 February 2016.

[101] Commission, 'An area of freedom, security and justice serving the citizen' (Communication From the Commission to the European Parliament and the Council) COM (2009) 262 final and Commission, 'Delivering an area of freedom, security and justice for Europe's citizens: Action Plan Implementing the Stockholm Programme' (Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2010) 171 final respectively.

> 'must also foresee and regulate the circumstances in which interference by public authorities with the exercise of these rights is justified and also apply data protection principles in the private sphere.'[102]

Applying data protection principles in the private sphere implies the collection of data about the private sphere, whilst respecting the right to privacy would take the absence of data collection as a starting point. These communications reveal a tendency to tilt the table towards the collection of data as a default policy guideline. Furthermore, it can be concluded that throughout its communications the Commission eliminates the original anchorage of Directive 95/46 in the right to privacy and replaces it with the right to the protection of personal data and does so systematically. In combination with the instrumental approach the Commission adopts towards data protection, this leads to the neglect of substantive norms provided by the data protection framework. Gutting the right to privacy out of data protection legislation contributes to a legal framework, in which the necessity of interferences with the right to private life is no longer tested. This way the values that privacy law aims to protect are slowly smoothed over by an instrumental approach to fundamental rights that can be characterised as the *rule by law*.

2.6 Implications for IoT systems

If data processing was a game, Directive 95/46 and the GDPR would be the instruction manual included in the box that came with it. The rationale of these legal acts is different from that of the right to privacy. The scope of the right to privacy covers a state of non-interference. The scope of data protection sees to a state of conditioned interference. Data protection sets rules and procedures for the processing of personal data in order to legitimise the interference. In the words of Gurtwirh en De Hert, data protection is a *transparency instrument*, whilst privacy is an *opacity instrument*.[103] The processing of personal data is subjected to a set of rules which aim to give a measure of control to the data subject through, amongst others, obliging the controller to be open about his operations. The right to privacy takes non-interference as the rule, whereas interference is the exception. This difference in rationale has been increased due to the recent changes adopted in the GDPR.[104]

Secondary data protection legislation knows no equivalent to the quality of law-requirements which follow from ECtHR case law on the right to private life, particularly on the requirement of foreseeability. The requirement that a measure must be 'necessary in democratic society' is retraceable to the requirement of necessity in the grounds for processing and to the data protection principle of data minimisation. Following the CJEU

[102] The Stockholm Programme – An open and secure Europe serving and protecting the citizens (Notice from the Council of the European Union) [2010] OJ C 115/1, 18.

[103] Paul de Hert and Serge Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in Eric Claes, Anthony Duff and Serge Gutwirth (eds), *Privacy and the criminal law* (Antwerpen/Oxford Intersentia 2006).

[104] Section 2.3.

case law a strict proportionality test is required, and even though this could yield considerable results for the design of IoT systems, it is unlikely that this test will be executed properly, if at all. This is due to the fact that data protection law leaves the application of its rules to the parties having an interest in the processing of personal data by these systems. This implies that the Commission can leave the application of data protection rules, including those encompassing the proportionality test, to parties further down the line in the IoT policy process. It should, also, be kept in mind that compliance with data protection legislation is not the same as respecting the right to privacy.[105]

In accordance with the principles relating to data quality the following demands should be met. The processing operations should be transparent and in line with other relevant laws, such as Article 8 ECHR and Article 7 of the Charter. Personal data can be collected only for a specific purpose and the scope of the processing operations should be established *a priori* and communicated to the data subject in an intelligible form. Furthermore, the data should not be processed further in a way incompatible with this purpose. The proportionality principle expressed here should be informed by ECtHR and CJEU case law, and therefore the collection, retention and use of the data collected through the IoT system should (again) not go beyond what is strictly necessary. The controller must respect the rights of the data subject. It would make sense for the right to access to be hardcoded in the design of the IoT system. This would effectively allow people to access their own data and subsequently invoke other rights such as rectification or erasure.

Both the grounds and the principles for the processing of personal data necessitate the legislature to make substantive choices on the design, much in line with the idea of *essential elements of design*, which will be further discussed in Chapter 4 section 4.1. The principle of data minimisation informs the legislature and the Commission to pursue a design of IoT systems in which the data is stored on the system itself.[106] Given the fact that the concept 'necessary' has to be informed by ECtHR and CJEU case law and the particular circumstances under which the IoT systems are deployed, their processing operations should be strictly necessary for the purpose they serve. Such correct application of data protection rules should lead to questioning the necessity of the initial recording of personal data *and* all the subsequent processing operations performed upon them. Moreover, additional safeguards that protect the interests and rights of the data subject can be put in place, which is in line with the methodology of the Commission's impact assessment.[107]

[105] Colette Cuijpers and Bert-Jaap Koops,'Smart Metering and Privacy in Europe: Lessons from the Dutch Case' in Serge Gutwirth and others (eds), *European Data Protection: Coming of Age* (Springer Science + Business Media 2013) 288.

[106] Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth and others (eds), *Data Protection in a Profiled World* (Springer 2010).

[107] Commission, 'Operational Guidance on Taking Account of Fundamental Rights in Commission Impact Assessments'(Commission Staff Working Paper) SEC(2011) 567 final 18.

3. Article 8 of the Charter: the scope of protection and its limitations

One of the novel features of the Charter of Fundamental Rights is the introduction of the right to the protection of personal data. It is heralded by commentators as a further fortification of data protection law.[108] It also further troubles the already murky waters where interferences with the right to the protection of personal data and the right to privacy coincide. The aim of this section is to establish the scope of Article 8 as well as the contested requirements for limiting it, or alternatively to establish the limitations which constitute this right.

3.1 The structure of Article 8

The right to the protection of personal data is different from secondary data protection legislation. Its substance consists of a stripped down version of this legislation. It is laid down in Article 8 Charter and consists of three paragraphs. Article 8(1) formulates the right to the protection of personal data. Article 8(2) reproduces the principle of fair processing and the purpose limitation principle (data protection principles), 'consent of the person or some other legitimate basis' as the grounds for processing and a right of access to and rectification of data (subjective rights). Article 8(3) establishes that compliance with the rules will 'be subject to control by an independent authority.' It is unclear on the basis of which considerations these choices were made, and the Explanations of the Charter remain silent on this matter. Whether Article 8(1) should be read as the right itself, or one element of the right, depends on how one views the structure of Article 8. The case law of the CJEU has not clarified this issue and differing views can be found among the commentators, most notably those of Kranenborg and Fuster.

According to Kranenborg, ArticIe 8 deviates from other rights, since the right 'constitutes the heading of a set of rights and obligations *and limitations of* these, which are put together as an elaborate system of checks and balances'.[109] As a consequence, he argues, the general limitation clause should not apply, because this would imply that personal data can only be processed without consent when this is justified in accordance with Article 52(1) of the Charter. Accordingly, this would disregard the difference between the right to privacy in Article 7 and the right to the protection of personal data in Article 8.[110] Kranenborg does not comment on the possibility for the legislator to apply Article 52(1) in order to limit the checks and balances provided.[111]

In his view, Article 8 contains the right and the limitation; but the limitation is also part of the right, since it is 'an elaborate system of checks and balances'.[112] The right to the protection of personal data, therefore, breaks away from the logic of rights and requirements for

[108] Paul de Hert and Serge Gutwirth (n 7).

[109] Herke Kranenborg, 'Article 8' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart 2014) 260.

[110] ibid. Kranenborg refers to the right to data protection

[111] In personal comments he confirmed that he does not exclude the application of Article 52(1) to Article 8(2).

[112] ibid 229.

limitations. Accepting his view implies that the requirements on the limitations to the right to privacy are different from the requirements on the limitations of the right to the protection of personal data.[113] This would mean that Article 8 provides less, or in any case different, protection than Article 7. He also claims that when Articles 7 and 8 coincide, yet secondary data protection legislation applies, the Court should assess the interference under the latter, 'compliance with which ensures that data processing does not breach the right to privacy'.[114] Even though data protection legislation can be interpreted in line with the right to privacy, this does not remedy their differences established in the first part of this chapter. Also, the scope of the right to privacy covers a stage prior to the recording of data; it protects a sphere and moment preceding the creation of data.

Fuster and Gutwirth (hereinafter Fuster) adopt a slightly different view on the structure of Article 8.[115] According to them, there are two ways to read it: *prohibitive* or *permissive*.[116] In a prohibitive reading, the first paragraph contains the right itself which prohibits the processing of personal data, while the second and third paragraphs are to be read as conditions that have to be met to legitimately interfere with the right to data protection, i.e. to process personal data. She refers to this as the binary structure that is reminiscent of the structure of Article 8 ECHR to which data protection law has been formally linked since 1995.[117] In this reading, the right's core is '*proscriptive*, to the extent that it basically withholds and principally prohibits the processing of personal data', i.e. the prohibitive reading. Fuster argues that in this reading, Article 8(1) constitutes the right and the limitations are primarily described by the last two paragraphs.[118] When this reading is adopted the right to protection of personal data provides different conditions for interference than those to interfere with the right to privacy. The conditions set out in the second paragraph call for fair processing, purpose specification, a legitimate basis for processing and access and rectification rights; it does *not* entail a *necessity test* subject to the principle of proportionality, nor a test if the *essence of the right is respected*. This implies that the proportionality of the processing is no longer a condition that has to be met. This contradicts the general approach of qualified rights which usually allow for interferences only when these are necessary. It could be that the legislature anticipated the applicability of Article 52(1) of the Charter when the processing of personal data would raise an interference with another Charter right. Secondary data protection legislation, nevertheless, provides consistently that the processing of data without consent must be *necessary* for one of the five alternative grounds to consent. When the drafters of the convention intended Article 8 of the

[113] ibid 229. He inextricably links the application of Article 52(1) to the consequence that the right to the protection of personal data would get the character of the right to informational self-determination, which he deems incorrect. A discussion of this concept falls outside the scope of this book.

[114] ibid 261.

[115] Gloria Gonzáles Fuster and Serge Gutwirth, 'Opening up Personal Data Protection: A Conceptual Controversy' (2013) 29 Computer Law & Security Review 531.

[116] ibid.

[117] She writes this structure out with the following formula:
'Art. 8 Charter = Art. 8(1) Charter – (Art. 8(2) Charter + Art. 8(3) Charter)'.

[118] Fuster and Gutwirth (n 115) 532.

Charter as a proscriptive right, their choice to leave out the requirement of necessity is noteworthy.

In the permissive reading, the right consists of all three paragraphs in Article 8, thus the second and third paragraph express the very right itself.[119] In this view, the provision is unitary which leads to a *permissive* right, also referred to as an *affirmative* understanding. It appears that the Article 29 WP supports this reading.[120] In a permissive reading, the right to personal data protection is comprised of all three paragraphs. This implies that the exceptions formulated in Article 8(2) are part of the right: 'the core content of the right to the protection of personal data is precisely described by the conditions allowing for the processing of personal data'.[121] In this reading Article 8 provides its own limitations. This seems to reflect Kranenborg's more holistic view of data protection, who views it as an elaborate system of checks and balances.[122] The difference is that Fuster and Gutwirth explicitly consider that the elements contained in paragraph 2 and 3 can be limited in line with Article 52(1).[123] Nothing in the text of the Charter suggests that this consideration is wrong. It is in line with secondary data protection legislation that the right to data protection subjects the processing to a set of rules and conditions, yet also allows limitations on this specific logic for a given set of legitimate aims in exceptional cases on the condition that the requirements for interfering with the right to privacy are met.[124]

Fuster notes the CJEU's inconsistent interpretation, where certain cases it adopts a reading that refers to Article 8(1) as the right to personal data protection, yet in others it refers to the entirety of Article 8 when interpreting this right.[125] In short, the conceptual confusion is not cleared up by the CJEU, instead it seems to contribute to it. [126] She further observes that these conflicting interpretations lead to different conclusions about the *nature* of the right to the protection of personal data, which should have consequences for what is conceived as the essence of the right.[127] According to Fuster, this is especially relevant in the light of Article

[119] ibid, 533.
[120] WP 211 (n 58) 4.
[121] Fuster and Gutwirth (n 115) 533.
[122] Kranenborg (n 109) 260.
[123] Fuster and Gutwirth (n 115) 533.
[124] To be found in Article 13 Directive 95/46 and Article 23 GDPR.
[125] Gloria González Fuster, 'Security and the Erasure of Privacy in the Data Protection Legal Landscape of the European Union' (Amsterdam Privacy Conference, October 2012) 6. For further reading I refer to her own note in this article:
'On the variable case law on balancing the EU right to the protection of personal data, see: González Fuster, Gloria (2012), "Balancing intellectual property against data protection: A new right's wavering weight", in *Challenges and Opportunities of Online Entertainment. Proceedings of the 8th International Conference on Internet, Law & Politics*. Universitat Oberta de Catalunya, Barcelona 9-10 July, 2012, pp. 385-400.'
[126] For the *prohibitive* reading see *Asnef* (n 15) para 41. Case C-291/12 *Michael Schwarz v Stadt Bochum* ECLI:EU:2013:670, para 24. For the permissive reading see Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* EU:C:2014:238, [2014], para 36. In Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, para 52. Here the Court found that the missing of consent rendered it necessary to justify the limitation on the ground of Article 52 (1) Charter.
[127] Fuster and Gutwirth (n 115) 532.

52(1) of the Charter, which holds that any limitation of a fundamental right must respect its essence. She seems to link the idea of proportionality to the notion of the essence: 'any interference with a right which is disproportionate (in view of the objective pursued) is to be regarded as impairing the right's very substance'.[128] Either a prohibitive reading is adopted in which the essence is a 'mere prohibition', or a permissive reading is adopted in which 'the central component is the detailed requirements in themselves'.[129]

The sources on which Article 8 of the Charter is based do not provide a definitive answer as to its structure. The first two sources mentioned in the Explanations of the Charter are Convention 108 and Directive 95/46 are both concerned with enabling the processing of personal data, rather than prohibiting it, which has been discussed above. These sources hint towards a permissive reading. Another source is the Regulation (EC) No 45/2001.[130] The Explanations of the Charter state: 'The above-mentioned Directive and Regulation contain conditions and limitations *for the exercise of the right to the protection of personal data*.'[131] This admittedly hints towards a prohibitive understanding, because the 'conditions and limitations' seem to apply to the right to prohibit the processing of personal data. This is confirmed in the first recital of the GDPR:

> 'The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of [the Charter] and Article 16(1) of the [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.'

At first sight this seems to imply that the right is actually limited to the first paragraph of Article 8, which implies the prohibitive reading is correct. Here, the scope of the right to the protection of personal data is the prohibition to process it, to which exceptions can be made. The mere prohibition to process personal data reduces the meaning of the right to the protection of personal data to a right to be left alone from data processing and places its limitations outside the scope of the right. Upon a closer look, the first recital does leave an opening for a permissive reading, because it provides that 'the protection of natural persons *in relation to the processing of personal data* is a fundamental right'. Placing the right in relation to the processing also links it to the conditions for processing. This is also consistent with the earlier observations of the different character of Article 8 as compared to Article 7 of the Charter. Observing data protection from a helicopter-view, one can see that the protection it offers to the individual consists of a body of rules, obligations, prohibitions, safeguards and subjective rights enacted in its legislative acts.[132] Data protection law provides rules relating to the protection of natural persons *with regard to the processing of personal data and rules*

[128] ibid 537.
[129] ibid 533.
[130] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8/1.532.
[131] Explanations on Article 8 – Protection of personal data, Explanations Relating to the Charter of Fundamental Rights [2007] OJ C 303/17.
[132] Please note that Article 8 of the Charter should not be confused with secondary data protection legislation and that the latter provides more extensive rules, prohibitions, safeguards and subjective rights.

relating to the free movement of personal data; these are the exact words of Article 1 GDPR, clearly permissive. The title of 'Fair Information Practices', which also served as a source for data protection rules, was inspired by the US Fair Labor Practices.[133] Just like FLPs did not aim to prohibit labour, the goal of FIPs is clearly to facilitate information processing, not blocking it. Put more simply, without data to process, there would be no need for data protection.

The mere fact that data is the central subject of this right indicates it is a different creature than the right to privacy. 'A right to data protection' should be understood as a body of rules, not as a single right, under which the processing of personal data is allowed. Article 52 of the Charter does not have to be invoked to process personal data. You could, therefore, claim that the right to the protection of personal data is a permissive right. The protection offered under Article 8 is fundamentally different from the protection under Article 7 and 52(1) of the Charter. The right to privacy takes freedom from interference, also in the form of the processing of personal data, as the rule and the interference as the exception to this. It would be, however, an oversimplification to claim the right to the protection of personal data turns the processing of personal data into the rule. If the processing of personal data also interferes with the rights under Article 7, the limitation clause of Article 52(1) of the Charter applies. This limitation clause can also be invoked to restrict the scope of the rules provided for in Article 8(2) and (3) of the Charter. The strict conditions provided by the right to the protection of personal data should be viewed as its core and exceptions to this, in accordance with CJEU case law, should be interpreted restrictively. These exceptions, therefore, should follow the rationale of Article 52(1) of the Charter.[134]

The essence of Article 8 of the Charter according to the Court

Conceptualising data protection as a body of rules which is essentially different from the right to private life is also in line with the case law of the CJEU on the essence of Article 8. The Court held in *Digital Rights Ireland* that the essence of the right to the protection of personal data was not affected by Directive 2006/24, since it provided that certain principles of data security and data protection had to be respected by providers of publicly available electronic communications services and public communication networks:

> 'According to those principles, Member States are to ensure that appropriate technical and organizational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of data.'[135]

[133] What-when-how, 'Fair information practices' <http://what-when-how.com/privacy/fair-information-practices/> accessed 7 June 2018.

[134] The restrictive application of exceptions to the purpose limitation principle is exactly what the Dutch delegation intended to change with the amendments it apparently proposed to Article 6(3), 6(4) GDPR and Recital 50. Tweede Kamer, Kamerstukken II [2015-2016] 32 761 no 91, 2.

[135] *Digital Rights Ireland* (n 126) para 40.

In its *Opinion 1/15 on the PNR Agreement between the EU and Canada*, the Court further elaborated on what constituted protection of the essence of Article 8.[136] It confirmed the relevance of rules on security, confidentiality and integrity, which were largely the same as those provided by the Data Retention Directive. It expanded the scope of the essence by providing that Article 3 of the Agreement limits the purposes for which the PNR data could be processed.[137]

What can be inferred from these cases is limited, but some contours of the Court's concept of the essence can be discerned regarding the recording, collection, storage and access to data. The Court has not included any limits with respect to the essence regarding the recording, collection and storage of data. The massive processing of this data which was central to the judgments in *Digital Rights Ireland*, *Schrems*, *Tele2 Sverige* and *Opinion 1/15 PNR* did not spark any thoughts from the Court on what is essential to the right to the protection of personal data. Article 8 and what it demands seems to be limited to a rather technical notion of data security. Interestingly, Article 8 does not mention anything about confidentiality, integrity or security. This part of the Court's conceptualisation of the essence does not resonate even remotely with the contents of Article 8 of the Charter.[138]

3.2 Confusion about the relation between Article 8 and 7

The case law of the Court lacks a coherent approach to the relation between the right to privacy and the right to the protection of personal data.[139] If an interference simultaneously occurs under Articles 7 and 8, the CJEU generally applies the limitation clause of Article 52(1) of the Charter. Sometimes it does this with reference to Article 52(3) of the Charter according to which the meaning and scope of Charter rights should be the same as the corresponding ECHR rights. Thus, Article 7 of the Charter should be interpreted in line with Article 8 ECHR.[140] Usually the Court does not elaborate on the differences in scope between privacy and data protection, but in one rare instance AG Villalón did elaborate on the difference between the fundamental right to privacy and the fundamental right to the protection of personal data:

> 'These are data which, qualitatively, relate essentially to private life, to the confidentiality of private life, including intimacy. In such cases, the issue raised by personal data commences, so to speak, further 'upstream'. The issue which arises in such cases is not yet that of the guarantees relating to data processing but, at an earlier stage, that of the data as such, that is to

[136] Opinion 1/15 of the Court, *Passenger Name Records; PNR* ECLI:EU:C:2017:592, para 150.
[137] ibid.
[138] The Court's thoughts on the purpose do for a small part, even though they do not even mention 'specific purposes', just 'purposes'.
[139] Kranenborg (n 109) 229.
[140] Case C-419/14 *WebMindLicenses* ECLI:EU:C:2015:832, para 70.

> say, the fact that it has been possible to record the circumstances of a person's private life in the form of data, data which can consequently be subject to information processing.'[141]

AG Villalón notes that *the right to protection of personal data* is concerned with the process following the adoption of a decision permitting the *recording* of the circumstances of a person's private life in the form of personal data[142] He contrasts this with the right to privacy; the enablement of the possibility to record circumstances surrounding a private life as personal data does fall under the scope of Article 7 of the Charter.[143] The mandatory installation of IoT systems which are designed in a privacy-infringing way does exactly this: it enables the recording of circumstances of a person's private life.

The intimacy of the nature of the data follows from the fact that these systems are installed in the private surroundings (home and car) of citizens. Moreover, the possibility of systematic recording necessitates looking beyond the initial nature of the data. What is required is an assessment of the nature of information that can be inferred from long term retention of this data. Also the context of the processing is important in establishing whether the initial recording of the data should be protected by the right to private life.[144]

For example, the private nature of data about electricity usage depends on what can be deduced from the data. If the amount of data recorded covers every fifteen minutes for a longer period of time this can reveal quite detailed information about a person's life and should be considered highly private. However, if the data only reveals the aggregate of electricity consumed in the past half year, the nature of this data will be much less revealing. This shows how the amount of data as well as the context in which it is processed can affect the nature of the data.[145]

AG Villalón further elaborated on the difference between the right to private life and the right to protection of personal data:

> 'The fact that Directive 2006/24 may satisfy fully the requirements of Article 8(2) and (3) of the Charter and be considered not to be incompatible with Article 8 of the Charter in no way means that it is fully compatible with the requirements resulting from the right to privacy guaranteed by Article 7 of the Charter.'[146]

AG Villallón seems to adopt a prohibitive reading, since he suggests that an exception is allowed on the prohibition of the processing of personal data enshrined in Article 8(1) when legislation meets the requirements of Article 8(2) and (3). He applies the proportionality test

---

[141] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* EU:C:2014:238, [2014], Opinion of AG Villalón, paras 61, 63 and 65.

[142] It should be noted that the recording of personal data, also, constitutes a form of processing of data. The GDPR, therefore, does allow questioning recording functions of IoT systems.

[143] This argument seems to lean on a permissive reading of Article 8, in which the issue of *possible recording* of the data is not questioned.

[144] Also see Chapter 3, section 2.1.

[145] See Chapter 2, section 2.1.

[146] *Digital Rights Ireland (Opinion)* (n 141) para 6o.

only to the right to privacy, implicitly rejecting the applicability of Article 52 to the right to protection of personal data. If we follow his interpretation, data can be processed legitimately in accordance with Article 8 of the Charter, while at the same time violating Article 7 and 52 of the Charter.[147] This confirms that Article 8(1) of the Charter can provide less protection than Article 7 of the Charter.

The twist given by the CJEU in executing the proportionality test in *Digital Rights Ireland*, already commented on in Chapter 2, becomes even more puzzling with the distinction exposed by AG Villalón. In *Digital Rights Ireland*, the Court established that:

> 'So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).'[148]

The Court bases this on *IPI*[149], which in turn refers to *Volker und Markus Schecke*[150] and *Satakunnan Markkinapörsi and Satamedia*.[151] By phrasing the necessity test in a manner, where the derogations and limitations in relation to *the protection of personal data* do not go further than what is *strictly necessary*, the Court mistakenly replaces the right to respect for private life by the right to the protection of personal data. By adopting such an approach, the Court fails to question the necessity of the initial recording and collection of the data, which is covered by the right to private life. Where AG Villalón argues that limitations compliant with Article 8 can still result in a disproportionate interference with Article 7, the CJEU reasons that Article 7 can be interfered with when the limitations to Article 8 do not go beyond what is strictly necessary. This begs the question: why does the CJEU not adhere to applying the proportionality test to the right to private life itself? Why does it, instead, apply it to the right to the protection of personal data in order to test if the interference with the right to private life is legitimate, even if it includes by default the adjective *strictly*? By this quirky move it may circumvent the protection offered by the right to private life in the EU legal order.[152]

[147] It is unclear if a permissive interpretation would have let to a different result.

[148] *Digital Rights Ireland* (n 126) para 52. Also repeated in Case C-203/15 *Tele2 Sverige* EU:C:2016:970, [2016]; *Schrems* (n 61).

[149] Case C-473/12 *IPI* EU:C:2013:715, [2013] para 39.

[150] *Volker und Markus Schecke and Eifert* (n 125) paras 77 and 86.

[151] Case C-73/07 *Satakunnan Markkinapörsi and Satamedia* [2008] ECR I-09831, para 56.

[152] For more commentary on the case law of the CJEU see Gloria González Fuster, 'Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection' (2014) 2(2) Birkbeck Law Review 263.

4. Conclusion

Data protection legislation consists of a patchwork of laws, mostly overlapping, yet all based on the underlying rationale of setting procedures, conditions and limitations to legitimise the processing of personal data. Secondary data protection legislation consists of a broad body of rules, which among others provide obligations to data controllers and rights to data subjects. The protection it offers largely depends on the interpretation and application of its open norms on the given data processing operation. The idea, which seems to motivate the European Commission and is supported by some authors, is that the right to privacy is respected as long as data protection legislation is complied with. This idea seems to stem from a desire for simplicity rather than correct legal analysis. Data protection legislation can be seen as a form of co-regulation enforced by the DPA, while the right to privacy is a classical human right with all the strengths and weaknesses associated with it. Although the aim of this chapter was to establish the differences in the requirements that follow from data protection legislation as opposed to the right to privacy, focusing on these differences blurs the bigger picture: the radically different rationale behind these rights. The rationale behind the right to privacy comes down to freedom from interference. The rationale behind data protection legislation is to condition interferences in order to offer a measure of protection to the data subject and legitimise the processing of personal data.

The rationale of legitimising the (mass) processing of personal data obviously raises tensions with our understanding of the right to private life. Questions of necessity, proportionality, foreseeability, pressing social needs, the nature of the interferences and others, can get lost when translated into the vocabulary of data protection. Data protection law pursues the normalisation of the processing of personal data. This normalisation can be used to justify data processing schemes, in which it is accepted that the exceptional nature of the interference with the right to private life is turned into the rule. The point of departure of data protection law, however, is that of a transparent relationship between data controller and data subject, usually entered into voluntarily: a company and the contracts with its customers, a public authority and the services it provides to its citizen, a sports club and the subscriptions of its members etc.

The deployment of IoT systems is controversial because it entails the installation of these systems in the private sphere of citizens: voluntarily, involuntarily or even unknowingly. These systems will function in an information society in which insight into data processing operations is becoming increasingly difficult to gain, which was demonstrated by the upheaval caused by the revelations about the collaboration between Facebook and Cambridge Analytica. There is no doubt that IoT systems, which are mandatorily installed in the private sphere under EU legislation and that record or are able to record private facts from a person's life, raise an issue under Article 8 ECHR and Article 7 of the Charter. Data protection law in isolation from the right to privacy, therefore, is unfit to guide the policy and legislative process of mandatory IoT systems. To the extent that data protection principles coincide and correspond to the requirements in Article 8(2) ECHR, their interpretation and application should be in line with ECtHR and CJEU case law and carried out by the legislature. Data protection legislation provides requirements which, if interpreted and applied properly, can

prohibit the equipping of IoT systems with certain data processing features. Data protection legislation has a 'prohibitive potential' even though this is not likely to be realised in the settings of IoT policy.

Relying solely on data protection law creates the pretext to designate the responsibility to interpret and apply the law to the parties responsible for the exploitation of these systems. In other words, the Commission's focus on data protection favours an outcome in which the Commission transfers political decisions about IoT systems to the parties seeking to benefit from them. Especially when the open norms of data protection law are left to parties such as ESOs to be interpreted and applied, the risk arises that the norms are watered down or simply ignored. It is absolutely inexcusable to leave these political decisions to parties which seek to profit from the installation of these systems.

Another drawback of the limited scope of Article 8 and the way data protection legislation is applied, is that it does not cover decisions on the presence of the possibility to record the circumstances of a person's private life in the form of personal data. This is particularly relevant for the choices of the design of IoT systems and the decisions regarding their mandatory installation. Excluding this phase in the preparatory work of a legislative proposal implies that these decisions, which have the potential of severely impacting the right to private life, are not accounted for by the Commission.

On a more substantive level, data protection legislation differs from the right to private life, because its essence is different. When the surveillance potential of IoT devices is fully considered, choices regarding their design could fundamentally alter the impact of their mandatory installation: ranging from a rather innocent one-purpose platform for a particular public interest to a multi-purpose surveillance system that can subject aspects of citizens' lives to government control to an increasing degree. With the mandatory installation of these systems in the back of the mind, the choice for a privacy-invasive design results in a generalised surveillance measures against the entire population of the EU. This goes against the essence of the right to private life. Data protection law does not raise such objections.

Chapter IV
The Commission's approach to and interpretation of the right to privacy in Internet of Things policy

1. Introduction

The European Commission is the central policy actor with regard to the Internet of Things in the EU.[1] It introduced the term in its communications from 2006 onwards, launching an IoT action plan in 2009.[2] Furthermore, it successfully proposed legislation that mandates the installation of IoT systems.[3] This legislation either delegates the power to adopt non-legislative acts or confers implementing powers concerning the design of these systems to the Commission. The Commission therefore plays a key role with regard to mandatory IoT systems and is the designated institution in the EU to take responsibility for the role of fundamental rights, particularly the right to privacy, in IoT policy.[4] The Commission is not free in how it deals with its policies. On a regulatory level, it is limited by the Charter of Fundamental Rights, the TFEU and the TEU. On policy and institutional level, it is influenced by several actors – institutional as well as private – in particular the Council.[5]

On 16 October 2006, the Commissioner for Information Society and Media, Viviane Reding, in a speech on the need for a European policy on RFID, mentioned the IoT as a future

[1] Although IoT policy has ceased to exist under this specific name, there are numerous policy areas in the EU that are related to the IoT and for which the lines of action from the action plan still represent relevant instruments that the Commission wields in the current execution of policy. Policy regarding IoT systems is still in development, therefore I will not write about it in the past tense. IoT policy also interlinks with other EU policies that have long been recognised to have an impact on a continental scale and therefore need a coherent approach, e.g. transport and energy.

[2] Commission, 'Internet of Things – An action plan for Europe' (Communication from the Commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions) COM (2009) 278 final.

[3] Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC [2012] OJ L 315/1 (hereinafter 'Directive 2012/27/EU'); Regulation (EU) 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 [2015] OJ L 123/77 (hereinafter eCall Regulation).

[4] Not in the last place because overseeing the application of Union law is one its competences according to Article 17 TEU.

[5] Neill Nugent, *The Government and Politics of the European Union* (6th edition, Palgrave Macmillan 2006) 167 – 168.

perspective.[6] She shared some preliminary conclusions deriving from a public consultation the gist of which was EU citizens' concern over privacy. Reding stated the following:

> 'The large majority are willing to be convinced that RFID can bring benefits but they want to be reassured that it will not compromise their privacy. This is the deal that we have to strike if we want RFID to be accepted and widely taken up. This is the deal I am looking to make.'[7]

These were clear-cut terms from the Commissioner which indicated the respect for the voice of the people regarding privacy, not to be compromised by the interests of businesses. One year later, Reding stated that in response to the consultation on RFID in 2006:

> '…the European Commission has made securing citizens' privacy on and offline a priority, but at the same time tried to balance it with the right approaches of not hampering their potential for business.'[8]

Privacy went from a value not to be compromised to a counterweight in the scale to balance against corporate interests. The emphasis was placed on a dialogue in which all stakeholders must actively engage to develop a win-win solution, 'where all concerned parties see an advantage in further deploying this useful and important technology'.[9] This phrase begs the question as to what would come of the position of those individuals that would fail to see the advantages of the IoT and refuse to be part of it. In other words, does IoT policy grant a choice to individuals or is it all-inclusive?

These quotes show the role of the Commission as a *policy entrepreneur*, in which it seeks to unite the interests of private and public actors in order to realise the common interest of European integration.[10] Despite the fact that the Commission is eager to include civil society in this process, it should be clear from the outset that in this role it tends to be servile to the actors which it needs to get 'on board' in order to make its plans succeed. The subtle shift in the Commissioner's quoted statements evidences the Commission's sensitivity to the voice of more powerful interests.

On 17 September 2010, the Vice-President of the Commission responsible for Justice, Fundamental Rights and Citizenship at the time, again Viviane Reding, lauded the Charter as one of the core elements of the new foundation of the Union:

[6] Viviane Reding, 'RFID: Why we need a European policy' (EU RFID 2006 Conference: Heading for the Future, Brussels, 16 October 2006).
[7] ibid.
[8] Directorate-General for the Information Society and Media (European Commission), *European policy outlook RFID* (final version, The Publications Office of the European Union 2017) 5.
[9] ibid.
[10] Michelle Cini, 'The European Commission: An unelected legislator?' (2002) 8 (4) The Journal of Legislative Studies 14.

> 'However, one thing must be clear: we cannot now sit back and rest on our laurels simply because the words have become law….we must now implement the Charter, breathe life into it and make sure it is effective in practice!'[11]

> 'The Charter must become the compass for all our EU policies. Particularly within the European Commission, the Charter will influence all actions of our services.'[12]

These quotes show another role of the Commission, that of the *guardian of fundamental rights,*[13] in continuation of its role as the guardian of the Treaties. Positioned in a policy field where it needs to yield to the desires of powerful actors with interests which can be at odds with fundamental rights, conflict between these two roles seems inevitable. The manner in which the Commission approaches such a conflict is of vital importance to the protection of fundamental rights as it is a key institution proposing and implementing EU law. The protection offered by rights, especially amorphous ones such as the right to privacy (and data protection in its wake), depend to a large extent on the interpretation and application of the right. The Commission's interpretation of the right naturally influences how it sees to its application and is, thus, also vital for its enforcement with respect to the design of mandatory IoT systems. This interpretation and applications takes place on different levels and stages of policy which will guide the structure of this chapter, namely policymaking (before the legislative acts), legislative acts, and delegated and implementing acts.

First is the pre-legislative phase. The Commission issues communications and recommendations on privacy and data protection in general, on the role of data in the future economy and those specifically tailored to the introduction of IoT systems. The analysis of these communications and recommendations is required in order to deduce the Commission's approach towards privacy and data protection.

Second, in the preparatory stage of a legislative proposal the Commission already examines the impact on fundamental rights in the impact assessment. It also considers the alternatives, partly on the merits of the potential impact on fundamental rights and eventually, through its legislative proposal it determines how personal data processing operations are to be executed. It is also at this stage that the Commission can follow up on opinions delivered by the Article 29 Working Party (WP 29).[14] The WP 29 has an advisory status, acts independently and its

[11] Viviane Reding, 'The importance of the EU Charter of Fundamental Rights for European legislative practice'(Lecture given at the German Institute for Human Rights, Berlin, 17 September 2010) 3.

[12] ibid 4.

[13] The protection offered by fundamental rights naturally focuses on individuals. Despite the fact that there are instances where businesses appeal to them, there should be no mistake about their main aim; the protection of citizens.

[14] The 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data' is established by Directive 95/46/EC (the Data Protection Directive) in Article 29, hence the name. It is composed of a representative of the supervisory authority or authorities designated by each member state and representative(s) of the authority/authorities established for the Union's institutions and a representative of the Commission.

competences are enumerated in Article 30 Directive 95/46.[15] It examines questions about the application of national measures adopted pursuant to the directive to serve their uniform application (1(a)), provides opinions to the Commission on the level of protection in the Union and in third countries (1(b)), gives advice to the Commission on proposed amendments of Directive 95/46, on additional or specific data protection measures and on proposed Union measures that might impact the right to personal data protection (all under 1(c)). The WP 29 never seems to miss a chance to publish opinions on a wide range of Commission measures, including those related to the IoT.[16] In performing this task, it advises the Commission on the interpretation of data protection legislation. The impact assessment in general and the opinions of the WP 29 will also be discussed in section 3. The purpose of this section is to illustrate the Commission's own view on how it should perform its tasks as the guardian of fundamental rights on the basis of its official rhetoric.

Finally, section 4 analyses the Commission's position as the executive responsible for implementing acts. The legislation introducing mandatory IoT systems confers executive power to the Commission that concern the design of these systems. The aim of this section is to establish the difficulty of this task for the Commission in the light of the problematic relationship between essential and non-essential elements of legislative acts, technical details of system design and the role of the European Standardisation Organisations (ESOs) as autonomous agents for developing IoT systems.

2. The Commission as a policy maker

One way in which the Commission moulds its' approach to the right to privacy and data protection legislation is through its communications and recommendations. In order for policy initiatives to be effective they need to be supported by legislation.[17] Nevertheless, the influence of recommendations and communications should not be underestimated either, because they allow the Commission to guide interpretation of specific legislation on IoT systems. Even though soft law in nature, these instruments have normative effects as they influence the application of the law to data processing operations by the addressees of these communications. These acts also hold the potential to create and perpetuate a certain vision

[15] Under the GDPR the name changed to the 'European Data Protection Board' and is instituted under Article 68 GDPR.

[16] Article 29 Data Protection Working Party, 'Working document on data protection and privacy implications in eCall initiative'(Adopted on 26th September 2006 1609/06/EN WP 125, The Article 29 Working Party 2006) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf> accessed 4 June 2018; Article 29 Data Protection Working Party, 'Opinion 12/2011 on smart metering' (Adopted on 4 April 2011 00671/11/EN WP 183, The Article 29 Working Party 2011) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf> accessed 4 June 2018; Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (Adopted on 16 September 2014 14/EN WP 223, The Article 29 Working Party 2014) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 4 June 2018.

[17] Nugent (n 5) 168.

by setting goals and commenting on set agendas, creating and addressing an epistemic community that follows this vision (especially in combination with funding).[18] Since these are authored by the Commission they carry the implicit authority of the EU-endorsed interpretation of legal norms embodied in Union legislation. The discourse of the Commission holds the power to set norms because it further elaborates on the management, supervision and implementation of the IoT policy in relation to other stakeholders. Therefore its interpretation shapes relationships between data controllers (e.g. public or private providers of IoT services) and data subjects.

These communications and recommendations can be divided into three approximate categories: on data protection and privacy in general, on the role of data in the future economy and on specific IoT systems, considered in turn below.

2.1 Communications on data protection and privacy in general

Over the last fifteen years, the Commission has issued a number of communications on data protection and privacy in general. As far back as 2003, the Commission issued a report setting a work programme for better implementation.[19] A few problems were already noted by the Commission back then, which it would return to in its later communications.[20] One such problem is the divergences in the legislation of Member States which complicate the free movement of personal data within the internal market. Other issues were the under-resourcing of national data protection authorities, fragmented compliance by data controllers and a low level of awareness among data subjects. The Commission firmly asserted the importance of enforcement, compliance and awareness for better application of the Directive. In later communications the Commission re-emphasised these points.[21] This time it came to the conclusion that there is a need for a new regulatory framework. The communications are quite similar and the sections – the individuals' rights, the dimension of the internal digital market, the use of data in police and criminal justice cooperation and the global dimension of data protection – largely overlap. In the 2010 communication there is an additional section on the need for stronger institutional arrangements for better enforcement, which focuses on the role of DPAs and the WP 29, which is found in the 2012 communication under the section on the digital single market. The Commission does not interpret specific data protection provisions, yet it holds that the core principles of Directive 95/46 are still valid and that the

[18] For a definition of 'epistemic community' see Peter M Haas, 'Introduction: epistemic communities and international policy coordination' (1992) 46 International Organization 1, 3. Haas gives this definition: "An epistemic community is a network of professionals with recognised expertise and competence in a particular domain and an authoritative claim to policy relevant knowledge within that domain or issue-area."

[19] Commission, 'First report on the implementation of the Data Protection Directive (95/46/EC)' (Report from the Commission) COM (2003) 265 final.

[20] Commission, 'A comprehensive approach on personal data protection in the European Union' (Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions) COM (2010) 609 final; Commission, 'Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century' COM (2012) 9 final.

[21] COM (2012) 9 (n 20).

introduction of new technologies calls for the clarification and specification of how these data protection principles should be applied to them.[22]

The Commission, furthermore, calls for individuals to be put in control of their data through asserting their subjective rights, improving the means to exercise these rights and reinforcing data security. The Commission's focus is on mechanisms that only become relevant once data is outside of the control of the data subject. This reveals the inclination of the Commission to apply data protection law after the initial recording of data. This way of applying data protection law is inadequate in protecting privacy at the core: the legislation's pliability in terms of the flexibility of the party that determines the purposes and means for the processing (the data controller) offers very limited protection against the initial recording of personal data. The necessity of the initial recording of the data is silently assumed, despite the fact it falls under the scope of EU data protection laws. If this necessity was rigorously tested, the control of individuals over their data could not be reconciled with the other ambition of the Commission: to make personal data a driving force of the economy. Apart from the right to be forgotten, no attention is paid to the capacity of data protection law to *prohibit* processing. Instead the focus seems to be on the justification of processing without due regard to the substantive norms of data protection.

With regard to the digital internal market the Commission formulated amongst others the ambition to eliminate unnecessary administrative practices for businesses (the cutting of red tape).[23] Here it already considered the introduction of a regulation in order to harmonise national differences, enhance the responsibility for data controllers through the introduction of policies and mechanisms that ensure compliance with data protection rules (introducing the 'accountability' principle) and increase the independence and powers of DPAs, and create conditions for more efficient cooperation among them. Another point emphasised by the Commission was that setting a practice of careful and diligent processing of personal data is key to gaining the trust of the consumer and thus forms an advantage in global competition for EU companies.[24] The ambitions of the Commission when it comes to the global dimension of data protection showed the will to promote the EU principles as the universal standard. On the one hand, the Commission sought flexible tools and mechanisms to facilitate international data transfers, while on the other hand it wanted a coherent and uniform approach. It wanted to expand the territorial application of data protection law:

> 'by specifying that whenever goods and services are offered to individuals in the EU, or whenever their behaviour is monitored, **European rules shall apply**'.[25] Other measures are

[22] In 2010 the Commission emphasised the importance of the principle of data minimisation for enhancing the individuals control and formulated the ambition to strengthen this principle. In 2012 it was lacking from the communication, yet this principle was introduced in the proposal for the GDPR and its final version.

[23] In 2010 it held that the current notification system to the DPA should be simplified. In 2012 it took the more firm position that it should be completely eliminated.

[24] COM (2012) 9 (n 20) 8.

[25] ibid 11. This can be seen as quite a radical reinterpretation of the territorial scope of data protection, which will prove hard to stick to in practice.

> setting clear criteria for 'adequacy decisions', harmonising rules on international transfers (e.g. Binding Corporate Rules) and engaging in dialogue with third countries and relevant international organisations 'to promote high and interoperable data protection standards worldwide'.[26]

The Commission's thoughts on privacy-enhancing technologies (PETs) and Privacy-by-Design (PbD) are particularly relevant. In 2007, the Commission articulated the ambition to enhance data protection through the promotion of PETs by setting a number of objectives.[27] These objectives consisted of supporting their development, use of available PETs by data controllers and encouragement of their use by consumers. On the one hand, it acknowledged that the aim of the legal framework on data protection is to minimise the processing of personal data. On the other hand, it stressed the following:

> 'The use of PETs should not prevent law enforcement agencies or other competent authorities from intervening in the lawful exercise of their functions for an important public interest. The responsible authorities should be in a position to access personal data where necessary to achieve those purposes and in accordance with the procedures, conditions and safeguards laid down by the law.'[28]

This could also be read as a rejection of encryption, or support for the idea that despite encryption (a PET) there should be a mandatory backdoor.[29] The Commission took a cautious approach and explicitly considers that PETs may be curbed by the need to safeguard public interests; an approach that defeats PETs purpose, since there is always a legitimate aim that can justify access to data.[30] It seems the Commission only applies the PETs to the access to data. It does not apply PETs to the first phases of data processing, i.e. the recording and collection of data. PETs are, thus, not applied in the phases where they would harness the most effect.

In a 2008 communication the Commission raised the question how to ensure that the rights to privacy and protection of personal data 'enshrined in European legislation, are adequately captured in the design and functioning of the Internet of Things?'[31] In the IoT action plan, under the heading 'Trust, Acceptance and Security', the Commission notes that privacy and information security should be taken into consideration in the design phase of IoT systems and confirms their importance in relation to trust and acceptance:

---

[26] ibid 2.

[27] Commission, 'Promoting data protection by privacy-enhancing technologies (PETs)' (Communication from the Commission to the European Parliament and the Council) COM (2007) 228 final.

[28] ibid 5.

[29] See for example: 'Europol chief warns on computer encryption' <http://www.bbc.com/news/technology-32087919> accessed 17 August 2016.

[30] As will be shown in the following section, to fuel the data driven economy would be one the Commission would deem legitimate.

[31] Commission, 'Communication on future networks and the internet' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2008) 594 final 12.

> 'It is therefore crucial that IoT components are designed from their inception with a privacy- and security-by-design mindset and comprehensively include user requirements…. Another key aspect to building trust is the capability to adjust the functioning and properties of technological systems to individual preferences (within safe boundaries). Studies have shown that giving users a sufficient level of control improves their level of trust and plays an important role in the uptake of technology.'[32]

The Commission does acknowledge the ability to design systems in a way that allows individual preferences with regard to privacy, the responsibility that follows for the parties that design these systems and how this is crucial for trust. It also recognises the necessity to address these qualities at the design stage.

In a 2012 communication, the Commission encourages reinforcement of data security through PETs, which are here described as 'technologies which protect the privacy of information by minimising the storage of personal data'.[33] If the storing of data cannot be avoided, the location of storage becomes pivotal to the protection of privacy.[34] The Commission also mentions introducing the PbD principle to 'make sure that data protection safeguards are taken into account at the planning stage of procedures and systems' under the heading of enhancing the accountability of those processing data.[35]

Despite the title of this communication – *Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century* – the Commission does not mention Article 7 of the Charter or Article 8 ECHR, merely referring to Article 8 of the Charter and 16 (1) TFEU which enshrine the right to the protection of personal data. The most important provisions on the right to privacy in the EU, thus, do not feature in the communication on safeguarding this right in the 21st Century. Neither does the Communication explicitly provide whether, and if so how, the data protection legislation is supposed to fill this void. The Commission simply states that it will only observe data protection legislation apparently assuming that the right to privacy can be protected effectively through the application of data protection legislation.[36] The differences in the scope of these two rights and the requirements on their limitations necessitate including the right to privacy in preparing and implementing its policies and legislation concerning mandatory IoT systems.[37]

---

[32] COM (2009) 278 (n 2) 6.

[33] COM (2012) 9 (n 20) 6.

[34] Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth and others (eds), *Data Protection in a Profiled World* (Springer 2010).

[35] COM (2012) 9 (n 20) 7.

[36] You can see this in the action plan, In European Commission, 'When your yogurt pots start talking to you: Europe prepares for the internet revolution' (IP/09/952 Press Release, Brussels, 18 June 2009) <http://europa.eu/rapid/press-release_IP-09-952_en.htm> accessed 4 June 2018.
and it is generally a recurring theme in any communication from the Commission on the IoT.

[37] The scope and requirements for limitation of the right to privacy and data protection were discussed in Chapter 2 and 3 respectively.

2.2 The role of data in the future economy

With the advent of ICT-systems and their influence on the organisation of society, the free movement of personal data across national borders became necessary for the functioning of the internal market. In the wake of the traditional four freedoms in the pre-digital era – the free flow of goods, services, capital and workers – the fifth freedom was required: the free flow of personal data. To this end, Directive 95/46/EC was adopted. While this directive still left considerable space for a Community in which laws on the processing of personal data were fragmented, the General Data Protection Regulation further harmonised the rules amongst Member States.[38]

The Commission seems to take a conservative attitude in its communications on data protection in general, but it seems less reserved in its work conducted on the role of data in the future economy. This is exemplified in a study financed by the Commission advocating for the reuse of public sector information, which is also actively stimulated through regulatory reforms amongst others.[39] In the *Review of recent studies,* it is shown that private databases (such as those held by banks) are linked to public databases (such as those held by tax authorities) to fight fraud.[40] Private parties like insurance companies also show an interest in the reuse of this type of data to reduce fraud. The data could be used by insurance companies to 'help customers to ensure they have the appropriate coverage'.[41] The cross-checking of databases of banks and tax services without awareness of the data subject is a major interference with the right to privacy. It is a big shift from a conservative approach to data protection legislation, under which these type of practices are illegal, because they result in a breach of the purpose limitation principle.

In 2014, the Commission adopted a new communication *'Towards a thriving data-driven economy'*, which was a reaction to, inter alia, the European Council's call to 'provide the right framework conditions for a single market for big data and cloud computing'.[42] Here as well, the increasing digitisation of public services is seen as an opportunity for increased innovation, sided by the remark on the necessity of trust for this data-driven economy. Two of the actions the EU should take to compete in the global data economy are:

[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.

[39] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information [2013] OJ L 175/1 (hereinafter Directive 2013/37/EU).

[40] Graham Vickery, 'Review on recent studies on PSI reuse and Related Market Developments' (final version) <https://ec.europa.eu/digital-single-market/en/news/review-recent-studies-psi-reuse-and-related-market-developments> accessed 4 June 2018.

[41] ibid 23.

[42] Commission, 'Towards a thriving data-driven economy' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2014) 442 final 1.

- ‘make sure that the relevant legal framework and the policies, such as on interoperability, data protection, security and IP are data-friendly, leading to more regulatory certainty for businesses and creating consumer trust in data technologies;
- rapidly conclude the legislative processes on the reform of the EU data protection framework, network and information security and support exchange and cooperation between the relevant enforcement authorities (e.g. for data protection, consumer protection and network security).’[43]

The digitisation of public services is put forward as an area of new opportunities to optimise data storage, transfer, processing and analysis.[44] Explicit mention is made of the effect on public trust of reported use of similar technologies for surveillance purposes by public and private actors, which the Commission promises to address enacting effective data protection, network and information security rules.[45] There are two problems in this respect. First, the strength of rules on data protection depends upon the will of the parties they are imposed upon to abide by them and upon the intensity with which they are enforced. Second, the national legislator can circumvent rules drafted at the EU level, despite the Commission's promises with regard to their protection. This observation applies to data protection rules in general, as well as data protection rules provided in sector-specific legislation (e.g. legislation on biometrics in passports).[46] The new GDPR contains a provision which gives the legislator of both Member States as well as the EU the freedom to deviate from substantial data protection norms provided by the GDPR, like purpose specification.[47] The intended harmonising effect of the GDPR will not bring relief in this respect, worse yet, it will aggravate the issue.

In the Commission’s communication on the data-driven economy explicit reference is made to the IoT linked to the ambition to fund large-scale projects aimed at answering questions concerning availability, quality and interoperability of data collected through smart objects. An implicit reference to the IoT is made in a section on *open standards* which is mentioned as a priority in Commission policies together with *data interoperability*. The adoption of these qualities is meant to facilitate the exchange of open data, inter alia in the areas of smart grid, health, transport and financial services, all considered big data areas.[48]

The storage of data in a European cloud aims to contribute to the accessibility of massive volumes of data, which then can be utilised by big data applications. The introduction of IoT systems will lead to the increase of the processing of personal data. Smart cities, smart grids, smart transport and smart health are recurring themes on the Commission’s agenda.[49] The

[43] ibid 3.
[44] ibid.
[45] ibid.
[46] Tijmen HA Wisman, 'Giving Member States the Prints and Data Protection the Finger’ (2015) 1 European Data Protection Law Review 245.
[47] Article 6(3)(4) GDPR. See Chapter 3, section 2.3.
[48] COM (2014) 442 (n 42) 9.
[49] See Smart Mobility and Living (Unit H2) ‘Smart Cities’(Policy, Digital Single Market, 2018) <http://ec.europa.eu/digital-agenda/en/smart-living> accessed 4 June 2018; Internet of Things (Unit E4) ‘The

way in which these systems are expected to contribute to irrigating personal data throughout the global information society is captured in a paragraph on the IoT in the following communication from 2008:

> 'These technologies will progressively create an almost invisible infrastructure, with far-reaching capabilities organized into global systems that serve society as a whole and our information and decision-making needs in adaptive and dynamic ways.'[50]

'Big data', 'availability of data and interoperability' and improved framework conditions for data sets that flow across sectors and national borders without inappropriate restrictions in order to facilitate value generation, are just some of the terms that make their appearance in this report. The focus of these communications, supported by the European Council, is to increase the value of data for the benefit of the economy. This increase of value is gained through making data interoperable across a wide spectrum of sectors, which means they can be used and re-used for a multitude of purposes. The Commission's ambitions are fuelled by corporate interests which results in an obvious tension with the other ambition of the Commission, discussed in the previous section, to put the individual in control over his data.[51] In addition, these ambitions are irreconcilable with the principle of purpose limitation.[52]

Extracting value out of IoT systems is explicitly considered in the latest communications of the Commission, both with a clear focus on energy and transport[53] The Commission frames 'restrictions on the free movement of data' as 'likely to constrain the development of the EU data economy' and announces the initiative 'to tackle restrictions on the free movement of data'.[54] In the context of IoT it holds that the diversity of data 'generated by these machines

---

Internet of Things', (Policy, Digital Single Market, 2018) <http://ec.europa.eu/digital-agenda/en/internet-things> accessed 7 June 2018.

This shows these themes fall under different branches.

[50] COM(2008) 594 (n 31).

[51] On page 4 of General Secretariat of the Council, 'Conclusions 24/25 October 2013'(EUCO 169/13 CO EUR 13 CONCL 7, European Council Conclusions 2013) that the Commission refers to in this communication has the following interesting line on the modernisation of public administrations: 'EU legislation should be designed to facilitate digital interaction between citizens and businesses and the public authorities. Efforts should be made to apply the principle that information is collected from citizens only once, in due respect of data protection rules.' It is unclear how the European Council intends to do this, yet it seems like the only way would be to change current legislation.

[52] Data protection legislation allows secondary use when this is not incompatible with the original purpose. The new GDPR, however, provides the possibility to Member States to adopt laws which allow incompatible use, or any other deviation from the rules laid down in the Regulation, for anything in the public interest. See Chapter 3, section 2.3.

[53] Commission, 'Building a European Data Economy' (Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2017) 9 final 8; Commission, 'on the Mid-Term on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All' (Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2017) 228 final.

[54] COM (2017) 9 (n 53) 3.

or processes presents rich opportunities for players in the data market to innovate and apply insights into this data'.[55] In the future EU framework for data access to anonymous machine-generated data is considered to be a source of value-creation.[56] This requires the anonymisation of this data to turn it non-personal, which occurs according to a document for Commission staff 'if identifiers linking the data to a natural person have being taken away and re-identification is not possible'.[57] From this future scenario it can be inferred that this data is first collected as personal data, before it is anonymised. The Commission indicates it is involved in stakeholder dialogues in which it discusses different levels of intervention: access by business is considered to 'non-personal data', yet access for public interest is considered to simply 'data'.[58] The most recent development is a proposal for a Regulation on the free flow of non-personal data, which refers to the IoT in the opening sentence of its Explanatory Memorandum.[59]

Let's return to the case law of the CJEU in which the format of data and the information which can be inferred from it, through cataloguing and profiling, were recognised as relevant for the sensitivity of data. This type of cataloguing and profiling is also possible in the envisioned clouds of the EU, fuelled by the data collected through mandatory IoT systems. Data only becomes knowledge after some form of analysis. Hence, the extent to which a data format allows analysis, with minor effort and maybe even without, or with little, human intervention, is decisive for the ease with which data can be transformed into knowledge. The format of the data, therefore, feeds back into the nature of the information that can be inferred from it. The European Commission's ambition to make data generated by IoT systems interoperable facilitates the potential of this data to profile and catalogue entire populations, although this is cloaked in the technocratic jargon which foresees that systems 'allow an adequate level of interoperability so that innovative and competitive cross-domain systems and applications can be developed'.[60]

2.3 Communications and recommendations addressed to IoT systems

Before the Commission issues a legislative proposal on IoT systems, it usually first tests the water by a communication.[61] Another instrument it uses in different manners is recommendations. In both cases the Commission shows a willingness to address privacy issues, yet it does so consistently through the reliance on data protection legislation as the

[55] ibid 8.
[56] ibid 11.
[57] Commission, 'on the free flow of data and emerging issues of the European data economy', SWD (2017) 2, 26.
[58] COM (2017) 9 (n 53) 12.
[59] Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, COM (2017) 495 final.
[60] COM (2009) 278 (n 2) 9.
[61] The IoT systems will be further elaborated on in Chapter 5 and 6.

instrument to solve issues related to privacy. Whether it is about RFID,[62] Intelligent Transport Systems (in which privacy is not mentioned at all),[63] or the smart meter,[64] the pattern is clear: a general instruction to respect data protection legislation is the way the Commission addresses privacy concerns. In the communications on smart meters and eCall, the two IoT systems mandated through EU law, the Commission does not adhere to its own call to clarify and specify how core data protection principles should be applied to newly introduced technologies.[65] Especially the principles with prohibitive potential are neglected in the Commission's work. This lacuna can be explained either by the lack of coordination within the Commission in its work on the protection of fundamental rights. Alternatively, it can be explained by the fact that a correct application of principles such as data minimisation and purpose limitation is irreconcilable with its own vision on the role of data in the future economy. It pays lip service to data protection without clarifying the principles which have the potential to impose substantive demands on the design of IoT systems.

In the action plan on the IoT, the Commission does confirm the importance of both data protection and privacy in the IoT, yet it positions data protection as the instrument to deal with privacy issues.[66] It is important to note that it at least recognises that this is an essential element of IoT policy. Although the Commission does not make this method explicit it is consequent in its approach. Through its communications it systematically neglects the difference between the protection offered by the right to privacy and data protection legislation.

2.4 Taking stock of the Commission's role as a policymaker

The attitude of the Commission towards privacy and data protection in general and specifically within the IoT is ambivalent and slightly opportunistic.

The Commission repeatedly designates data protection legislation as the tool to deal with privacy concerns. This approach contributes to the systematic neglect of the right to privacy. The differences between the right to privacy and data protection legislation (see Chapters 2 and 3) demonstrate that their scope and substance are far from identical. By excluding the right to privacy from its armamentarium, the Commission omits it from the catalogue of fundamental rights it is supposed to protect. From the perspective of the guardian of fundamental rights, this amounts to the surrender of its most powerful weapon. From the

[62] Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification [2009] OJ L 122/47, 4.

[63] Commission, 'Action Plan for the Deployment of Intelligent Transport Systems in Europe' (Action plan) COM (2008) 886 final. It should be noted that this action plan was issued before the Commission's call in 2010, however, the silence on the appliance of core data protection principles is perpetuated in all the other work of the Commission on eCall. This will be further discussed in Chapter 6.

[64] Commission Recommendation 2012/148/EU on preparations for the roll-out of smart metering systems [2012] OJ L 73/9.

[65] COM (2010) 609 (n 20) 3. This will be further elaborated on in Chapter 5.

[66] COM (2009) 278 (n 2) 6.

perspective of policy entrepreneur, it amounts to ignoring the most important rule in the book in order to please the commercial parties it wants to keep close.

The choice of the Commission to rely on data protection legislation solely seems to be fuelled by the desire to facilitate the interests of companies, rather than to defend the rights of citizens. This legislation is not the suitable instrument to guide the conflict ridden area of interests in IoT policy, because it invites a biased interpretation which justifies the processing of personal data without questioning its necessity, particularly in the phases of recording and storage. The data protection rhetoric of the Commission plays into the hands of corporate interests, rather than to uphold citizens' rights. This approach to data protection by the parties responsible for the design of IoT systems is unlikely to result in anything close to PbD, but will probably result in what can be coined data security-by-design.[67]

The problem of the Commission's reliance on data protection legislation becomes especially poignant in light of all its communications in which the future role of data is envisioned. Where paragraph 2 of Article 8 ECHR sets strict demands for public authorities to interfere with the right to private life, data protection is more flexible, pursuing practical relations between citizens on the one hand and governments and companies on the other. Key to the validity and legitimacy of this different legal regime is the purpose limitation principle, which as discussed above requires 'that personal data must not be processed further to collection in a way incompatible with the specified, explicit and legitimate purposes for which those data were collected'.[68] Viewed in the light of these reports this principle is breached by current practices which will extend to data produced in the IoT. More than that, it seems the Commission views exactly this further processing incompatible with the original purpose as a central feature of the IoT. Purpose limitation is central to the protection offered by data protection law, because it imposes a substantive limit on the exercise of power,[69] which results in respect for the contextual integrity of a data processing operation. If the current state of affairs is observed critically, it is evident that the hands and feet that data protection legislation aim to give to the right to privacy will be amputated in the future network society, leaving the data subject without any real substantive protection. A data subject still convinced of his ability to defend himself against this force must be as stubborn as Monty Python's black knight yelling 'it is merely a fleshwound!', while it is clear to the common observer he is chopped into bits and pieces.[70]

In conclusion, these communications show a shapeshifting Commission which mostly ignores the right to privacy and whose attitude towards data protection defies its very substance. The Commission wants the impossible: to give control to citizens over their data and freedom to companies and governments to (re-)use this data. The Commission relies on data protection as a tool to deal with concerns about privacy, but wilfully ignores the point that the type of data usage it envisions in the IoT, reproduces the same circumstances that

[67] See also the conclusion of Chapter 3.
[68] Recital 11 of Directive 2013/37/EU.
[69] Serge Gutwirth, *Privacyvrijheid! De vrijheid om zichzelf te zijn* (Rathenau 1998) 114.
[70] Python (Monty) Pictures, 'Monthy Python and the Holy Grail' (1975).

provoked the ECtHR to grant Malone the protection of Article 8 against the British government some thirty years earlier.[71] The preservation of the contextual integrity is the legal fundament to justify the processing of personal data. When an exception is made to this confidentiality within the usual relationship and data is used against the data subject a foreseeable legal basis needs to be in place in line with the requirements discussed in Chapter 2 to justify this exception. In the future envisioned by the Commission this data is involuntarily collected, stored and made accessible by default. The confidentiality of personal data is sacrificed for potential utility. Through the language of data protection, the Commission seeks to do the impossible: to reconcile the goal of giving citizens control over their own data, whilst allowing companies and governments to use this data.

3. The Commission in the legislative process

To interfere lawfully with the right to private life, the legislative act concerning the introduction of these systems has to meet the requirements provided in Article 52(1) Charter when setting the parameters to the design of mandatory IoT systems. The Commission participates in the exercise of the legislative power in a number of ways, in which it implicitly or explicitly interprets the right to privacy.[72] It plays an important role in this part of the process — particularly in the impact assessment and the legislative proposal —where it can critically evaluate matters of system design.

The law authorising the installation of these systems governs their design in two important ways. First, it establishes, to a varying degree of detail, certain functions a system should perform and thus forms a basic instruction for its design. Second, this law sets the quasi-legislative framework partly governing the relationship between the Commission and ESOs in which they negotiate the standards regulating the design of an IoT system.[73]

The aim of this section is to demonstrate the Commission's practice as well as stated ambitions to take fundamental rights into account throughout this process. This section covers the Commission's duty to guard fundamental rights in its preparatory work which precedes a legislative proposal, the proposal itself and the legislative process. The special relationship between the Commission and the WP 29 is also explored below. The final subsection will address the possibility for the Commission to propose additional regulatory instruments.

3.1 Assessing fundamental rights impacts in a legislative proposal

With the signing of the Lisbon Treaty the Commission's task of guardian of the Treaties was extended to the Charter of Fundamental Rights. Mere respect for fundamental rights is no

[71] *Malone v The United Kingdom* App no 8691/79 (ECtHR, 2 August 1984).
[72] The legislative acts that see to the introduction of IoT systems are treated in Chapter 5 and 6.
[73] This will be further discussed in section 4.

longer sufficient, as in the Commission's view the EU should fulfil an exemplary role by making the Charter rights '*as effective as possible*'.[74] The way this ambition was formulated resonates with the principle of effectiveness from the ECtHR case law as discussed in Chapter 2. The Charter should enable people to enjoy their rights whenever 'they are in a situation governed by Union law'.[75] This is also deemed important for 'public confidence in the Union's policies'.[76] The Commission's ambitions are of particular significance for the legislative proposal which mandates the installation of IoT systems, as they show the Commission's willingness to make the rights in the Charter as effective as possible, which in turn should translate into certain requirements imposed on the design of these systems. One of such requirements is that IoT systems do not unnecessarily introduce interferences or risks to interferences with Article 7 and 8 of the Charter. In order to realise the ambition of the Charter to be(come) 'a living instrument', the Commission undertook the duty to use horizontal policy programming instruments, inter alia the impact assessment and the explanatory memorandum:

- 'the impact assessment, which should include as full and precise a picture as possible of the different impacts on individual rights…'
- 'the explanatory memorandum, which for certain legislative proposals should contain a section on the legal basis for compliance with fundamental rights…' [77]

Impact assessment[78]

The impact assessment serves to 'further reinforce and systematise the practical aspects of scrutiny at the interdepartmental consultation stage' and is of great importance, since the 'conformity of Commission actions with fundamental rights is a primary aspect of their constitutional legality'.[79] Legislative initiatives by the Commission that have a specific link with fundamental rights need to be accompanied by an assessment in which these impacts are established. The Commission sets out the guidelines for a methodology to ensure that the Charter is 'properly implemented in Commission proposals'.[80] The most relevant objective of this methodology is 'to allow Commission departments to check systematically and thoroughly that all the fundamental rights concerned have been respected in all draft proposals'.[81] The impact assessment serves as the groundwork for a legislative proposal and

[74] Commission, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'(Communication from the Commission) COM (2010) 573 final 3.
[75] ibid 3.
[76] ibid 4.
[77] Already in: Commission, 'European Governance: A White Paper' COM (2001) 428 final, impact assessments were proposed as a means for the Commission to improve the quality of policy proposals, C-287/25.
[78] This section is based on the discussion of impact assessments in Tijmen HA Wisman, 'eCall and the Quest for Effective Protection of the Right to Privacy' (2016) 2 European Data Protection Law Review 59.
[79] Commission, 'Compliance with the Charter of Fundamental Rights in Commission legislative proposals: Methodology for systematic and rigorous monitoring'(Communication from the Commission) COM (2005) 172 final 3.
[80] Ibid 2.
[81] Ibid 3.

should be executed when this proposal is in its early development.[82] It provides analysis for 'later legal control'.[83] The Commission claims it seeks to promote a fundamental rights culture, which it underscores itself as the 'essential underpinning of the detailed examination of the necessity for and proportionality of the proposals that the Commission puts forward'.[84] More broadly, it refers to the relevance of the standards set in ECtHR and CJEU case law when examining the legality of interferences with fundamental rights.[85]

The execution of an *impact assessment* consists of a number of steps in which the drafter of the assessment must establish the problem, the policy objectives, the policy options and the likely impacts.[86] In the context of IoT systems the problem and policy objectives are usually not concerned with privacy, but with matters such as energy efficiency and road safety. An initial assessment of the impact of different policy options on fundamental rights can help to discard the options which would clearly result in interferences with fundamental rights that cannot be justified.[87] At a later stage the assessment, usually executed upon alternative policy options to compare the different impacts, can help in choosing the option which does not limit fundamental rights, or does so only to a minimal extent.

In the analysis of the impact the Commission has to fully identify the impacts on fundamental rights and make a qualitative assessment.[88] It should be noted that the Commission guidelines explicitly mention 'individuals, private and family life, personal data' amongst the key questions for social impact and that negative impacts should be identified in order to see whether measures can be introduced to mitigate these impacts.[89] The assessment has to establish the intended benefits, but also the direct costs as well as the negative impacts both intended and unintended.[90] Unintended negative impacts are of particular significance for the mandatory installation of IoT systems, since these systems can introduce vulnerabilities and data processing operations which can be exploited in unforeseen ways by third parties at a later stage.[91]

The Commission has to assess the *likelihood* of the negative impact by taking into account factors that do not fall under the control of the parties managing the intervention. One of these factors is the extent to which the system and the data generated by the system can serve different functions, i.e. function creep. The Commission staff also has to consider the

[82] Commission 'Report on the practical operation of the methodology for a systematic and rigorous monitoring of compliance with the Charter of fundamental rights' (Report from the Commission) COM (2009) 205 final, 7.
[83] ibid 7.
[84] COM (2010) 573 (n 74) 5.
[85] COM (2009) 205 (n 82) 7.
[86] This is the order chosen in the Commission, 'Impact Assessment Guidelines' SEC(2009) 92.
[87] This corresponds to the 'less restrictive alternatives'-test , a sub test of the proportionality test.
[88] SEC (2009) 92 (n 86) 38.
[89] Commission, 'Operational Guidance on Taking Account of Fundamental Rights in Commission Impact Assessments'(Commission Staff Working Paper) SEC(2011) 567 final 11-18.
[90] SEC (2009) 92 (n 86) 38.
[91] This can be linked to the case law of the CJEU and ECtHR and the factors discussed in Chapter 2, section 2.1. In particular the factor *Future privacy violations*.

magnitude of this impact by taking into account aspects such as the socio-economical context. The significance of the impact can be established on the basis of these two factors. The guidelines provide that the Commission officials should keep in mind the short-term and long-term impacts, not overlook impacts other than monetary and quantitative ones and should be aware of the interaction between the factors that influence the impact.[92] This part of the guidelines establishes a positive obligation for the Commission to explore negative impacts that cannot be readily foreseen.[93] This makes the impact assessment, at least in theory, a suitable instrument to explore the unforeseen surveillance and control potential of an IoT system.

In the Operational Guidance the Commission does elaborate on the requirements following from the Charter and ECHR.[94] It establishes that in case of a negative impact it should be tested whether this impact is necessary to achieve the objective of general interest recognised by the Union or to protect the rights and freedoms of others, and in the latter case to identify these.[95] Also, it should be established that the means are appropriate to realise the objective and do not go 'beyond what is necessary to achieve it, and in particular is there an alternative that is equally effective but less intrusive'.[96] This can be linked to other Commission documents in which it establishes that during the drafting of the legislative proposal standards of *necessity* and *proportionality* are tested, which the Commission explicitly links with the standards that follow from ECtHR and CJEU case law.[97] It means that design features which avoid both the processing of personal data and the introduction of vulnerabilities are to be preferred to design features which do not. These standards are crucial for an answer to the question if the interference with Article 7 and 8 of the Charter can be justified.[98]

When the negative impact cannot be prevented, it should be formulated in a clear and predictable manner, thereby sufficiently clarifying the scope of any discretion granted to authorities and the modalities of exercising it in order to prevent arbitrary decisions by public authorities.[99] This corresponds to the requirement of foreseeability. If all these conditions are met, the *interference* can be *justified*, if not it results in a *violation.*[100] This is a clear-cut instruction to Commission officials responsible for performing impact assessments to include the requirements that follow from the ECtHR and Charter in their work. The Operational Guidance sets another important duty for the Commission officials which, also, corresponds to the requirement of foreseeability and safeguards from ECtHR and CJEU case law:[101]

[92] SEC (2009) 92 (n 86) 38.
[93] Here the Commission could use the factors discussed in Chapter 2, section 2.1.
[94] SEC (2011) 567 (n 89).
[95] SEC (2011) 567 (n 89)18.
[96] ibid.
[97] COM (2009) 205 (n 82) 7.
[98] COM (2005) 172 (n 79) 7.
[99] SEC (2011) 567 (n 89) 18.
[100] ibid 9.
[101] ibid.

> 'If a policy option has a negative impact on fundamental rights, consider and identify which safeguards might be necessary to ensure that the negative impact would not amount to a violation of these fundamental rights. For instance, the requirement that any limitation of the identified fundamental right would need to be provided for by law (i.e. in the legislative proposal) and formulated in a clear and predictable manner as well as other effective safeguards. When *considering effective safeguards that could mitigate the negative impact on a fundamental right* of a given policy option, it is necessary to develop the type and content of these safeguards. In this way, the Impact Assessment will provide *concrete elements* to guide the drafting of the legislative proposal and the legal assessment of the proposal which will have to be made at a later stage. Merely referring to general safeguards is not sufficient.'[102]

'*Effective safeguards that could mitigate the negative impact on a fundamental right'* can be adopted in a legislative proposal mandating the installation of IoT systems. These safeguards could contribute primarily to the effective protection of the right to privacy and secondarily the protection of personal data.[103] Support for this view can also be found in the Commission's call (mentioned in section 2.1) to clarify and specify the application of core data protection principles to the introduction of these new systems. The most effective of these safeguards would be mandatory PETs that would mitigate the negative impact, instead of regulating it further 'downstream'. In combination with the duty to find equally effective but less intrusive alternatives, this instruction amounts to a duty for the Commission to establish requirements for a design which limit the interference with the right to privacy to the minimum necessary to attain the purpose of its installation. To the extent that data processing is necessary the Commission can require design features following from data protection law, such as minimising the data collected and retained, as well as facilitating the data subject's right of access to her or his data.[104] This working method bears close resemblance to the notion of PbD, an approach to system-design that takes privacy as the point of departure, as opposed to the ineffective approach that tries to fix privacy-issues after the system has been designed. A distinction should be made between elements that prevent interferences and elements that minimise the effects. It follows from the Commission's communications that these effective safeguards should already be addressed in the explanatory memorandum of the legislative proposal.[105]

The demands for system design that follow from applying the aforementioned requirements are referred to hereafter as *concrete elements of the design*. In order to ensure the effective protection of the right to privacy these would have to be adopted in the legislative proposal. This would be in line with the Commission's ambitious agenda to make the rights contained in the Charter as effective as possible and to address the full spectrum of potential negative impacts, whether intended or unintended.[106]

[102] Emphasis added, SEC (2011) 567 (n 89)18.
[103] COM (2009) 205 (n 82) 7.
[104] In doing so the Commission would comply with the sub-test of necessity which follows from the proportionality test in Article 52(1) CFEU.
[105] COM (2010) 573 (n 74) 8.
[106] ibid 3.

The explanatory memorandum of legislative acts with a particular link with fundamental rights must summarise why the proposal is compatible with the Charter.[107] This summary must reflect the recitals, which need to address the specific fundamental rights that are interfered with and why this would be justified under Article 52 of the Charter. This should address the issue whether the interference could not be mitigated through the adoption of effective safeguards. Interferences with fundamental rights that follow from the legislative proposal are amenable to judicial review. Addressing these interferences as well as the safeguards in the recitals should provide insight into the reasoning behind the act and facilitate possible judicial review.[108]

Pitfalls of the impact assessment

Two considerations in the guidelines are especially relevant to the level and scope of the impact assessment: the significance of likely impacts and the political importance.[109] The significance of the impact is proportionate to the level of analysis. Establishing this is not always as straightforward as establishing which fundamental rights are affected by the IoT system introduced in the legislative proposal.[110] When the initial processing of personal data is only considered within the specific context for which the IoT system is deployed, it might not be considered a grave interference with the right to privacy. The IoT system can be equipped with features or introduce vulnerabilities which can be used to facilitate further interferences introduced in later EU or Member State legislation.[111] If these further interferences or vulnerabilities do not reside within the ambit of the anticipated legislation, they are unlikely to be considered in the assessment.[112] In other words, potential future privacy violations as a result of secondary use of IoT systems should be part of the impact assessment.

Another problematic aspect of the assessment is that it focuses on the main legislative act, while the significance of the impact can be hidden in the tail of the legislation; the implementing or delegated acts. The Commission does articulate the ambition to pay attention to these acts and subject them to scrutiny already at an early stage.[113] It is impossible to assess, however, that which is not there yet. If features of the design are left to the discretion of parties other than the legislator and are of a complex technical nature, it remains to be seen if the potential impact on fundamental rights will be noticed. On a more practical level, privacy needs to be taken into account in the early stage of the development of

[107] ibid 8.
[108] ibid 7.
[109] These also correspond to the criteria used by the CJEU to establish what part of a legislative act constitutes an essential element, see section 4.1.
[110] 'What fundamental rights are affected?' is the first question of the Fundamental Rights 'Check-List'.
[111] See Chapter 2, section 2.1.
[112] This is despite the Commission's ambition to include unintended negative impacts in the assessment.
[113] COM (2009) 205 (n 82) 7; COM (2010) 573 (n 74) 6.

a system. This exposes a tension between protection of the right to privacy and the reserve of the legislator to deal with complex, technical issues.

In its Operational Guidance, the Commission advises those who execute the impact assessment to develop a deeper understanding of fundamental rights through the case law of the CJEU and the ECtHR when this 'proves necessary in the course of [the] Impact Assessment'.[114] The 'fundamental rights reflex' the Commission envisions in its own policymaking should result in testing the negative impacts against the key requirements developed in ECtHR case law. This case law is voluminous and complicated and its application to complex, technical issues inevitably leads to novel interpretation and application of these rights. To test the key requirements following from this case law on policy alternatives involving complex socio-technical issues is not an easy task. One of the questions to be addressed here is whether the measures the Commission foresees to ensure the readiness of its staff, e.g. through internal training,[115] will guarantee a sufficiently thorough level of understanding to realise the fundamental rights ambitions the Commission aspires to.

All Commission departments should use the check list in Figure A which intends to 'make it easier to understand the methodology for addressing questions on fundamental rights'.[116]

Fig. A [117]

Fundamental Rights 'Check-List'

1. *What fundamental rights are affected?*
2. *Are the rights in question absolute rights (which may not be subject to limitations, examples being human dignity and the ban on torture)?*
3. *What is the impact of the various policy options under consideration on fundamental rights? Is the impact beneficial (promotion of fundamental rights) or negative (limitation of fundamental rights)?*
4. *Do the options have both a beneficial and a negative impact, depending on the fundamental rights concerned (for example, a negative impact on freedom of expression and beneficial one on intellectual property)?*
5. *Would any limitation of fundamental rights be formulated in a clear and predictable manner?*
6. *Would any limitation of fundamental rights:*
   - *be necessary to achieve an objective of general interest or to protect the rights and freedoms of others (which)?*
   - *be proportionate to the desired aim?*
   - *preserve the essence of the fundamental rights concerned?*

[114] ibid.
[115] COM (2010) 573 (n 74) 6.
[116] SEC (2011) 567 (n 89) 6.
[117] SEC (2011) 567 (n 89) 7.

What stands out in this check-list (figure A) is the absence of four important requirements.[118] First, there is no clear elaboration on the demand of foreseeability. The fifth question whether any limitation of fundamental rights is formulated in a clear and predictable manner attempts to produce this, but it is incomplete. As discussed in Chapter 2, foreseeability requires that the scope and manner in which the competence limiting the fundamental right can be exercised is provided with reasonable clarity.[119] Second, the final point of the check-list provides three questions on proportionality without addressing the necessity of the interference, namely whether there are alternatives which do not limit or limit the fundamental right(s) to a lesser extent. The third requirement missing is that breaches of fundamental rights can only be justified if they 'genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.[120] Without establishing the purpose of the interference it is impossible to give an accurate answer to the proportionality of the means to realise it. The fourth omission in this check-list is the duty to establish adequate safeguards once an interference with a fundamental right is established. These requirements are further elaborated in the same document, only eleven pages later.[121] This is surprising since this list, according to the Commission, should make it easier for all Commission departments confronted with questions on fundamental rights to understand the 'basics of this methodology', which 'are further explained in the following explanation'.[122] Despite these glaring gaps, the ambitions of the Commission should be welcomed. The Charter is not a mythical document that magically corrects any fundamental rights violations enshrined in EU legislation.

The final pitfall concerns the policy environment of Commission employees responsible for performing the impact assessment. A legislative proposal often follows years of policy-making, including elaborate negotiations with stakeholders. Commission communications sometimes indicate that the major decisions with respect to policy are already taken. Furthermore, the impact assessment is executed by Commission employees whose conception of data protection and privacy will likely be affected by the rhetoric of the Commission discussed in section 2. These considerations raise the question whether the impact assessment allows for genuine proofing of fundamental rights, or whether it is destined to be a mere box-ticking activity.

3.2 Guarding fundamental rights in the legislative process

The coming into force of the Lisbon Treaty made the Charter legally binding on the legislative institutions of the Union.[123] The Commission is responsible for the first drafts of

[118] These requirements occur in the same document only eleven pages later, but are absent in this 'Check-List'.
[119] See also *MM v The United Kingdom* App no 24029/07 (ECtHR, 13 November 2012) para 194.
[120] Article 52(1) CFEU.
[121] The Commission's considerations about avoiding negative impacts and mitigating them, occurring in the same document only eleven pages later, do not occur in this 'Check-List'.
[122] SEC (2011) 567 (n 89) 7.
[123] Article 6(1) TEU.

EU legislation which are then subject to amendments by the Council and the EP. The Commission has a duty to examine the legality of the proposal, and the compatibility with the Charter.[124] Although the Commission is no longer the master of a proposal once it is released, it can exercise considerable influence by dedicating careful attention to the right to privacy in the first draft. The drafting of a proposal can be guided by the *concrete elements of design* which follow from a carefully executed impact assessment. Adopting these elements in the legislative proposal, which can avoid or mitigate the violation of the right to privacy by an IoT system, would be a welcome step in guarding fundamental rights in the legislative process. Furthermore, the Commission expressed the ambition to take the Charter into account in the process following the initial proposal, including by defending the standards contained in the proposal in the face of amendments of the co-legislators which seek to lower them.[125] The Commission can take three actions: request the adoption of the act unanimously, withdraw the proposal, or bring an action for annulment once the act has been adopted. When specific amendments potentially violating fundamental rights are adopted, which can be said to change the substance of the legislative proposal beyond the Commission's original goal, the annulment action allows the Commission to tackle them.[126] This way, the rest of the legislative process remains intact.[127] In this manner, the Commission can defend the *concrete elements of the design* vital to a privacy-friendly system. If the Council or the EP wished to amend these elements, this could be viewed as a change of substance which is no longer compatible with the Commission's original goal. When either of these institutions amend these elements or perhaps add elements that are in clear deviance from the original proposal and detrimental to the protection of the right to privacy, the withdrawal by the Commission could be the preferred option.[128]

If the amendments are consistent with the Charter, there is no need for further action by the Commission. In the phase of the inter-institutional dialogue, the Common Approach to Impact Assessment enables for the Parliament and Council to assess the impact of their own 'significant' amendments. Fundamental rights are not mentioned in this document.[129] In this phase, the Commission has no formal leverage over the Council and Parliament, still it can exercise considerable soft power by emphasising the merits of the proposal.

There are reasons, however, to be sceptical about the Commission's and the Council's understanding as to what it means to be in compliance with the Charter and the Convention. The Commission, in its own communications on implementation of the Charter, refers to the European Council's call 'on the EU institutions and Member States to ensure that legal

[124] COM (2010) 573 (n 74) 7; COM (2009) 205 (n 82) 7-8. Underlining is copied from the original document.
[125] COM (2010) 573 (n 74) 8.
[126] Eva Poptcheva, 'The European Commission's right to withdraw a legislative proposal' <https://epthinktank.eu/2015/04/23/the-european-commissions-right-to-withdraw-a-legislative-proposal/> accessed 4 June 2018.
[127] COM (2009) 205 (n 82) 9.
[128] ibid.
[129] COM (2010) 573 (n 74) 9.

initiatives remain consistent with fundamental rights'.[130] In the Stockholm Programme – which was the major policy document on the area of Freedom, Security and Justice – there was much attention for promoting citizen's rights. Under the heading of 'Protecting citizen's rights in the information society', data protection and privacy had to be served by the EU by promoting data protection, and by foreseeing and regulating 'the circumstances in which interference by public authorities with the exercise of these rights is justified', as well as by applying 'data protection principles in the private sphere'.[131] The private sphere is pre-eminently a place where a citizen should be free from interference by the government: applying data protection principles in this sphere prior to questioning the government's presence therein is contrary to the logic of a society which takes freedom from interference as the point of departure. The fact that the proposal of the Future Group – this predicted that virtually any act of individuals in future society would amount to the creation of a detailed digital record that would create 'huge opportunities' for public security organisations – served the Council of the EU in preparing the Stockholm Programme does little to debunk the suspicion that these institutions pursue an agenda in which the right to privacy is breached by default.[132]

3.3 Consulting the Article 29 Working Party

According to Article 30(3) and (4) of Directive 95/46/EC, the Working Party can take the initiative to make recommendations and opinions which will be forwarded to the Commission. The Commission has the duty to inform the Working Party about the action it has taken in response to this in the form of a report, which is also sent to the Parliament and the Council. This report must be made public.[133] This provision thus holds important democratic controls that can significantly enhance the legitimacy of the Commission's policy that is legally obliged to give a public response to WP 29 concerns. Although the WP 29 does make recommendations and opinions, the duty to respond in the form of reports seems to be a dead letter in the law.[134] These reports could have been useful to see how the Commission responds to the recommendations and opinions on IoT systems. Nevertheless, conclusions

[130] ibid 8.

[131] Council of the European Union, 'The Stockholm Programme – An open and secure Europe serving and protecting the citizens' (2009) Brussels <https://ec.europa.eu/anti-trafficking/eu-policy/stockholm-programme-open-and-secure-europe-serving-and-protecting-citizens-0_en > accessed 7 June 2018, 18.

[132] Future Group, 'Public Security and Technology in Europe: Moving Forward' (Concept paper on the European strategy to transform Public security organisations in a Connected World, Portugal 2007) <http://bit.ly/PqvWIJ> accessed 17 August 2012 , 8.

[133] Article 30(5) Directive 95/46/EC.

[134] After repeated writing to the secretariat on two mail-accounts there has been no reply from either of them. Two former employees of the Article 29 Working Party both did not know about these reports being published. One of them thought that the feedback is usually given orally during the WP meetings. It is understandable that the reports might not be drawn up due to the administrative burden that they cause, yet it would be valuable if the minutes of the meeting on this part would be made public. This information could prove valuable for understanding the relationship between the Commission and the data protection watchdogs.

about this can be drawn from the subsequent actions of the Commission, which will be discussed in Chapter 5 and 6.

Recurring themes in the documents issued by the WP 29 include the importance of PbD, proportionality, data minimisation, purpose limitation, additional sectoral and specific regulations for specific technological contexts as well as the embedding of privacy and data protection principles in these contexts.[135] The WP 29 takes a constructive attitude when it comes to PbD, proposing that it should 'be binding for technology designers[136] and producers as well as for data controllers who have to decide on the acquisition and use of ICT' and explicitly linking this new principle to the data protection principles. It expressly mentions that PbD should go beyond data security and include the requirement for ICT systems to be designed in a way that avoids or minimises the personal data that is processed.[137] Thereby it leaves no doubt about how the data quality principles are to be interpreted and complied with in practice. According to the Article 29 WP it should have the same effect as a strict proportionality test. It is consistent in all its communications with regard to this point.[138]

In its 2014 opinion on the Recent Developments on the Internet of Things, the WP 29 provides a useful oversight of privacy and data protection challenges in the IoT, inter alia the lack of control and information asymmetry, the quality of user's consent, the repurposing of original processing and profiling.[139] It also addresses the applicability of EU law and deals inter alia with such thorny issues as the notion of personal data, and the legal qualification of device manufacturers as data controllers. It elaborates, furthermore, the data quality principles, sensitive data, transparency requirements and security, as well as the rights of the data subject. Finally, it ends with a set of recommendations to all stakeholders involved.[140] It does not address here, however, the specific issue of IoT systems that are mandated through EU law and the peripheral problems relating to the design of these systems. It refers to this matter superficially in a joint response of WP 29 and the Working Party on Police and Justice to the Commission's consultation on the legal framework for the right to protection of personal data. In this response, additional sectoral and specific regulations are expressly considered in the context of the employment of intelligent transport systems.[141] The controversial nature of legislation that forces IoT systems into people's lives and the risks that these systems harbour indicate a need to assess if additional regulatory instruments can provide the means to eliminate or mitigate these risks.

[135] Article 29 Data Protection Working Party, 'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (Adopted on 01 December 2009 02356/09/EN WP 168, The Article 29 Working Party 2009) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf> accessed 4 June 2018, 12.

[136] This can be read as an implicit reference to ESOs.

[137] WP 168 (n 135) 13.

[138] ibid.

[139] WP 223 (n 16).

[140] ibid.

[141] WP 168 (n 135) 8.

The fact that the opinions are non-binding makes it unlikely for the Commission to adopt them when the latter is subject to pressure from other, more powerful, policy actors. The aim of data protection authorities to balance the power a-symmetry between data controllers and data subjects is, thus, hard to realise on the institutional level of the EU, because the WP 29 lacks the required institutional power to make a tangible impact. In the context of mandatory IoT systems, this lack of power is particularly manifested in the extent to which the Commission follows up on their opinions.

3.4 Additional regulatory instruments

'Additional regulatory instruments' is one of the four actions considered by the Commission in the action plan on the IoT in order to monitor the application of data protection legislation.[142] It held that the technological developments require detailed guidance with regard to questions concerning the applicability of data protection legislation and enumerated amongst others the objective of minimising the processing of personal data together with key principles of data protection (proportionality, purpose limitation and transparency) as a starting point for guidance.[143] According to the Commission, 'specific legislation should not be excluded where self-regulation or interpretation prove insufficient', clearly indicating the will to propose binding alternatives if the more general legislation does not lead to compliance.[144]

The Commission can propose legislation that ensures the protection of the rights enshrined in the Charter. Article 16 TFEU confers the power to the Council and EP to lay down rules relating to the protection of individuals with regard to the processing of personal data. Additional regulatory instruments become necessary when the original regulatory framework does not provide for effective protection of the right to the protection of personal data, and arguably the right to privacy.[145] Where the right to the protection of personal data coincides with the right to privacy, its interpretation should follow the case law of the ECtHR regarding positive obligations. If legislation does not effectively address the behaviour of parties that interfere with this right and therefore does not offer a remedy for those affected by these interferences, there is a need for additional regulation to repair this gap.

In the 2009 IoT action plan the Commission introduced a potential additional regulatory instrument: *a right to silence* with regard to IoT systems. The *right to silence of the chips* expresses the idea 'that individuals should be able to disconnect from their networked

[142] COM (2009) 278 (n 2) 6.
[143] COM (2008) 594 (n 31) 8.
[144] ibid
[145] Hielke Hijmans, *The European Union as Guardian of Internet Privacy* (Springer 2016) 128.

environment at any time'.[146] In the context of IoT, this would be a right to be disconnected and unmonitored. As of now, the Commission has not launched such a debate.

Line of action 3 — The 'silence of the chips'

The Commission will launch a debate on the technical and legal aspects of the 'right to silence of the chips', which has been referred to under different names by different authors and expresses the idea that individuals should be able to disconnect from their networked environment at any time.'

The right to silence does hold a promise for the individual to be able to decide not to be connected and not to have any data about herself or himself collected and processed. The right to silence could function as the legal remedy for those who seek solitude. The right to silence appeals to the imagination as it allows one to envision actual protection against an interference with one's private life in a networked world, much like the original formulation of *the right to be let alone*.[147] It can, however, also be argued that this would make such a state exceptional and thus suspicious. Citizens could choose to be disconnected from the omnipresent networked sensors, but their wish to be invisible would not go unobserved.

4. The Commission as the 'executive'

The final phase in which the Commission is involved in the interpretation of the right to privacy and data protection concerns non-legislative acts, namely delegated and implementing acts under Article 290 and 291 TFEU. The legislative acts on smart meters and eCall confers implementing and delegating powers to the Commission in order to establish uniform conditions benefitting the massive roll-out of IoT systems.[148] The relationship between the Commission and ESOs is, in part, governed by this legislative act.

This distinction of acts introduced in the Lisbon Treaty is relatively new, but its rationale – to shift the burden of determining non-basic elements from the legislator to the executive – is not. The duty for the legislature to determine the *essential elements* of the legislative act has been described as 'a long-established canon of EU constitutional law'.[149] This canon took on a different shape in the 'the New Approach', which was introduced in a Council Resolution

[146] COM (2009) 278 (n 2) 6. European Parliament resolution of 15 June 2010 on the Internet of Things, point 16. This concept derives from Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (1st edition, Pearson Education 2006).

[147] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy', (1890) 4 Harv L Rev 193.

[148] Examples of this are found in Article 6 and 9 of the eCall Regulation and in Article 22 and 23 of Directive 2012/27/EU.

[149] Kieran St C Bradley, 'Legislating in the European Union' in Catherine Barnard and Steve Peers (eds), *European Union Law* (Oxford 2014) 125.

in 1985 to deal with the problem of 'technical barriers to trade'.[150] Before 1985, the Council attempted to remove technical barriers to trade by harmonising the technical requirements in the legislative process. Due to the relevance of technical requirements for products, production processes and services to access national markets, these attempts of legislative harmonisation led to fierce intergovernmental negotiations, exhausting the resources of the EC legislator.[151] The New Approach was about limiting legislative harmonisation to essential requirements in the public interest, particularly safety and health, leaving the definition of technical specifications to standardisation bodies. The ratio of standardisation is similar to the divide between legislative and non-legislative acts and requires the essential elements to be laid down by the legislature. According to the Council, reference to the standards would only take place if a clear distinction could be made between 'essential requirements' and 'manufacturing specifications'.[152]
The essential elements, historically 'essential safety requirements (or other requirements in the general interest)', serve the protection of public interests.

Like safety and health, data protection is a public interest. At the time of adopting the New Approach, the EC did not even start to develop data protection legislation. Data protection was not considered a relevant public interest at that time. Today, data protection would probably rank among the public interests which fall under the essential elements of a legislative act. Support for this assumption can be found in the fact that Article 16 TFEU provides that the Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data. This provision ranks under Title II of the TFEU 'Provisions Having General Application', along with environmental and consumer protection.

The New Approach was based on the contested premise that there is a clear distinction between political and technical aspects of a legislative act; the possibility to divide the political aspect ('What do we want?') and technical aspect ('How do we do it') of an act.[153] Weiler has described this distinction as a 'constitutional fiction of clear ontological boundaries'.[154] This distinction is especially difficult to maintain with respect to legislation introducing IoT systems, because here the technical and political coincide. Answering the 'how do we do it' question carries a high risk of being influenced by a 'what do we want' bias. In the context of legislation introducing IoT systems, the non-essential elements are generally viewed as technical specifications of these systems. These specifications, however,

[150] Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standards (85/C 136/01) [1985] OJ C 136/1.
[151] Maintaining certain technical requirements can effectively constitute a barrier to national markets.
[152] Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standards (85/C 136/01) [1985] OJ C 136/8.
[153] Frankel and Højberg formulate this distinction with the aid of two questions: 'What do we want?' and 'How do we do it?'. See: Christian Frankel and Erik Højberg, 'The constitution of a transnational policy field: negotiating the EU internal market for products' (2007) 14(1) Journal of European Public Policy 96, 108-109.
[154] Joseph HH Weiler, 'Epilogue: "Comitology" as Revolution – Infranationalism, Constitutionalism and Democracy' in Christian Joerges and Ellen Vos (eds), *EU Committees: Social Regulation, Law and Politics* (Hart 1999) 344.

can make the difference between equipping all EU citizens with intrusive surveillance systems or systems that are not even able to record detailed personal data in the first place. The implementing and delegated acts are therefore an interesting testing ground to examine the Commission's rhetoric, as well as ability to uphold the fundamental rights stipulated in the Charter, particularly in its interpretation and application of these rights in relation to ESOs.

4.1 The Commission's margin of discretion

The freedom of the Commission in exercising implementing powers, and thus in taking decisions on the design of IoT systems affecting fundamental rights, is a subject of intensive academic debate. The distinction between delegated and implementing acts was not codified in EU law until the adoption of the Lisbon Treaty as noted above. According to Article 290 TFEU, the Commission can adopt delegated acts 'to supplement or amend certain non-essential elements of the legislative act'. Implementing acts, on the other hand, refer to acts which merely implement legally binding acts.[155] Of particular relevance here is Art 291(2) TFEU, granting the Commission power to adopt implementing acts '[w]here uniform conditions for implementing legally binding Union acts are needed'. The Commission's role here would be confined to the implementation of the legally binding act. Logical examination, the history of implementing acts in the EU, as well as academic commentary, point towards the impossibility of implementing legislation without actually adding something to the legislative act. This is what Paul Craig dubs 'the language problem'.[156] In the default procedure where the Commission adopts the implementing act, this adding can be found in the implementing act adopted by the Commission. In the specific context of the Commission implementing EU law through collaboration with standard bodies, *the addition* extends to harmonised standards developed by the ESOs. The Commission's request for such a harmonised standard to ESOs is governed by Article 10(1), (2) and (6) of Regulation 2012/1025.[157] Article 10(1) establishes *limits* as well as *instructions* relevant to the Commission's margin of discretion:

> 'The Commission may within the limitations of the competences laid down in the Treaties, request one or several European standardisation organisations to draft a European standard or European standardisation deliverable within a set deadline. European standards and European standardisation deliverables shall be market-driven, take into account the public interest as well as the policy objectives clearly stated in the Commission's request and based on

[155] Art 291 TFEU.

[156] Paul Craig, 'Delegated Acts, Implementing Acts and the New Comitology Regulation' (2011) 36 ELR 673.

[157] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council [2012] OJ L 316/12 (hereinafter 'Standardisation Regulation').

consensus. The Commission shall determine the requirements as to the content to be met by the requested document and a deadline for its adoption.'

These limits consist of *constitutional limits*, following from the demand that the Commission must act within the boundaries of the competences laid down in the Treaties. The instruction consists of two parts. First, the Commission must state the policy objectives clearly in the request. The second part is more implicit and follows from the requirement for ESOs to take into account the public interest in tandem with the Commission's duty to establish the requirements regarding the content to be met by the requested document.

Article 10(6) establishes that the requirements which the standards aim to cover 'are set out in the corresponding Union harmonisation legislation', i.e. the legislative act. This means that the primary responsibility to formulate these requirements lies with the EU legislature. It is the task of the Commission to translate these requirements from the legislative act into clear demands for the ESOs in the relevant request. Finally, the Commission has to monitor the development of the standard and assess whether the requirements in the corresponding legislation/main legislative act are satisfied, before it publishes a reference to the harmonised standard.[158] Since the Commission usually proposes this legislation, an impact assessment would be the appropriate instrument to establish the public interests concerned, also where these coincide with (possible) interferences with fundamental rights. An impact assessment can be used to map out (possible) interferences with the right to privacy and then address these in the legislative act in the form of clear requirements, which could overlap or be equivalent to the *concrete elements of the design*, discussed above.[159]

Constitutional limits

The instruction of the legislature has to respect the constitutional limits. The Commission has to formulate the requirements and policy objectives in the request issued to the ESOs. In this endeavour the Commission is bound by the instruction of the legislature as well as the constitutional limits. These constitutional limits follow from the TFEU and the Charter, and how these are developed in the relevant case law of the CJEU.

In the pre-Lisbon context, there were three constitutional limits developed by the CJEU: the *specificity principle*, which required the enabling provision to 'clearly specify the bounds of the power conferred on the Commission';[160] the *non-delegation doctrine*, which entailed that the essential elements of the act and area, sometimes referred to in the past as 'the fundamental guidelines of Community policy', are reserved for the EU legislature;[161] and the *prohibition for the Commission to act outside its competence*, which means the Commission is not allowed to use its wide implementing power in one policy area to interfere with the

[158] Article 10(5) and (6) of the Standardisation Regulation. This will be further discussed in the next section.
[159] See section 3.2 on the role of the Commission within the legislative process.
[160] Robert Schütze, '"Delegated" Legislation in the (new) European Union: A Constitutional Analysis' (2011) 74 The ModLRev 661. This is an assignment to the legislature.
[161] Case C-240/90 *Germany v Commission* [1992] ECR 1-5383, para 37.

powers of the Council and the EP in another.[162] The limits of the Commission's power must be judged 'with regard to the basic general objectives of the organization of the market and less in terms of the literal meaning of the enabling word'.[163] It is a longstanding practice that the CJEU assesses the boundaries of the implementing power in relation to the aim of the legislation.

The introduction of a specific provision on implementing acts in the Treaty of Lisbon triggered a scholarly debate concerning the question of constitutional limits applicable to the Commission whilst implementing EU legislation. Article 290 TFEU codifies the Pre-Lisbon constitutional limits, with the exception of the prohibition for the Commission to act outside its competence which is implicit. First, it prescribes the non-delegation doctrine in two parts. The Commission may adopt 'non-legislative acts of general application to supplement or amend certain *non-essential elements of the legislative act'* and that 'the *essential elements of the area* shall be reserved for the legislative act'.[164] Second, it requires that the '*objectives, content, scope and duration* of the delegated power shall be explicitly defined in the legislative acts', i.e. the specificity principle.[165] Third, it establishes that there is a hierarchical relation between the delegated and the legislative act; the former 'will be able to amend primary legislation and must therefore enjoy at least relative and limited hierarchical parity'.[166] In the text of Article 291 TFEU on the implementing acts these limits are absent.[167] This raises the question whether the drafters of the Treaties have intended to exclude these limits from the implementing acts. One side of the debate claims that a systematic reading of Article 291 TFEU suggests:

> '…that while the Member States are principally responsible under paragraph 1, the Union will be competent under paragraph 2. The Union competence would thereby derive from Article 291(2) *as such*, while the specific Union act only regulates the *delegation* of implementing powers to the Commission (Council).[168] This systematic interpretation is reinforced by teleological considerations. A competence reading of Article 291 TFEU would allow the Union to adopt any type of implementing act – including implementing decisions – without

[162] Case C-22/88 *Vreugdenhil and Others v Minister van Landbouw en Visserij* ECLI:EU:C:1989:277, para 16-25; Schütze (n 160) 671.
[163] Case 23/75 *Rey Soda v Cassa Conguaglio Zucchero* (1975) ECR I-1279, 14.
[164] Article 290 TFEU. Italics added by the author.
[165] ibid.
[166] Schütze (n 160) 683.
[167] Article 291(1) TFEU: Member States shall adopt all measures of national law necessary to implement legally binding Union acts. (2) Where uniform conditions for implementing legally binding Union acts are needed, those acts shall confer implementing powers on the Commission.
[168] (Original footnote numbered 59): Some have even claimed that the Commission enjoys an autonomous power under Art. 291(2) TFEU, cf. Jean-Paul Jacqué, 'Le Traité de Lisbonne: Une vue cavalière' (2008) 44 Revue trimestrielle de droit européen 439, 480: "le pouvoir d'exécution appartient à la Commission qui ne dispose plus, comme dans la situation actuelle, d'un pouvoir délégué, mais d'un pouvoir proper".

> recourse to Article 352 TFEU. This reading would thus provide the Union with solid legal foundation for its executive action.'[169]

On the other side, it is claimed that these limits are equally important for the implementing acts, despite the fact that Article 291 TFEU does not mention them.[170] In the European Convention the drafters define the legislative act, in accordance with EC law and case law up to that point:

> 'legislative acts are adopted directly on the basis of the Treaty and contain the essential elements and the fundamental policy choices in a certain field. The scope of such a concept is to be determined on a case-by-case basis by the legislature.'[171]

Following the intention of the drafters, the part of the non-delegation doctrine which concerns the reservation of the essential elements for the legislative act should also apply to implementing acts, whilst the other part of this doctrine which prohibits the delegation of power involving essential elements does not apply to implementing acts. This does not mean essential elements and fundamental policy choices can be established outside the legislative act. The Court confirmed on multiple occasions, also after the Lisbon Treaty came into force, that 'implementing measures cannot amend essential elements of basic legislation or supplement it by new essential elements'. [172] The Commission itself argued that the legislature should not have the freedom to confer an act which leaves it little to no discretion under Article 290 TFEU, instead this absence of discretion should be reserved for Article 291

[169] Robert Schütze, 'From Rome to Lisbon: "Executive Federalism" in the (New) European Union' (2010) 47 CMLRev 1385, 1398. It should be noted though that Schütze refers to 'the Union', which can cover both the Commission and the Council. For further elaborations see Robert Schütze, *European Constitutional Law* (2nd edition, Cambridge University Press 2016) 321-324. Bergström, and in his footsteps Chamon, came to a similar conclusion that the implementing act will not have to be limited to the essential elements and the former even held that the implementing acts 'have the same substantive quality as legislative acts'. However, they did confine this conclusion to the implementing acts the Council conferred to itself under Article 24 and 26 TEU. This can be read as an implicit rejection of the idea that unconfined power is conferred on the Commission. See Carl F Bergström, *Comitology: Delegation of Powers in the European Union and the Committee System* (Oxford Studies in European Law, Oxford University Press 2006) 353-354; Merijn Chamon, 'Institutional balance and Community method in the implementation of EU legislation following the Lisbon Treaty' (2016) 53 CMLRev 1501, 1516.

[170] Dominique Ritleng, 'The Reserved Domain of the Legislature' in Carl Fredrik Bergström and Dominique Ritleng (eds), *Rulemaking by the European Commission: The New System for Delegation of Powers* (1st edition, Oxford Scholarship Online 2016) 143-144; Steve Peers and Marios Costa, 'Accountability for Delegated and Implementing Acts after the Treaty of Lisbon' (2012) 18 ELJ 427, 445-446 ; Craig (n 156) 673; Paul Craig, 'Comitology, Rulemaking, and the Lisbon Settlement' in Carl Fredrik Bergström and Dominique Ritleng (eds), *Rulemaking by the European Commission: The New System for Delegation of Powers* (1st edition, Oxford Scholarship Online 2016) 179. Craig argues that the implementing act can be used when it does not supplement the legislative act "by adding any 'new' non-essential element", which implies that only 'non-new' non-essential elements are reserved for the implementing act. Herwig Hoffman, 'Legislation, Delegation and Implementation under the Treaty of Lisbon: Typology Meets Reality' (2009) 15 ELJ 482, 488.

[171] Working Group IX on Simplification, 'Final report of Working Group IX on Simplification' (CONV 424/02 WG IX 13 The European Convention Brussels, 29 November 2002) 10.

[172] C-355/10 *Parliament v Council* ECLI:EU:C:2012:516, para 66.

TFEU.[173] This conferral of power under Article 291 TFEU does not, however, exclude essential elements *a priori*. The marginal discretion it leaves to the Commission allows freedom to the legislature to confer essential elements of the act. This power of the legislature is subject to the specificity principle, in line with the doctrine of the inter-institutional balance, in order to clearly delimit the executive powers of the Commission. This can be viewed as the continuation of the separation of powers.[174] In fact, the lack of or at least very limited margin of discretion for the Commission can be viewed as a precondition to confer potentially intrusive power to the Commission. The CJEU allowed the Commission to interfere with fundamental rights through implementing measures, which consisted in a transfer of personal data, on the condition that

> 'it is apparent that the very principle of the transmission of personal data to certain third States and the framework within which the transmission must take place were laid down by the legislature itself.'[175]

Whether the Commission is competent to adopt implementing acts which interfere with fundamental rights depends, thus, on whether this power is explicitly conferred upon it in the legislative act. If this was not a requirement, the power of the Commission would exceed that of the EU legislature. In combination with its competence to take the legislative initiative, this would give the Commission almost unfettered power to adopt policy severely violating human rights.[176] The delegated act confers a wider margin of discretion to the Commission, but this power can only be exercised as long as the Commission does not supplement or amend essential elements of the legislative act.

What the earlier quote of the drafters of the European Convention[177] also seems to suggest is that it is entirely up to the EU legislator to decide what constitutes an 'essential element'.[178] In the *Schengen Borders Code*, however, this margin of discretion was restricted

[173] Case C-427/12 *Commission v Parliament and Council* ECLI:EU:C:2014:170, para 47.
Anne Pieter van der Mei, 'Delegation of Rulemaking Powers to the European Commission post-Lisbon' (2016) 12 European Constitutional Law Review 538, 543. He refers in fn 16 of his case note that the Commission opposing the use of a delegated act is remarkable given their usual preference for this. An explanation could be that the Commission, by arguing that only minor discretionary power would rule out the possibility for the legislature to confer powers under Article 291 TFEU, tried to expand the scope of Article 290 TFEU and leave little to no discretion to the EU legislature to choose for implementing acts. The nett result would be an increase in the adoption of delegated acts at the cost of implementing acts. In a figure in Wim J M Voermans, Josephine Hartmann and Michael Kaeding , 'The quest for legitimacy in EU secondary legislation' (2014) 2 The Theory and Practice of Legislation 5, 16.
it shows that between 2010-2013, 93 % of the of the acts adopted by the Commission were implementing acts, only 7% is delegated.
[174] Chamon (n 169).
[175] Case C-363/14 *Parliament v Council* ECLI:EU:C:2015:579, para 54.
[176] *Malone* (n 71).
[177] 'Final report of Working Group IX on Simplification' (n 171)
[178] This was repeated by Voermans, who stated that the question on what constitutes an non-essential element 'is what the primary legislator considers to be a non-essential element'. In his view 'the Court of Justice is unlikely to render a substantive opinion on this subject', which it did little than a year later in *Parliament v Council* (n 172). See Wim JM Voermans, 'Delegation Is a Matter of Confidence' (2011) 17(2) EPL 313, 321.

significantly. According to the Court, the decision on whether 'elements of a matter must be categorised as essential' should be subject to 'objective factors amenable to judicial review', for which purpose 'the characteristics and particularities' of the specific area should be taken into account.[179] The Court considered a number of factors relevant. First, it held that the adoption of these specific rules entailed 'political choices falling within the responsibilities of the European Union legislature, in that it requires the conflicting interests at issue to be weighed up on the basis of a number of assessments'.[180] In short, the presence of conflicting interests which merit the intervention of the legislature, whose duty it is to mediate conflicting interests, is an important factor in assessing whether a measure involves essential elements. The second factor is the possibility that the 'fundamental rights of the persons concerned may be interfered with to such an extent' that it would require the intervention by the EU legislature.[181]

Regarding the political nature, it is clear from the outset that the IoT and the way systems function is a contested issue, exactly because there are opposing interests. These are represented in the conflicting outcomes of consultations, where citizens and consumer organisations opt for extra privacy measures and specific principles like PbD and consent, whilst companies prefer less regulation.[182] Whether conflicting interests merit an intervention by the legislature is intrinsically linked to the competence of the latter.[183] In this respect the significance of Article 16 TFEU, which establishes the competence for the EP and the Council to adopt data protection rules, in the context of legislation mandating the installation of IoT systems is highly relevant. The Commission cannot lawfully use its wide implementing powers in a technologically complex area to interfere with the powers of the Parliament and the Council to legislate on data protection.[184] This was implicitly acknowledged by the CJEU in *Europol*, when the Court allowed the conferral of a competence to the Commission to transmit data, on the condition that the principle governing the transmission was adopted by the legislature itself in the main legislative act.[185]

After the entry into force of the Lisbon Treaty, additional constitutional limits became relevant to the Commission's margin of discretion. Whilst implementing Union law, the Commission (as any other EU institution) is bound by the Charter (Article 51(1) of the Charter). The first requirement to lawfully interfere with fundamental rights is that it should be provided for by law (Article 52(1) of the Charter). This raises the question when acts of institutions qualify as law. It is common among Member States that measures which interfere

[179] *Parliament v Council* (n 172) paras 67- 68.
[180] ibid para 76.
[181] Ibid, para 77. Maarten den Heijer and Eljalill Tauschinsky, 'Where Human Rights Meet Administrative Law: Essential Elements and Limits to Delegation' (2013) 9 European Constitutional Law Review 513, 519.Also Merijn Chamon, 'How the concept of essential elements of a legislative act continues to elude the Court: Parliament v. Council' (2013) 50 CMLRev 849, 859.
[182] European Commission, 'Report on the Public Consultation on IoT Governance' (16 January 2013).
[183] Chamon has held that the political choice criterion is problematic, because what is an essential element is the result of a political choice. Chamon (n 181) 858. Chamon (n 169) 1501,1515.
[184] Schütze (n 160) 671.
[185] *Parliament v Council* (n 175) para 54.

with civil rights need to be provided in legislation in the formal sense, but according to some this is not the threshold which is maintained by the CJEU.[186] At least in one case the CJEU has held that implementing acts adopted by the Commission qualify as law, however it is not clear if this is the odd one out.[187] The ECtHR also understands the law in a 'substantive' as opposed to 'formal' sense, and the Charter provides that where the rights of the Charter and ECHR correspond they should have the same meaning and scope.[188] Foregoing has led some to argue that acts adopted by the Commission qualify as law and that the reservation of interferences with fundamental rights for the EU legislature does not stem from the Charter 'but only from the understanding of the "essential elements of an area" developed by the Court of Justice'.[189]

This argument, however, does not take into account the distinction introduced in the TFEU between the nature of the powers given to the Commission in delegated acts and implementing acts, which is respectively legislative and executive.[190] In its role of the executive, it could only implement an act which would interfere with the fundamental right to privacy to the extent that intervention of the legislature is required, if this interference is provided for by law (Article 52(1) of the Charter). The exercise of this power can only interfere with fundamental rights if this interference is set out in detail in the legislative act which governs the implementing act.[191] In line with the demand of foreseeability that follows from ECtHR and CJEU case law the legislative act needs to establish the modus operandi in which power conferred on a principal can be exercised.[192] It should be repeated here that the level of precision that has to be met depends on the subject matter, 'the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed'.[193] The surveillance and control potential of IoT systems and the fundamental implications for society inform the legislator to provide a foreseeable legal basis which arranges in sufficient detail the conferral of power.[194] This will bring the legislative act also in line with the part of the non-delegation doctrine that reserves the essential elements for the legislature. The demand of foreseeability which follows from the rationale of human and fundamental rights protection, can be seen as the peer of the specificity principle in EU

[186] Jürgen Bast, 'Legal Instruments and Judicial Protection' in Armin von Bogdandy and Jürgen Bast (eds), *Principles of European Constitutional Law*, (Second Revised Edition, Hart 2011) 391.

[187] Case C-92/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, para 66.

[188] *Huvig v France* App no 11105/84 (ECHR, 24 April 1990) para 28. Article 52 (3) of the CFEU.

[189] Ritleng (n 170) 22-23.

[190] Schütze (n 160) 661.

[191] *Parliament v Council* (n 175). This is also in line with:
Commission, 'Implementation of Article 290 of the Treaty on the Functioning of the European Union' (Communication From the Commission to the European Parliament and the Council) COM (2009) 673 final, 3 and 4, where it states is does not exercise quasi-legislative power in the implementing act, but purely executive. See for arguments for allowing the implementing act as a legal basis in: Ritleng (n 170) 12,18.

[192] Case C-201/14 *Smaranda Bara* ECLI:EU:C:2015:638, para 40.

[193] For the subject matter, see *Malone* (n 71) para 68; *Vogt v Germany* App no 17851/91 (ECtHR, 26 September 1995).

[194] For an account of these implications see Bart Jacobs, 'Keeping our surveillance society non-totalitarian' [2009] 1(4) Amsterdam Law Forum <http://amsterdamlawforum.org/article/view/91> accessed 7 June 2018.

constitutional law. Both contain a duty for the legislature to clearly formulate the boundaries of the Commission's competence when it comes to taking measures interfering with fundamental rights. These boundaries should be reflected in the requirements as established in the basic act, which sets the stage for the request the Commission can issue to the ESOs.

These limits which apply to the relation between the EU legislature and the Commission, equally apply to the relation between the Commission and ESOs.[195] It is within these limits that the Commission should determine the requirements and policy objectives that are adopted in the requests towards the ESOs. In the specific context of IoT systems and the interference constituted by the mere obligation to have these systems installed in the private environment, the Commission has a duty to provide clear instructions to the ESOs that restrict their freedom to take decisions on the systems design which could further engrave this interference. This constitutional setup is, however, subject to the test of reality.

Oversight in practice

The Treaties establish numerous limitations of the competence of the Commission to interfere with fundamental rights whilst issuing a request to ESOs. In practice, however, the only means of ex post control for either EP or Council is to indicate this to the Commission when they find that the draft implementing act exceeds the implementing powers provided for in the basic act.[196] This is a soft power and, if the Commission refuses to amend or withdraw its proposal, the only option left is to apply for judicial review. Under the Standardisation Regulation, the EP as well as the Member States are provided with the possibility to inform the Commission that they do not hold the harmonised standard to 'entirely satisfy the requirements which it aims to cover and which are set out in the relevant Union harmonisation legislation'. [197] The EP or Member States have to provide a detailed explanation and the Commission has to consult a committee that consists of representatives of Member States,[198] before it decides either:

a) 'to publish, not to publish or to publish with restriction the references to the harmonised standard concerned in the *Official Journal of the European Union*;
b) to maintain, not to maintain or to maintain with restriction the references to the harmonised standard concerned in the *Official Journal of the European Union.*'

The decision under Article 11(1)(a) is adopted under the advisory procedure,[199] which means that the Commission can deviate from the advice given by the committee. The decision under

[195] Case 9/56 *Meroni & Co, Industrie Metallurgiche SpA v High Authority of the European Coal and Steel Community* (1958) ECR 133.
[196] Article 11 of Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers [2011] OJ L 55/13 (hereinafter 'Regulation (EU) No 182/2011').
[197] Article 11(1) of the Standardisation Regulation.
[198] Article 11(1) of the Standardisation Regulation; and Article 3(2) of Regulation (EU) No 182/2011.
[199] Article 4 of Regulation (EU) No 182/2011.

Article 11(1)(b) is adopted under the examination procedure, which means the Commission is bound by a negative advice. These technical committees are likely to operate with their own biases and moral premises, which will likely be uncritical towards the questions pertaining to essential elements.[200] Given the technical character of developing specifications for IoT systems, neither the Parliament, nor the Council, nor the Member States are likely to meddle in this matter. It is to be expected they confer to the Commission wide implementing powers to keep pace with technological developments.[201]

4.2 The request of the Commission to the ESOs

The Commission issues a request to ESOs to develop a 'harmonised standard'.[202] These ESOs are private bodies which, upon accepting the request, have to develop the standard governing the design of IoT systems. The Commission, together with the ESOs, assesses the compliance of the draft standard with the original request and when it satisfies the requirements that follow from it as well as the corresponding EU harmonisation legislation, then the Commission publishes a reference to the standards in the *Official Journal of the EU*.[203] This practice where the Commission requests the ESOs to draw up a harmonised standard formally qualifies as an implementing act under Article 291(2) TFEU and is further governed by the Standardisation Regulation and Regulation 2011/182/EU. As discussed above, the issue of addition comes into play at this stage. This issue is further complicated by the Commission relying on ESOs in this process, with which they engage in a contractual relationship governed by the Standardisation Regulation. The interpretation of the right to privacy and the protection of personal data takes place in three different phases:

1. Whilst drafting the request from the Commission to the ESOs.
2. Whilst drafting the standard, the Commission's together with the ESO assesses compliance with the initial request.
3. The Commission's assessment of the draft standard for compliance with the request and the essential elements of the harmonisation legislation.

The negotiation process that eventually leads to the standard is not neutral itself and allows the ESOs a considerable margin for manoeuvre. The eventual standard is a resultant of the negotiation dynamics between the Commission and the ESOs, in which the ESOs wield considerable power. First of all, a mandate issued by the Commission is subject to negotiations between the ESOs and the Commission. The ESOs, thus, share a say in the objectives of the standards' *content* in addition to having the final say about the procedures

[200] Paul Craig and Gráinne de Búrca, *EU Law: text, cases and materials*, (5th edition, Oxford University Press 2011) 137. For further reading see Weiler (n 154) 344.
[201] On the bases of comparable considerations in the field of agriculture and foreign trade the CJEU gave the Commission wide implementing powers. Dominique Ritleng (n 171) 9.
[202] Article 2(1)(c) of the Standardisation Regulation.
[203] Article 10(5) and (6) of the Standardisation Regulation.

for their *creation*.[204] The ESOs draft harmonised standards after receiving a request from the Commission. [205] Although the Commission refers to them as 'mandates' in its communications, which has a certain ring of hierarchy to it, the Regulation on European standardisation refers to them as 'requests'. This is more accurate, since the ESOs can reject them at their discretion. [206] The legal status of a request is a contract. Although the Commission formally exercises the discretion to determine the requirements and policy objectives, they are in fact dependent on the ESOs in fulfilling their task.[207] There are only three ESOs which hold a monopoly with respect to these requests, so if they refuse a request, the Commission reaches a dead end. This dependent position is likely to affect the Commission whilst adopting system requirements with respect to the right to privacy and the protection of personal data in the request. The ESOs are, thus, in the unusually powerful position where they can potentially veto the interpretation of these rights by the Commission, for instance, if they think the legislative act allows the Commission to make them a better offer. This demonstrates that the more space is left in the legislative act, the worse the position of the Commission in the negotiation process and the more difficulties it will have in keeping the ESOs within the constitutional boundaries of implementing and delegated acts as set by the Treaties and the Charter.

If the legislature in contravention of the specificity principle fails to clearly delineate the essential elements of the design, the risk arises that the Commission in turn provides a mandate to the ESOs in which this openness of the design is perpetuated. Consequently, a margin of discretion on essential elements, involving decisions on the surveillance and control potential of the system, is handed to these private parties.[208] Elements of IoT system-design which can negatively impact fundamental rights and which contain opposing interests between industry and citizens, should be regarded as *essential features of design*. Decisions on the interpretation and application of core data protection principles involve essential elements, since these are the preserve of the Council and EP under Article 16 TFEU. The body of safeguards addressing the design of the system in order to avoid or, alternatively, mitigate interferences with fundamental rights is a task that coincides with the Commission's formulation of concrete elements of design following the impact assessment and conjoins in the term *essential elements of design*. The impact assessment of the Commission is the first place where the concrete elements of design should be established, before they are adopted in the legislative proposal. Here these elements are open to scrutiny by the EU legislature who has to decide on the essential elements of design. This should, ultimately, contribute to a design of IoT systems that respects the rights to privacy and the protection of personal data. The legislature has a duty to live up to the specificity principle. The Commission must ensure

[204] Christian Frankel and Erik Højberg (n 153) 108.

[205] Article 2(1)(c) of the Standardisation Regulation.

[206] Article 10(3) of the Standardisation Regulation. It is interesting that the Regulation does not mention what should happen with the refusal of the request, it is probably not documented, while analysing these refusals could tell a lot about the power of the ESOs.

[207] Christian Frankel and Erik Højberg (n 153) 109.

[208] This mandate is susceptible to judicial review if it produces legal effects. *Parliament v Council* (n 172) para 50.

that the ESOs do not adopt decisions on essential elements, potentially leading to the Commission acting in breach of the non-delegation doctrine and the sidelining of the legislature's preserve.

4.3 The Commission's attitude towards the ESOs

Whilst overseeing the development of the standard the Commission, together with the ESOs, assesses the compliance of the document with the initial request (Article 10(5) Regulation 2012). This task of monitoring is complicated due to the gap between the expertise available at the Commission compared to that of the ESOs. The expertise a-symmetry is even starker in the case of the Parliament and the Council whose task it is to formulate the requirements in the legislative act for the Commission to follow. The problems which follow from this are also known in literature on principal-agent relationships as *agency shirking* and *slippage. S*hirking means lack of effort from the agent, in this context the ESO, to genuinely meet the requirements set out in the request. Slippage occurs because it is hard for the principal (the Commission) to observe the actual behaviour of the agent.[209] This is also confirmed by Schepel who observes the Commission lacks expertise, resources and willingness to attend the meetings of the ESOs as observers.[210] The Commission's dependence on the ESOs and its knowledge a-symmetry hampers its ability to function as a guardian of fundamental rights.

Another complicating factor is that standardisation bodies do not qualify as data controllers, nor processors, therefore their activities do not fall under the scope of EU data protection legislation. With respect to EU data protection law, these ESOs operate in a legal vacuum allowing them to implement privacy-infringing features in the design which blatantly conflict with the GDPR, without facing the threat of the newly introduced mountainous fines. In its communication on PETs, the Commission seems to address the special position of ESOs when it states that:

> 'Whilst strictly speaking data controllers bear the legal responsibility for complying with data protection rulers, others also bear responsibility for data protection from a societal and ethical point of view. These involve those who design technical specifications and those who actually build or implement applications or operating systems.'[211]

In the same document it explicitly addresses their activities:

> 'The Commission will consider the need for respect of data protection rules to be taken into account in standardisation activities.'[212]

[209] Michelle Egan, 'Regulatory strategies, delegation and European market integration' (1998) 5 Journal of European Public Policy 485, 489.
[210] Harm Schepel, *The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets* (1st edition, Hart Publishing 2005) 243.
[211] COM (2007) 228 (n 27) 2-3. It does not mention the 'legal' point of view, thereby implicitly rejecting that the laws impose norms on the design of systems.
[212] ibid 7.

This quote reveals the Commission's attitude towards data protection as well as the ESOs. For PETs to be effective they need to be integrated into the architecture of IoT systems. In that manner they can prevent the unnecessary collection and processing of personal data, whilst maintaining the functionality of the system. The ESOs develop the rules for the design of a system. They are, therefore, in the most important position to align their actions with the effective protection of the right to privacy and the protection of personal data. As a guardian of EU law, one would expect the Commission to monitor the observance of data protection rules and to remedy any vacuum it notices, which could have been done in this communication and in its subsequent action.[213] Instead of addressing this vacuum, the Commission makes a statement which does not even ensure the application of the rules to standardisation activities, but merely notes to 'consider the need' for the rules 'to be taken into account'. This non-committal, ineffective approach is at odds with the rhetoric on the efficiency of the rights enshrined in the Charter.[214]

In contrast to the legal vacuum in which they operate, the parties represented by the ESOs do not decide on system-design in a vacuum; they have interests in deploying these systems in their own business models and administrative practices.[215] Designing these systems in line with the right to privacy and data protection legislation goes against ESOs their own interest. In sum, they have real-world interests, in a legal vacuum. The interests vested in the ESOs result in *non-compliance bias* towards data protection. Given their constituency it is unlikely that the ESOs will voluntarily develop standards which include PETs that avoid or minimise the processing of personal data as well as functions permitting remote control. Most, if not all, parties involved in the ESOs have an interest in weakening features that will advance the privacy related interests of citizens and limit the collection of personal data. Geoff Strawbridge, then Secretary for the British Standards Institution in London, accurately described the mindset of those involved in standardisation in the following sentence:

> *'If you know what you want, you should be taking the initiatives that will enable you to achieve it.'* [216]

Strawbridge elaborates on the process of standard setting by suggesting that the ´possibilities are almost limitless´ for the representative interests that are involved.[217] According to him, for the efficiency of these procedures 'specifiers, users and consumers' must see to their position being reflected in the adoption of the relevant standards, placing the burden of responsibility on the shoulders of the individual.[218]

[213] Eg by addressing ESOs in the proposal for the GDPR.
[214] COM (2010) 573 (n 74) 3.
[215] The interests vested in ESOs are industry and government, but they are renowned for being industry-dominated bodies.
[216] Geoff Strawbridge, 'The Single Market Effect: European Standardization in Theory and Practice' (1990) 8 European Management Journal 174.
[217] ibid 176.
[218] ibid 176.

The utmost difficulty here lies in the lack of awareness of the procedure or of the fact that citizens' interests are at stake which makes it practically impossible to defend societal interests. Strawbridge also underlines that the document that follows from the standardisation process must be exposed to wider comment until consensus is reached which requires 'absence of sustained opposition to substantial issues by any important part of the concerned interests'.[219] Even though the process is aimed at taking all views into account, it is clear from the outset that the parties with significant expertise, important interests, long breaths and deep pockets have the highest chance to press their views through.

Personal data has been described the 'new oil', and just like the process of drilling for oil, collecting personal data can be a dirty business.[220] Drawing from the lessons of activism against oil companies, the Commission should not expect interests groups to play a meaningful role in the process of standard setting. The fact that personal data has become an economic asset inevitably has consequences for the way companies organise their business processes. Obeying the laws of the market and their shareholders, they seek to maximise their profits and if personal data generates profit, this goal comes down to maximising the amount of personal data they can collect within this process.

One of the ways in which the Commission attempts to justify its soft attitude towards the ESOs' activities is maintaining the contested fiction that standards are voluntary. This implies they are not legally binding, unless this is provided for by the main legislative act. When producers of IoT systems comply with the standard, it provides the presumption of conformity, through which they can access the internal market. The CJEU decided that this does give harmonised standard legal effects.[221] The choice to comply with a standard is not fully voluntary, since it requires great investments for companies to deviate from it.[222] This means that standards only improve competition in a quantitative sense by creating access to the supply-side of the market through compliance with the standard.[223]

This soft approach of the Commission stands little chance in guaranteeing the respect for the citizens' right to privacy. The foregoing shows that clear requirements with respect to system design and fundamental rights in the legislative act are essential in order to prevent the ESOs from decision-making which might result in supplementing or amending the essential elements of IoT policy, reserved for the EU legislature. If the legislature and the Commission fail to fulfil their duty, they become accessory to the breaches of privacy that follow from the

[219] ibid 178.

[220] 'Data is giving rise to a new economy' (Economist, 6 May 2017) <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> accessed 7 June 2018.

[221] Case C-613/14 *James Elliott Construction* ECLI:EU:C:2016:821, para 39.

[222] Robin Hoenkamp, *Safeguarding EU policy aims and requirements in smart grid standardization* (2015, UvA-Dare) <http://hdl.handle.net/11245/2.158793 > accessed 7 June 2018.

[223] When it comes to quality though, the standards actually carry the risk to block innovation and thus competition. In the Netherlands this was experienced first-hand by network operator Liander, which tried to get a standard approved for the smart meter that would respect customer privacy, but did not get the necessary support for it in the national standardisation body, most likely because it hampered business-interests.

work of the ESOs. The contradictory interests inherent in the deployment of IoT systems should be recognised and decided on by the EU legislature, not a clubhouse for tech-companies.[224]

5. Conclusion

The Commission is the most important institution in the policy and rulemaking process concerning mandatory IoT systems. It sets the agenda, it publishes communications, engages in stakeholder dialogues, executes impact assessments, adopts legislative proposals, it is involved in the legislative process, and it plays a pivotal role as executive and negotiator with the ESOs. Throughout this process, it is the main interpreter of the right to privacy and data protection legislation. It has produced an impressive amount of communications, recommendations and other documents on the right to privacy and data protection. In this process it has created a body of promises; it declared its will to use the role as guardian of the Treaties and newly acquired role of guardian of the Charter, in conjunction with its role as initiator of policy, to ensure the efficiency of fundamental rights in the face of technological developments. In doing so, it seeks to reconcile the opposing interests which characterise this policy field.

The Commission, nonetheless, is caught between two worlds. It only has limited power to impose its will on powerful stakeholders, which means it has to take their interests into account. In order to initiate policies successfully the Commission must ensure that there is an incentive for private parties it seeks to involve. One of the attractive features of IoT systems for these parties is their property to collect and disseminate vast amounts of personal data. This is the proverbial carrot that drives the mule. A firm stance of the Commission that would impose a reserve on governments as well as industry parties with regard to the exploitation of this property, would leave the Commission without any rewards to hand out. The Commission seems to rely on the language of data protection in order to reconcile its rhetoric on safeguarding fundamental rights, whilst retaining the possibility to hand out these rewards. The assumption of the Commission seems to be that privacy is protected as long as the processing of personal data is in line with its loose interpretation and application of data protection legislation. The rhetoric of the Commission results in a variant of data protection in which the prohibitive potential is taken out and can be coined the *data protection-light* approach.

The concerns voiced by civil society actors regarding privacy are at the margins of this policy field and are generally weakly organised and too diffused for their opinions to have a meaningful impact.[225] The consultations show it is this opposing view and interest that keeps recurring and is alive among citizens. The control over the detailed personal data IoT systems collect is what serves the autonomy of citizens and is the interest that conflicts with those

[224] Rob van Gestel and Hans-W Micklitz, 'European Integration through standardization: how judicial review is breaking down the club house of private standardization bodies' (2013) 50 CMLRev 145.

[225] This problem also occurs in other areas, see Lawrence Lessig, *Code* (Version 2, Basic Books 2006) 200-201.

industry and government stakeholders in a less restricted processing of personal data. It is the latter interest that the Commission primarily attends to and which is negatively affected by a strict interpretation and application of the right to privacy and data protection. It is, therefore, not a surprise that this critical voice is hardly echoed in any of the communications of the Commission.

The approach the Commission advocates towards its own legislative work is thorough and ambitious. In its communications, it demonstrates an awareness of the critical factors relevant for establishing the impact on fundamental rights, as well as the background against which they should be assessed, namely the case law of the ECtHR and the CJEU. In the context of executing fundamental rights impact assessments for IoT systems, however, a number of critical points arise. The negative impact that these systems might have on fundamental rights are difficult to foresee easily, in part due to their technical complexity. Another problem consists of the interests of powerful stakeholders in the policy field, which are likely to influence the way the Commission will interpret the right to privacy within such assessments. It is to be expected that the approach towards impact assessments the Commission advocates in its communications, will deviate from the impact assessments it performs. To assess this it is necessary to turn a critical eye towards the way it actually performs these assessments.[226]

A properly executed impact assessment can result in the development of effective safeguards that could mitigate the negative impact on a fundamental rights. This body of safeguards are referred to as *concrete elements of design*, which should be adopted in the legislative proposal. These can then be adopted in the legislation as *essential elements of design* and translated into requirements guiding the Commission's request to the ESOs. The adoption of essential elements in the legislative act reinforces the Commission's position vis-a-vis the ESOs. Elements of IoT design which can negatively impact the right to privacy and/or which are politically sensitive are *essential features of design* and fall strictly under the competence of the EU legislature.

The division of legislative acts and non-legislative acts into respectively essential and non-essential elements proves particularly challenging in the face of complex IoT systems mandated by law with features that prove politically sensitive and/or capable of interfering with the right to privacy. A clear separation of the essential and non-essential elements is vitally important in order to prevent ESOs from taking political decisions. The projected imagery of ESOs as tame a-political organisations merely guiding decisions on technical details with voluntary effects is as misleading as the appearance of the Rabbit of Caerbannog.[227]

In pursuit of its policies the Commission contributes to conceptual confusion of the right to privacy and data protection and subsequently erodes the substantive protection offered by these rights. The Commission's tendency is to exclude the right to privacy from policy considerations. This, together with the narrow focus on data protection when data is

[226] This will be done in Chapter 5 and 6.
[227] Python (Monty) Pictures, 'Monthy Python and the Holy Grail' (1975).

processed, is likely to result in failing to question the necessity of the initial recording and collection of data. Thereby it risks reducing data protection to a matter of data security, as in the secure storage of data. Through all its powers relating to IoT policy the Commission actively contributes to an understanding of data protection legislation in which the substantive norms are gutted to the point where protection is only offered through realising transparency and security of processing operations. By creating the idea that this *data protection-light* is suited to deal with privacy issues, the Commission departs from its intended guardianship of fundamental rights. The Commission's systematic neglect of the right to privacy in the documents thus far analysed is incomprehensible in the face of its own ambitions with respect to the Charter of Fundamental Rights.

Chapter V
The regulatory framework of the smart meter: a case study

1. Introduction

The smart electricity meter, or simply *smart meter*, is a device that is said to be indispensable to achieve the EU's goals concerning energy end-use efficiency in two ways, namely by raising consumer awareness and by being a building block for the smart grid.[1] The definition provided in Directive 2012/27/EU[2] is that a smart meter (or smart metering system) not only measures energy consumption, but provides more detailed information than a conventional meter. Moreover, it can transmit and receive data using a form of electronic communication.[3] These features of the smart meter partially coincide with those of IoT-objects that can be 'read, recognised, addressed, located and/or controlled remotely through the internet'.[4] The only distinction is that the communication does not take place through the use of the internet-protocol, but usually by GPRS or power line communication (PLC).[5] In its current form, the smart meter displays the key IoT-features: it has an identity, it registers the consumption of electricity on a detailed level, it communicates this information and it can be remotely controlled. It is therefore unsurprising that it is considered one of the building blocks of the IoT in the home environment. Smart meters are considered to be stepping stones, in combination with other ICT-hardware, for a 'fully interconnected, smart environment'.[6] In the Commission's action plan smart meters are referred to in the paragraph on some existing IoT applications.[7] Smart meters could have a significant impact on the right to respect for private life and the home. Drawing on the work of Elias Quinn,[8] Ian Brown demonstrates how the information revealed by smart meters exposes some of the following data and raises the following questions (a selection):

---

[1] The meaning of the smart grid will be discussed in section 2.2.2.

[2] Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC [2012] OJ L 315/1 (hereinafter 'Directive 2012/27/EU').

[3] Recital 28 Directive 2012/27/EU.

[4] European Parliament resolution of 15 June 2010 on the Internet of Things 2009/2224 (INI), para E.

[5] Although the smart meter does not communicate over tcp/ip, they do have the capacity to communicate measurements over the internet.

[6] Directorate-General for the Information Society and Media (European Commission), Vision and challenges for realising the Internet of things (The Publications Office of the European Union 2010) 51.

[7] Commission, 'Internet of Things – An action plan for Europe' (Communication from the Commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions) COM (2009) 278 final 3.

[8] Ian Brown, 'Britain's smart meter programme: A case study in privacy by design' (2014) 28 International Review of Law, Computers & Technology 172.who refers to Elias Leake Quinn, 'Privacy and the New Energy Infrastructure' (2008) Cees working paper no. 09- 001 <http://dx.doi.org/10.2139/ssrn.1370731> accessed 5 June 2018.

1. ‘When are you usually away from home?
2. How often do you arrive home around the times the bars close?
3. What’s the relative frequency of microwave dinners to three-pot feasts?
4. Is your household protected with an electronic alarm system?
5. Are you a restless sleeper, getting up frequently throughout the night?
6. Do clinically depressed or bipolar individuals have distinctive energy profiles? What about people with behavioral disorders? Could you tell if someone hadn’t been taking his or her medication?’[9]

In the future, data concerning detailed electricity usage will even reveal more: e.g. the use of specific medical devices, baby monitors or whether individuals sleep in the same room.[10] The potential severity of the interference with the right to private life and the home constituted by the collection of smart meter data and its further processing has to be assessed against the background of a highly invasive network society in which these meters can serve a plethora of public and private interests. The significance of the interference lies in the fact it takes place in the home, a sphere historically protected from the scrutiny of the public gaze. The home is protected under most European constitutions, as well as under the ECHR and the CFEU. Historically, it was sufficient to safeguard the right to respect for the home by law, because it was structurally protected by the physical impracticability of penetrating this sphere without taking special measures like placing bugs.[11] The mandatory installation of a smart meter, which could be used to register behaviour behind closed doors, is a major step in dissolving this structural protection. The architectural choices on design adopted in EU legislation on the smart meter deserve careful consideration as it could result in subjecting one of the last strongholds of privacy to permanent surveillance, which could be subsequently tapped into by public authorities. An ill-considered design holds the potential to make this pillar of a free society collapse.

Directives 2012/27/EU on energy end-use efficiency and 2009/72/EC concerning common rules for the internal market in electricity (hereinafter ‘the energy directives’), establish obligations regarding the installation and functions smart meters are equipped with.[12] The rules regarding the installation and the functions of the meter determine the extent to which smart meters interfere with the right to private life and the home, and whether this interference meets the requirements as set forth in the ECHR and the Charter. Moreover, through an analysis of these rules and the standard for the smart meter, it can be established whether the doctrine of the institutional balance was respected. In its turn, this raises questions on the reservation of the essential elements by the legislature and on the specificity

[9] If these questions can be answered depends in part on the frequency of the measurements the smart meter takes.

[10] European Data Protection Supervisor, ‘Opinion of the European Data Protection Supervisor on the Commission Recommendation on preparations for the roll-out of smart metering Systems’, (EDPS 2012) 5.

[11] Harry Surden, Structural Rights in Privacy (2007) 60 SMU Law Review 1605.

[12] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC [2009] OJ L 211/55 (hereinafter ‘Directive 2009/72/EC’).

of the instruction of the EU legislature to the Commission and from the Commission to the ESOs.

The aim of this chapter is to assess the impact of smart meters on the right to privacy and the factoring of the right to privacy and data protection legislation in the Commission's work throughout the legislative process, including the preparatory work. First, the mandatory character of the smart meter will be assessed in the light of the objective of energy efficiency. Second, an inventory will be made of the functions which constitute an interference with the right to privacy, followed by the determination if these derive from the energy directives or from a non-legislative act.[13] Next, the impact assessment and explanatory memoranda of the energy directives will be assessed in order to determine if and how fundamental rights, as clarified in the case law of the CJEU and ECtHR, were taken into account in the process leading up to the legislative proposal.[14] The final part will assess whether the allocation of the smart meter functions complies with Article 291 TFEU (see Chapter 4, section 4), as well as the issue of instructing the ESOs and their approach towards privacy.

2. The mandatory character of the installation

Whether Directive 2012/27/EU makes the installation of the meter mandatory is relevant, because when it does not, it leaves citizens a choice of installing a conventional meter. The controversy surrounding mandatory installation of smart meters at national level was highlighted by the political entanglements of 2009 when former Dutch minister of Economics, Maria van der Hoeven,[15] defended a bill that made the installation of smart meters mandatory in front of the Dutch Senate. The bill provided sanctions for those who would refuse the installation of a smart meter. These consisted of six months detention, community service or a fine up to 17 000 euros. Before the bill was discussed by the Senate, the Dutch Consumers' Association published a report written by the University of Tilburg in which the meter was tested against Article 8 ECHR. One of the conclusions of the report was that the frequent generation and transmission of data constituted a significant breach of the right to private life, while the indications that this would contribute to the saving of energy were insufficient.[16] Furthermore, the report claimed that the aim to save energy could be realised with less infringing alternatives which had not been properly explored. Ultimately, it argued that the Directive did not demand a mandatory installation and pointed out that the

[13] The determination of which is important to assess whether functions that interfere with the right to private life and the home are provided for by law, which is a central requirement that follows from both the Charter and the ECHR.

[14] This is done to assess if the Commission lives up to its task of guardian of fundamental rights, which it proclaims in a number of communications treated in section 3.1 and 3.2 of Chapter 4.

[15] She became director of the International Energy Agency after ending her term.

[16] Colette Cuijpers and Bert-Jaap Koops, 'Het wetsvoorstel "slimme meters": een privacytoets op basis van art. 8 EVRM' (Onderzoek in opdracht van de Consumentenbond, Universiteit van Tilburg TILT – Centrum voor Recht, Technologie en Samenleving 2008) 29.

smart meter would use more energy than the conventional one.[17] The civil rights association Vrijbit also protested heavily against the bill, stating that the meter could be used as a spy-device and handed over a petition signed by approximately 12 000 people.[18] After the Senate refused to enact the bill, Van der Hoeven reintroduced a revised version in which installation became a voluntary act. Cuijpers and Koops (the authors of the report of the Dutch Consumers' Organisation) also underlined that the level of privacy-infringing functions has implications for the privacy-requirement of necessity: the smarter the meter the less likely it can be considered necessary in a democratic society.[19]

2.1 Installation according to EU law

In recital 27 of Directive 2012/27/EU, it is stated that 'where the roll-out of smart meters is assessed positively, at least 80% of consumers should be equipped with intelligent metering systems by 2020.'[20] This is a repetition of the goal set in Annex I of Directive 2009/72/EC.[21] The Commission provided in the Recommendation that:

> 'Member States are required to ensure the implementation of smart metering systems that assist the active participation of consumers in the electricity supply (…) implementation of those metering systems may be subject to an economic assessment of all the long-term costs and benefits to the market and the individual consumer or which form of smart metering is economically reasonable and cost-effective and which timeframe is feasible for their deployment.'[22]

Article 9 of Directive 2012/27/EU determines that final customers are 'provided' with a smart meter. The verb 'provide' leaves space to argue about the mandatory character of the installation, which was exactly what the authors of the Tilburg report did. The first paragraph of Article 9 deals with the conditions under which a smart meter is provided, which slightly deviates from the previous directive:

> '1. Member States shall ensure that, in so far as it is technically possible, financially reasonable and proportionate in relation to the potential energy savings, final customers for electricity, natural gas, district heating, district cooling and domestic hot water are provided with competitively priced individual meters that accurately reflect the final customer's actual energy consumption and that provide information on actual time of use.

[17] ibid 30, respectively 27.

[18] See 'Chronologic dossier 'slimme' energie meters' (Wij vertrouwen slimme meters niet) < http://www.wijvertrouwenslimmemetersniet.nl/> accessed 1 November 2011.

[19] Colette Cuijpers and Bert-Jaap Koops,'Smart Metering and Privacy in Europe: Lessons from the Dutch Case' in Serge Gutwirth and others (eds), *European Data Protection: Coming of Age* (Springer Science + Business Media 2013) 291.

[20] The minimum of 80% is only for electricity, not for gas.

[21] Annex 1, paragraph 2 fourth alinea of the Directive 2009/72/EC determines that 80% of *consumers* shall be equipped with intelligent metering systems by 2020, if the roll-out is assessed positively.

[22] Commission Recommendation 2012/148/EU on preparations for the roll-out of smart metering systems [2012] OJ L 73/9 (hereinafter 'Recommendation 2012/148/EU').

Such a competitively priced individual meter shall always be provided when:

a) an existing meter is replaced, unless this is technically impossible or not cost-effective in relation to the estimated potential savings in the long term; [23]
b) a new connection is made in a new building or a building undergoes major renovations, as set out in the Directive 2010/31/EU.'

An instant mandatory replacement of conventional meters by the smart meter does not unequivocally follow from this formulation, although some Member States have adopted such obligation in their national law implementing the energy directives.[24] After the lifespan of the last conventional meter has expired, however, the final household should be equipped with a smart meter. The exceptions provided in Article 9(1)(a) are based on objective grounds. This should be read as an implicit rejection of subjective grounds (a refusal on principal grounds) as well as a rejection of an opt-out, which would allow customers to retain the old meter. What is more, these objective exceptions do not apply when the smart meter is provided in a new building or in the course of a major renovation. This is confirmed in Recital 30:

> 'When a connection is made in a new building or a building undergoes major renovations, as defined in Directive 2010/31/EU, such individual meters should, however, always be provided.'

In time every building needs to be renovated or will be replaced by another. Time is therefore the only thing that stands in the way of full-scale deployment of smart meters.

2.2 The goals supposedly served by mandatory installation

The necessity of the mandatory installation of smart meters should be assessed in relation to their objective of contributing to energy end-use efficiency. The meters supposedly aim to achieve this objective in two ways. First, the meter should provide up-to-date information to customers on their actual consumption frequently enough to enable them to regulate their electricity-consumption, in other words, by raising awareness. Second, the meters should

[23] These are not just theoretical exceptions. In 2013 Ernst & Young delivered a report by government order of the German Federal Ministry of Economics in which they concluded the following: 'The EU Scenario targeting a roll-out quota of 80% by 2022 by a general mandatory installation provides a negative net present value and is also not economically reasonable for the majority of consumer groups. Even under optimistic assumptions, the majority of end consumers cannot compensate costs related to the installation and operation of smart metering systems by energy conservation and load shifting. Furthermore, a system charge must be paid by end customers over many years without benefiting from a smart metering system. Therefore, a system charge of €29 p.a. and per customer in addition to the current charge of €21.60 p.a. was not justifiable.' See Ernst & Young, 'Cost-benefit analysis for the comprehensive use of smart metering' (On behalf of the Federal Ministry of Economics and Technology, Ernst & Young GmbH 2013) 57.

[24] For example Italy and Sweden.

facilitate the active participation of consumers in the electricity market through the realisation of the smart grid.[25]

The capacity of smart meters to contribute to these objectives has not been firmly established in all Member States. In a 2014 Commission report benchmarking the smart meter deployment, the numbers thus far were taken as an indication that 'the business case for rolling out smart metering is not yet overwhelming throughout Europe'. [26]

Raising awareness

One of the assumptions behind the smart meter is that it would allow for frequent and detailed billing which would encourage customers to regulate their own behaviour. This assumption rests on the contested theory of the rational consumer borrowed from economics. According to Directive 2012/27/EU it is the implementation of smart meters[27] that 'enables frequent billing based on actual consumption'.[28] The Directive itself provides that smart meters are not necessary to provide frequent billing, since this also may be performed through 'a system of regular self-reading by the final customers whereby they communicate readings from their meter to the energy supplier'.[29]

It could nevertheless be argued that the smart meter is much more proficient in allowing people to monitor their electricity consumption. According to the Commission, in the impact assessment as well as the explanatory memorandum, the provision of detailed energy consumption data to households through billing and smart metering is:

> 'valuable in reducing the information gap that is one of the barriers to efficiency and could yield major energy savings. Other options to promote energy efficiency via voluntary measures are assessed as insufficient to tap all the available potential for savings.'[30]

[25] It should be noted that the smart grid adds a lot of factors which complicate the assessment of the necessity of the mandatory installation of smart meters. The smart grid is only relevant in the context of electricity. It will be further discussed below.

[26] Commission, 'Benchmarking smart metering deployment in the EU-27 with a focus on electricity'(Report from the Commission) COM (2014) 356 final 4.

[27] Although the Directive speaks of 'intelligent metering systems' there are strong indications that the drafters use this term interchangeably with smart meters, although there are also indications that state the opposite, which could reveal that these are technical issues which specificities go beyond the knowledge of the drafters.

[28] Recital 33 Directive 2012/27/EU.

[29] Article 10 (1) Directive 2012/27/EU.

[30] Commission, 'Impact Assessment accompanying the document Directive of the European Parliament and of the Council on energy efficiency and amending and subsequently repealing Directives 2004/8/EC and 2006/32/EC' (Commission Staff Working Paper) SEC (2011) 779 final 69; Proposal for a Directive of the European Parliament and of the Council on Energy Efficiency and Repealing Directives 2004/8/EC and 2006/32/EC COM (2011) 370 final. For an elaborate description see: The European Council for an Energy Efficient Economy, 'Steering through the maze #5. Your eceee guide to following the approval process of the proposed Energy Efficiency Directive' (The European Council for an Energy Efficient Economy 2017). I owe these findings to Cuijpers and Koops (n 19) 269.

In 2011 the Commissioner for Energy Oettinger held a speech stating that first experiences showed a reduced energy consumption of around 10%.[31] In a later report by the Commission the estimated energy saving was expected to be 3%, this included gas as well as electricity.[32] One of the reasons for the estimated saving is the presence of an in-home display which allows people to become more aware of their consumption. In the Netherlands, however, the smart meters lack such a display. According to the authors of a report submitted in 2016 from the Dutch Planning Office for Environment (Planbureau voor de Leefomgeving, a government agency), this was the reason that the estimated benefits of 3,5% did not even reach 1%.[33] The reason for this gap, according to the authors, lies in the fact that the smart meter does not provide an interface like an app, website or display.

Even if it is correct that providing consumers with easily-accessible information about their energy usage rates leads to a reduction of consumption, this does not justify the conclusion that we need smart meters. In any case, people can just observe on a display what their energy-usage is and for this the data does not have to be communicated to a server outside the household. In conclusion, raising awareness does not require equipping a meter with two-way communication features.[34]

Smart grid

The smart grid was introduced in Directive 2009/72/EC[35] as a project for Member States to optimise the use of electricity. The Commission, the Article 29 WP, as well as EU Commission Task Force on Smart Grids (TFSG) all agree that smart meters are a necessary component to realise a smart grid.[36] The smart meter is said to perform an essential function in the smart grid on a low voltage level and to 'bring intelligence to the "last mile" between the grid and the final customer'.[37] The smart meter enables two-way digital communication allowing the grid to record individual electricity usage. This allows for the dynamic coordination of supply and demand within the electricity grid, hence rendering it *smart*.

---

[31] See Günther Oettinger, 'Speech of Commissioner Oettinger at the Press point EUSEW' (EUSEW, Brussels, 12 April 2011).

[32] COM (2014) 356 (n 26) 6. In the same report it was concluded that the cost benefit analysis of 7 out of 23 Member States was either negative or inconclusive.

[33] Kees Vringer en Ton Dassen, 'De Slimme Meter, Uitgelezen Energie(K)?' (Achtergrondstudie, PBL Planbureau voor de Leefomgeving 2016).

[34] Another reason for the disappointing result of the benefits is that five out of nine smart meters that have been tested in a research of the University of Twente and the Amsterdam University of Applied Sciences (Hogeschool Amsterdam), show that they register substantially higher values than are actually consumed, up to 582% higher, which renders the meters quite smart for electricity providers, but less so for consumers. Frank Leferink, Cees Keyer and Anton Melentjev, 'Static energy meter errors caused by conducted electromagnetic interference' (2016) 5 (4) IEEE Electromagnetic Compatibility Magazine 49.

[35] Article 3(11) of Directive 2009/72/EC.

[36] EU Commission Task Force for Smart Grids, Expert Group 1: Smart grid standards, 'Functionalities of smart grids and smart meters' (Final Deliverable, The Publications Office of the European Union 2010) 6.

[37] ibid 16.

Smartening up the grid through the implementation of smart meters provides the supply-side of the market with an insight into the real-time use of electricity on the level of the individual household. Using this information, it can manage supply and demand more efficiently, e.g. by automatically or manually switching devices off. The balancing of demand and supply can be established through dynamic pricing, which provides an incentive for final customers to adapt their consumption to the time of the day when demand is low.[38] Utilities using different tariffs to encourage customers to use electricity in times when demand is low is a longstanding practice well before the introduction of the smart meter.

The general idea is that the smart meter allows a more pro-active approach, because it has the ability to mediate which devices within the household actually run. The smart meter can, for example, be programmed in a way that it runs the dishwasher whenever it is told by the server of the meter operator that demand is low.[39] This is referred to as *demand response management*. This allows utilities to shave off peak loads, instead of relying on either expensive back-up capacity, for instance gas reactors, or too large a *base load* — the minimum uninterrupted supply of power generated by static power plants that are not easy to shut down (i.e. coal or nuclear plants), irrespective of the demand, that keep the conventional grid running.[40] Peaks in electricity demand require the activation of smaller and more responsive power plants that usually run at a higher cost, therefore utilities try to minimise their use.

On top of dynamic pricing,[41] the argument is made that the smart grid integrates decentralised generation and storage of electricity, facilitating the use of future renewable energy sources.[42] Although there is no central definition of smart grid functionalities,[43] the policy documents show that the aim of smart meters is to bring demand response management from the level of big industrial customers to that of individual households. The anticipated energy saved by this move is actually the most important benefit that comes from the introduction of the smart meter and should be balanced against the costs in the impact assessment.[44] The smart meter is positioned as a measure to realise a functioning smart grid on micro-level.

Even this positioning, however, should not be conceived uncritically. Smart meters do not have the monopoly on the integration of decentralised electricity generation into the grid.

[38] Recital 44, 45Annex XI (3) Directive 2012/27/EU.

[39] EU Commission Task Force for Smart Grids Expert Group 2, 'Regulatory Recommendation for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems' (The Publications Office of the European Union 2014) 74.

[40] EU Commission Task Force for Smart Grids, Expert Group 1 (n 36) 16.

[41] In section 4.2 of this chapter it is explained why dynamic pricing does not require the communication of detailed consumption data.

[42] EU Commission Task Force for Smart Grids, Expert Group 1 (n 36) 46. This argument, as far as it tries to paint conventional meters as being unable to perform the same task, is actually false. This will be explained in the last paragraph of this section.

[43] Michael Specht and others, *Standardization in Smart Grids* (Springer-Verlag 2013) ch 11, 179-188.

[44] Luciano De Castro and Joisa Dutra, The Economics of the Smart Grid (Published conference paper from the 49th Annual Allerton Conference on Communication, Control, and Computing, IEEE 2012).

Both smart and conventional meters are able to deliver electricity back to the grid.[45] The only distinction is that at the end of the year the conventional meter shows the net difference between consumption and production, while the smart meter shows the exact amount of electricity produced and consumed. Smart meters, therefore, facilitate the taxation of home-produced electricity and their installation can result in less return of investment for people who, for instance, invest in solar panels. In Spain, the government uses the surveillance features of the smart meters to protect the vested interests of conventional industry, by taxing the electricity that people produce and consume themselves. It even made it mandatory to connect to the grid, in order to find out how much energy is produced per household. The fine faced by citizens who produce energy and do not connect to the grid can run up to a shocking € 30 000 000. This shows that within certain circumstances the functionalities of the smart meter can be used to consolidate existing oligopolies which is in direct conflict with the stated policy goal of energy efficiency. Therefore, smart meters are not unequivocally beneficial to the uptake of decentralised and sustainable power production.

Finally, it is important to repeat here that a smart grid can also exist on macro-level, where demand and supply are integrated on neighbourhood-level together with big industrial customers. In the Netherlands, the grid is already smart on that level. A relevant question that should have been asked before the introduction of smart meters is how big the energy savings are when smart meters are deployed in individual households as opposed to the smart grid on this higher level. It is this difference which should put the weight in the scales of policymakers balancing costs and benefits of introducing smart meters. The industry also commented on the annual convention of Europe's electricity association Eurelectric in 2016 that smart meters are actually not necessary for the transition to an intelligent electricity grid.[46]

Even if the fiction that the smart meter is indispensable for the smart grid is accepted, the realisation of the smart grid becomes fully dependent upon the successful roll-out of the smart meter. Consequently, trust in these meters is of vital importance for this immense project. The follow-up question is then whether the smart meter needs to share detailed data outside the household, in order for the smart grid to function and whether it needs to be equipped with a function which allows it to remotely shut down the electricity supply. These questions are addressed in the next section.[47]

---

[45] Radar, 'Slimme meter: van het meterkastje naar de muur' (20 March 2017) <https://radar.avrotros.nl/uitzendingen/gemist/20-03-2017/slimme-meter-van-het-meterkastje-naar-de-muur/> accessed 5 June 2018, 7:15.

[46] See Elza Holmstedt Pell, 'Smart meters 'not needed' after all for European power grid' (Euractiv) <https://www.euractiv.com/section/energy/news/smart-meters-not-needed-after-all-for-european-power-grid/> accessed 23 October 2013.

There are a number of studies that actually cast shadow over the sunny predictions made by consultancy firms on the positive return of investment of the smart meter. The Brattle Group, a US based consultancy firm, made a calculation of the profits to be gained through successful adoption of dynamic tariffs. In their own report they estimate the cost of investment to be € 51 billion, the highest benefits gained through dynamic tariffs € 67 billion, yet the lowest benefits only € 14 billion. According to these estimates the best-case scenario would

3. The functions of the smart meter

The aim of this section is to establish the functions of the smart meter that interfere with the right to respect for private life and the home, as well as the sources of these interfering functions, whether in the Directive 2012/27/EU (the legislative act) or the implementing acts conferred on the Commission. Determining the functions explicitly provided in the Directive is of fundamental importance for the assessment whether these functions comply with the requirements that follow from the Charter. If the functions are not found in the Directive, or any other legislative act, yet they do interfere with the right to privacy, they are not provided for by law. This means they constitute a breach of the right to privacy. Moreover, in this case they will conflict with the rules for implementation as established in Article 291 TFEU.

3.1 Groundwork by the Commission

The smart meter was first introduced in Directive 2006/32/EC as an instrument for realising energy efficiency. This Directive found its legal basis in Community policy on the protection of the environment (former Article 175 TEC, current Article 192 (1) TFEU) and was later repealed by Directive 2012/27/EU — with the legal basis now deriving from the Union policy on energy (Article 194(2) TFEU). The main rationale thereby shifted from the protection of the environment to the establishment of the internal market in energy. Under Article 175 TEC, the competence to take action resided with the Council, which shifted to the Commission under Article 192(1) TFEU.

Before the last directive was adopted, the Commission aimed to reach consensus on the functions of the smart meter in order to enable Member States to carry out cost benefit assessments (CBAs).[48] On the basis of 11 CBAs of Member States, 13 key functionalities were established, which were adopted in a questionnaire. This questionnaire was then answered by these 11 Member States and consensus was reached on 10 of them. Just before Directive 2012/27/EU was adopted the DG Energy (hereinafter DG ENER) and the DG for

---

result in € 18 billion profits, yet the worst-case scenario € 37 billion loss. The result seems to be a far cry from the proverbial carrot that would tempt the mule. The smart grid as a business case and legitimate policy goal to reach energy efficiency is therefore at least questionable.

[47] See '60 años de investigaciones económicas han impulsado el desarrollo del país' (ElPais, 16 August 2015) <http://www.elpais.cr/2015/08/16/60-anos-de-investigaciones-economicas-han-impulsado-el-desarrollo-del-pais/83700/?fb_action_ids=604341192919588&fb_action_types=og.likes&fb_source=other_multiline&action_object_map> accessed 5 June 2018; Kelly Phillips Erb, 'Out Of Ideas And In Debt, Spain Sets Sights On Taxing The Sun' (Forbes, 19 August 2013) <https://www.forbes.com/sites/kellyphillipserb/2013/08/19/out-of-ideas-and-in-debt-spain-sets-sights-on-taxing-the-sun/#353dbbc894e5> accessed 18 April 2016; Don Quijones, 'The Men Who're Stealing The Sun' (Wolf Street, 14 June 2015) <https://wolfstreet.com/2015/06/14/the-men-who-stole-the-sun-spain-solar-power-taxes-fines-to-protect-giants/> accessed 18 April 2016.

[48] EU Commission Information Society and Media Directorate-General and Energy Directorate-General, 'A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the Smart Meter' (Full Report, The Publications Office of the European Union 2011) 3.

the Information Society (hereinafter DG INFSO) published a report in which these functionalities were introduced as the 'Set of common functional requirements'.[49]

In the final act, the Commission convened a workshop with the regulators of the Member States to forge consensus on the functionalities. The functionalities that were agreed upon were the result of a questionnaire answered by the ministries responsible for energy and then finalised in a workshop with the national regulators. This process relied heavily on the involvement of the executive branches of government. The final functionalities with high consensus were that the meter:

- Provides readings from the meter to the customer and to equipment that he may have installed;
- Updates these readings frequently enough to allow the information to be used to achieve energy savings;
- Allow remote reading of meter registers by the Meter Operator;
- Provides two-way communication between the meter and external networks for maintenance and control of the meter;
- Allows readings to be taken frequently enough to allow the information to be used for network planning;
- Support advanced tariff systems;
- Allows remote ON/OFF control of the supply and/or flow or power limitation;
- Provides Secure Data Communications;
- Fraud prevention and detection;
- Provides Import/Export & Reactive Metering.

These functionalities were adopted in a Recommendation the Commission adopted in 2012.[50] Some of these functionalities clearly interfere with the right to privacy. First, function 2 means that usage of electricity will be updated every 15 minutes.[51] These registrations can provide a detailed oversight of the time of activity within the house. Second, function 3 allows the meter operator to read the meter registers remotely. The last interference is of a different nature and concerns the function to remotely throttle or shut down the electricity supply, which is found in function 7. Although this function does not see to the registration of any data, it still allows for a major interference with a household. The question is what legitimises this function. This is a risk to the respect for the home as it allows interference with the very occurrences powered by electricity that take place within it. These three functions most obviously interfere with the right to private life and the home.[52]

[49] ibid.
[50] Recommendation 2012/148/EU.
[51] ibid.
[52] The severity of this interference will be established in section 4.2.

3.2 Privacy infringing functions in the Directive

This section is concerned with establishing whether the privacy infringing functions of smart meters are required by law. Article 13 of Directive 2006/32/EC arranged metering and billing issues, which was instructive for the functions the smart meter should perform.[53] In Directive 2012/27/EU, these issues were rearranged under Article 9 and 10. Article 9(2)(a)-(d) provide the functionalities that the Member States should equip the smart meters with:

> '2. Where, and to the extent that, Member States implement intelligent metering systems and roll out smart meters for natural gas and/or electricity in accordance with Directives 2009/72/EC and 2009/73/EC:
>
> a) they shall ensure that the metering systems provide to final *customers information on actual time of use* and that the objectives of energy efficiency and benefits for final customers are taken into account when establishing the minimum functionalities of the meters and the obligations imposed on market participants;
> b) they shall ensure the security of the smart meters and data communication, and the privacy of final customers, in compliance with relevant Union data protection and privacy legislation;
> c) in the case of electricity and at the request of the customer, they shall require meter operators to ensure that the meter or meters can account for electricity put into the grid from the final customer's premises;
> d) they shall ensure that if final customers request it, metering data on their electricity input and off-take is made available to them or to a third party acting on behalf of the final customer in an easily understandable format that they can use to compare deals on a like-for-like basis.'

A number of final functionalities can be discerned in these subs. Sub a explicitly determines that the meter provides information to the customer on the actual time of use and sees to the *recording of this data* and corresponds to functionality 1. Sub b corresponds to functionality 8, the providing of secure data communications. Sub c implies that electricity can be received and delivered to the grid, which can be linked to functionality 10.

Some other functions can be discerned from this text, but they are not made explicit. For example, 'data communication' implies data can be communicated, but it does not clarify which data it refers to, for which purposes it is processed, to whom it is communicated and under which conditions. The taking into account of energy efficiency when setting the minimum functionalities, could be read as an implicit demand that the meter should be able to manage the demand of the customer.

[53] According to: Commission, 'Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability' (Enterprise and Industry Directorate-General , Consultation date: 21 January 2009) M/441 EN; Article 13 of Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC [2006] OJ L 114/64 'is a performance-related requirement which must be satisfied as fully as possible by means of measures which need not be technical specifications'.

Furthermore, the meters should enable the provision of accurate billing information based on actual consumption. According to Article 10(2),

> '…..Member States shall ensure that final customers have the possibility of easy access to complementary information on historical consumption allowing detailed self-checks. Complementary information on historical consumption shall include: …
>
> b) '*detailed data according to the time of use* for any day, week, month and year. These data shall be made available to the final customer via the internet or the meter interface for the period of at least the previous 24 months or the period since the start of the supply contract if this is shorter.'

Here, the term 'detailed data' is introduced for the first time. The Commission refers to the rights of final customers to detailed information.[54] It can also be read differently, as an obligation for Member States to introduce a mandatory data retention regime for detailed data on the personal household generated by the smart meters. That this detailed data is one of the most problematic aspects of the smart meter seems to be lost on the legislator. The formulation of this provision seems to suggest that the possibility of reading this data from either the meter itself or the internet is a trivial matter, while in terms of privacy protection the difference is of paramount importance. If the data can only be read from the meter itself this allows for the possibility to store the data locally on the meter and only grant access to the final customer. This solution favours privacy (although it still creates a risk to privacy of individual members within the household). When the detailed data can be accessed through the internet it means that the data has to be stored outside of the control of the data subject and third parties might get access to it as well.[55]

Proponents would argue that ex post controls can legitimise this storage. This argument ignores two important and interrelated matters. First of all, efficient privacy protection requires a proactive approach to design. Personal data should not be recorded unless this is absolutely necessary. If data are recorded nevertheless, it should be recorded in a form which only reveals the necessary information within the smart meter context, like billing information and avoiding fraud.[56] Second, assuming ex post controls will limit the access to

---

[54] Commission, 'Implementing the Energy Efficiency Directive – Commission Guidance'(Communication from the Commission to the European Parliament and the Council) COM (2013) 762 final 6.

[55] There are forms of remote feedback that do not require detailed data and still achieve energy reductions, see Eoghan McKenna, Ian Richardson and Murray Thomson, 'Smart meter data: Balancing consumer privacy concerns with legitimate applications' (2012) 41 Energy Policy 807, 810.

[56] Both of which can take place anonymously, see Klaus Kurasawe, George Danezis and Markulf Kohlweiss 'Privacy-friendly Aggregation for the Smart-grid' (Microsoft Research, 2011) < https://www.microsoft.com/en-us/research/publication/privacy-friendly-aggregation-for-the-smart-grid/?from=http%3A%2F%2Fresearch.microsoft.com%2Fpubs%2F146092%2Fmain.pdf> accessed 5 June 2018; Information and Privacy Commissioner of Ontario and The Future of Privacy Forum, 'SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation'(Information and Privacy Commissioner of Ontario 2009) <https://www.smartgrid.gov/files/SmartPrivacy_for_Smart_Grid_Embedding_Privacy_into_Design_El_200909.pdf> accessed 5 June 2018; Eoghan McKenna (n 55)

the data to the original designated parties ignores reality, as well as the underlying vision on the IoT, which is increasingly permeating the organisation of information flows in society.

The requirement for meters to *provide information on the actual time of use* (Article 9(2)(a)) in combination with the enablement of accurate billing on the basis of *detailed data according to the time of use* (Article 10(2)(b)), implies that the meter should record detailed data which can reveal intimate aspects of one's life. This recording in conjunction with the communication functions turns the smart meter into a potential surveillance device, the mandatory installation of which equals forcing spy equipment into the homes of virtually all citizens of the EU. The recording and communication of data regarding electricity usage every 15 minutes for long periods of time, allows drawing very detailed maps of people's personal lives, which can be used by commercial parties as well as public authorities. The CJEU has determined in the past that the recording and communication of data of a more personal nature raises an interference with the right to private life, where the prospect of purpose creep (again central to the IoT-vision) multiplies the severity of this interference.[57]

These meter functions correspond to function 2 and 3 of the 'Set of common functional requirements of the smart meter' to update readings and allow them to be remotely read by the meter operator. Nevertheless, they are not explicitly provided in the Directive and therefore lack a legal basis.

An implicit reference to function 6 and 7 — supporting advanced tariff systems and remotely turning the flow of power on/off or limiting it — could be read in Article 15(4):

> 'Member States shall ensure the removal of those incentives in transmission and distribution tariffs that are detrimental to the overall efficiency (including energy efficiency) of the generation, transmission, distribution and supply of electricity or those States shall ensure that network operators are incentivized to improve efficiency in infrastructure design and operation, and within the framework of Directive 2009/72/EC, that tariffs allow suppliers to improve consumer participation in system efficiency, including **demand response**, depending on national circumstances.'[58]

Although Article 15 does not define functions explicitly, advanced tariff structures do depend on meters that are able to perform demand response, i.e. 'the ability to time-shift demand'.[59] 'Demand response', the possibility for the meter operator to communicate the actual state of the demand to the customer, in combination with 'advanced tariff structures' are labelled by the Commission as 'a key driving force for empowering the consumer and for achieving energy efficiency'.[60] Dynamic pricing through fluctuating tariffs is already a popular practice

[57] For the interference see Case C-195/06 *Österreichischer Rundfunk (ORF)* [2007] ECR I-08817 and see the potential future use from Chapter 2, section 2.1.

[58] Emphasis added by author.

[59] Eoghan McKenna (n 55) 811.

[60] EU Commission Information Society and Media Directorate-General and Energy Directorate-General, 'A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the Smart Meter' (Full Report, The Publications Office of the European Union 2011) 48.

with large scale customers but, as explained in section 2.2, the smart grid can take it a step further to individual households.

In conclusion, the privacy infringing functions of the smart meter (2, 3 and 7) are not established by the Directive. The Directive does not need to flesh out all details of data processing, it can establish principles guiding the work of the Commission and specifying the boundaries of its mandate. Nevertheless, all data processing that potentially constitutes an interference with the right to private life and the home should be explicitly provided for in the Directive in order to be in accordance with the ECHR and the Charter.

3.3 Privacy and data protection in the Directive

The only reference to privacy and data protection in Directive 2012/27/EU is generic and provides that Member States have to ensure the security of the smart meters and data communication, and the privacy of final customers, in compliance with relevant Union data protection and privacy legislation.[61] The EP included this provision during the drafting process.[62] Member States are bound to other EU legislation when they implement directives. In this respect, the mentioned provision does not provide anything new. It could be viewed, however, as an attempt by the EP to compensate its omission in demanding clarity with respect to the meter function; a warning that the space of indeterminacy is bound by privacy and data protection legislation. This is a very general instruction, nevertheless, which does not provide any guidance on the interpretation of the open norms inherent in privacy and data protection law. Establishing the applicability of relevant EU legislation does not result in effective protection of the right to the protection of personal data. Directive 2012/27/EU has a particular link to fundamental rights and therefore the specific limitations of fundamental rights should have been addressed in the explanatory memorandum and why these are compatible with the Charter. This would also be in line with the Commission's stated strategy for the effective implementation of the Charter as discussed in Chapter 4.[63]

In the legislative process towards the adoption of Directive 2012/27/EU, the functions of the smart meter were already established by the Commission in collaboration with the ministries of eleven Member States. The roll-out of smart meters fell under the scope of the Directive and was part of its implementation. The EU legislature, thus, should have been aware that the mandatory deployment of smart meters equipped with the functions discussed earlier 'may interfere with the fundamental right of the persons concerned, and some of those interferences may be so serious that intervention by the EU legislature becomes necessary'.[64]

[61] Article 9(2)(b) of Directive 2012/27/EU

[62] European Parliament Committee on Industry, Research and Energy, 'Report on the proposal for a directive of the European Parliament and of the Council on energy efficiency and repealing Directives 2004/8/EC and 2006/32/EC (COM(2011)0370 – C7-0168/2011 – 2011/0172(COD))'(A7-0265/2012), 55.

[63] Commission, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'(Communication from the Commission) COM (2010) 573 final 8.

[64] Case C-363/14 Parliament v Council ECLI:EU:C:2015:579, [2015], para 53 ; C-355/10 Parliament v Council ECLI:EU:C:2012:516, [2012], para 77.

The EU legislature should have determined the principles governing the processing of personal data through the smart meter. Given the fact that the meter is deployed on the basis of legislative power, there should have been a definition of the data processed and detailed arrangements for their processing.[65] In the end, these factors were left to be determined by the ESOs in standards which are not even properly published. It is unclear why the legislature relies on the Member States to ensure the privacy of final customers and does not choose to address the issues at the European level.

First of all, in section 3.1 it became clear that Directive 2012/27/EU was adopted only after the most important decisions on the design of the meter were taken. Considerations on the right to privacy and data protection legislation were seemingly absent from these decisions. This saddled the Member States with a very tough challenge, which only Germany has taken on successfully.[66] The fact that Germany could meet this challenge even after a privacy-unfriendly design had been adopted, demonstrates that the smart meter in its current state could never meet the 'less restrictive means' test. PbD should have been the default that followed from the Directive, instead of the prerogative for German citizens. The current situation is somewhat comparable to giving a person a car without brakes and then telling him he should be careful not to cause any accidents. The decisions on design were informed by a consensus between the ESOs and the representatives of national ministries responsible for energy, without the involvement of ministries of justice or other parties with expertise in fundamental rights. In other words, the parties responsible for making choices about the design cannot be expected to be particularly aware of law and fundamental rights.

A counter-argument could be that this is why the EU has a fundamental rights framework; to function as a backstop. Taking an anticipatory approach to the design of IoT- and other devices introduced by law, would be, however, more in line with the proactive attitude proclaimed by the Commission, and could ensure that privacy is taken into account before a system is designed. Waiting until a system is challenged before a court would mean that if it is struck down it needs to be redesigned, which is both ineffective and unlikely to happen. Moreover, even if the design of these systems is successfully challenged within the EU legal system, it is unrealistic to expect that it will lead to Member States complying with a judgment and redesigning the systems. This is a lesson which can be drawn from the current state of data retention laws in the EU, in particular in relation to the implementation of Directive 2006/24/EC. Whilst this Directive was annulled by the CJEU in 2014, in eight out of 21 Member States the original implementation is still in place.[67] In the majority of the

[65] Compare Case C-201/14 Smaranda Bara ECLI:EU:C:2015:638, [2015], para 40. Case C-363/14 *Parliament v Council* ECLI:EU:C:2015:579.

[66] Germany, for example, has actually deployed smart meters with an additional system which guaranteed 'data sovereignty' to customers over their measurement data. Frank Pallas, 'Beyond Gut Level – Some Critical Remarks on the German Privacy Approach to Smart Metering' in Serge Gutwirth and others (eds) *European Data Protection: Coming of Age* (Springer 2013).

[67] Privacy international, 'National Data Retention Laws since the CJEU's Tele-2/Watson Judgment: A Concerning State of Play for the Right to Privacy in Europe' (Privacy International, 2017) <https://privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf > accessed 5 June 2018, 12.

Member States where national laws implementing the Data Retention Directive were annulled, after the CJEU declared this directive invalid in *Digital Rights Ireland*, this was the result of a challenge brought by NGOs to national courts.

Secondly, by not formulating explicit demands regarding privacy for the design of the meter the EP and the Council are left without a reference point to overseeing the work of the Commission and the ESOs. Details of the design of the meter which do impact the right to privacy will most likely be formulated in hard to impossible to understand technical jargon embodied in voluminous standards. The effective protection of fundamental rights is lost in the ESOs' translation.

4. Impact assessment and Explanatory memorandum

This section addresses the Commission's position leading to its legislative proposal, in particular to its observance of the right to privacy and data protection legislation. To analyse the latter, the impact assessment and explanatory memoranda of the relevant directives are discussed.[68] The Data Protection Impact Assessment Template, a document which is meant to assist stakeholders in the process of deploying and maintaining the smart grid in line with data protection legislation is also analysed below.[69]

The last section revisits the impact assessment and explanatory memorandum in light of the Commission's rhetoric and against the case law of the ECtHR and CJEU.

4.1 Impact assessment and Explanatory memorandum of the Commission

When legislation is considered that forces citizens to have an ICT-system installed into their homes, one would expect a buzzer to go off and Commission staff gliding down a pole in fireman-like-fashion to meticulously scrutinise the impact of this legislation on fundamental rights. At least, this is the impression made by the Commission's rhetoric on the respect of fundamental rights. [70] Directive 2006/32/EC, Directive 2009/72/EC and Directive 2012/27/EU, however, share a common characteristic: in the explanatory memorandum of their initial proposals not a single word is dedicated to either fundamental rights, or data protection legislation. The impact assessments executed prior to the proposal of Directive 2009/72/EC and Directive 2012/27/EU laid a firm foundation for this awkward silence on fundamental rights; neither mentioned privacy or data protection. The result is a compelling

[68] Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC [2006] OJ L 114/64 was not preceded by an impact assessment.

[69] This was written by a group of experts set up by the Commission also known as the Smart Grids Task Force.

[70] Andrew Murray commented on this as follows: "I love this idea. Unfortunately no I don't think this would ever happen, instead I imagine a conversation like this. Commission Employee 1: Are we compliant with the EU Charter? Commission Employee 2: *Shrugs*. I think so, if we're not I'm sure someone will bring a challenge. Commission Employee 1: Good enough for me."

contrast against the background of Commission communications praising impact assessments as the tool to realise a fundamental rights culture in its proposals and the subsequent legislative process. In keeping with the commitment of the Commission to turn the EU into a shining example of effective protection of fundamental rights, the logical thing to do would have been to execute a separate impact assessment on fundamental rights. Apparently the buzzer was defective, or the firemen were deep asleep.

Smart meters and their supposed benefits are not critically assessed in the impact assessments of the energy directives. The impact assessment of Directive 2009/72/EC does mention smart meters, but only as a measure to enhance retail competition.[71] The main problem established in the assessment of Directive 2012/27/EU is how to realise 20% energy savings by 2020.[72] It does not follow unequivocally what the benchmark is for calculating this 20%, which is problematic in itself. Smart meters are supposed to contribute to this goal by improving the ability of consumers to manage their energy consumption.[73]

In the impact assessment two policy options are considered in relation to metering and billing: enhanced obligations for energy companies (C5), and voluntary measures by Member States (C6).[74] In the first option, common EU requirements are set for the provision of feedback by metering and the frequency of billing based on actual consumption. Member States were held to properly implement and monitor the provisions, whilst retaining flexibility to decide on technical aspects of the meter.[75] These options are only further discussed in the context of environmental impact and impact on energy consumption. Nothing is mentioned about possible implications for fundamental rights. In the consideration of both options, weight was attached to the supposed saving of energy following the insight smart meters provide into consumption behaviour (this is also mentioned under social impacts). The fact this insight can be gained without communicating detailed meter data to external parties is not addressed. Other benefits mentioned are the cutting back of administrative burdens. C5, imposing obligations, is, therefore, presented as the preferred option.[76]

In a table on the different policy options C5 is depicted as the option that scores higher on effectiveness and efficiency.[77] Subsidiarity and proportionality in C5 are justified because of 'the number of complaints from citizens on transparency and accuracy of metering and billing indicates that the problem has not been solved in many countries.'[78] The example

[71] Commission, 'Impact Assessment Accompanying the Legislative Package on the Internal Market for Electricity and Gas COM (2007) 528 final COM (2007) 529 final COM (2007) 530 final COM (2007) 531 final COM (2007) 532 final SEC (2007) 1180' (Commission Staff Working Document) SEC (2007) 1179/2 53. This is in stark contrast with the findings of R Anderson, which will be treated in section 5.4.2.

[72] SEC (2011) 779 (n 30) 9.

[73] In section 5.2.2 this was already criticised.

[74] SEC (2011) 779 (n 30) 20.

[75] I will return to this flexibility and to what extent this is out of place in the next section.

[76] SEC (2011) 779 (n 30) 44

[77] ibid 54.

[78] ibid 54.

mentioned are 12 000 complaints in Italy in one year. It is not clear how these complaints justify the imposition of a mandatory smart metering regime on the entire territory of the EU. The main message is that the smart meter will provide customers with more control over their own consumption. In the section of 'Economic impacts', the possibility of a 100% roll-out of smart meters (when assessed positively) in 2022 is mentioned, after the initial 80% in 2020.[79] The functions of the meter are not addressed in the assessment. The character of the assessment is purely economic, which is demonstrably at odds with the fundamental rights ambitions the Commission has been declaring since 2005. This document highlights the severe gap between theory and practice of the Commission's *fundamental rights reflex*.

4.2 The Data Protection Impact Assessment Template

In 2009 the Commission set up the Smart Grids Task Force, consisting of five 'Expert Groups' each with their area of focus. A substantial part of the work undertaken by Expert Group 2 (EG2) 'Regulatory recommendation for privacy, data protection and cyber-security in the smart grid environment' focused on privacy and data protection issues. EG2 started with a critical attitude towards smart meters which materialised in the draft of their first report in 2011, in which they stated that the following principles should apply to data retention:

> '(a) data minimisation — i.e. the scope and length of both (i) data collection and (ii) data retention shall in any case not exceed absolute minimum.'

In the final report this text was replaced by:

> '(a) data minimisation — i.e. the scope and length of both (i) data collection and (ii) data retention shall in any case not exceed what is necessary to achieve specific and lawful purpose.'

The difference is small but indicative for the further decline of the critical attitude of this group which reached its height in the 'Data Protection Impact Assessment Template' (hereinafter 'the Template'), which it issued in 2014. The purpose of the Template is to:

> '…contribute to organisations that initiate or already manage smart grid deployments as well as those introducing changes to existing smart grid architecture platforms in identifying and assessing the privacy risks of these initiatives. In this way, organisations can take adequate measures in order to reduce these risks and, as such, reduce the potential impact of the risks on the data subject, the risk of non-compliance, legal actions and operational risk, or to take a competitive advantage by providing trust.'[80]

This was the final version, after two former concepts both received feedback and criticism from the Article 29 Working Party. The Working Party issued two opinions on the draft Template before the adoption of the final version. There were two important points of

[79] ibid 44.
[80] EU Commission Task Force for Smart Grids Expert Group 2 (n 39) 6.

criticism on the first draft. First, there was a flaw in the methodology: only risks were to be assessed while the actual impact was ignored. The second point of criticism was the absence of a section on 'best available techniques' (hereafter 'BATs').[81] The Article 29 WP pointed out to the Commission that the employment of Privacy Enhancing Technologies (PETs) and other BATs would allow citizens to keep their fine-grain meter-readings confidential. This means that these data do not have to be shared with third parties for the smart meter to function within the smart grid.[82] This confirms that privacy can be embedded in the design of a system without detriment to its functionality.[83] It is also in line with Jacobs architectural choices for a non-totalitarian society.[84]

In the second opinion, it appeared that the first point of criticism was addressed, although not to the full satisfaction of the Article 29 Working Party. Strangely, the purpose of the Data Protection Impact Assessment (hereinafter DPIA) in the final Template quoted on the previous page neglects actual impacts and only mentions risk. The second point of the criticism regarding BATs, which was most relevant for the design of the smart meter, was refused by the Commission 'reportedly because of their scope limited to the common minimum functional requirements for smart metering and their evolutive nature'.[85] The footnote directly thereafter refers to the reply of the Commission:

> '"I consider this that would not be as beneficial as you intend for the following reasons: (i) In line with the Commission Recommendation 2012/148/EU, the BATs focus only on the common minimum functional requirements for smart metering, whereas the DPIA template's scope of application strives to go beyond the last mile and include the whole smart grid spectrum; and (ii)Should the BATs be enshrine in the DPIA template, their evolutive and illustrative nature would ipso facto condemn the template to be ephemeral and possibly subject to impractically frequent revisions."

[81] Article 29 Data Protection Working Party, 'Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force' (Adopted on 22 April 2013 00678/13/EN WP205, The Article 29 Working Party 2013) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf> accessed 5 June 2018 7-8. WP 29 referred to its main points of criticism in the later opinion: 'the lack of clarity on the nature and objectives of the DPIA, methodological flaws in the DPIA Template and lack of sector-specific content: industry-specific risks and relevant controls to address those risks to be identified and matched'.

[82] ibid.

[83] Charles Raab, 'Surveillance: effects on privacy, autonomy and dignity' in David Wright and Reinhard Kreissl (eds), *Surveillance in Europe* (Routledge 2015) 261-262.

[84] Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth and others (eds), *Data Protection in a Profiled World* (Springer 2010).

[85] Article 29 Data Protection Working Party, 'Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force' (2064/13/EN WP209, The Article 29 Working Party 2013) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf> accessed 5 June 2018, 4. Italics in the original.

(letter ener.b.3 VL/cv(2013)1506536 to Mr. Kohnstamm, 27 May 2013)'[86]

Here, the Commission hides behind its initial establishment of the set of common functional requirements to justify their inaction with regard to BATs. The focus on BATs by both the Article 29 WP and the Commission is not helpful in setting the scope of the discussion, because in extension to BATs their arguments also apply to PETs.[87] This allows the Commission to argue that BATs, and by implication PETs, are not suitable for the DPIA on the basis that these are in constant flux, whilst ignoring choices on PETs which relate to fundamental architectural choices which can prevent or mitigate risks on privacy and the protection of personal data.[88] The key difference between a smart meter which stores detailed data centrally or locally on the meter is not mentioned, nor recognised, despite the fact that the Article 29 WP made this possibility explicit in the Annex of its first opinion and the EG2 pointing out this choice in its Recommendation to the Commission.[89] This is not, as the Commission comments, a feature that would make the DPIA template 'ephemeral and possibly subject to impractically frequent decisions'.

The choice between centralised or decentralised processing of detailed meter data is a political decision. It is an *essential element of smart meter design*, which is not for the ESOs, or for the Commission to decide upon. A decision like this does not suffer any of the Commission's projected fears about volatility surrounding the DPIA, instead it would provide clarity and a clear signal that citizens their fundamental rights trump business interests. The fact that the Commission has established a set of minimum functional requirements does not abdicate it from responsibility to set requirements for the design of the smart meter which reduce interference with the right to private life to a minimal extent. The Commission simply brushes off its constitutional duties under a false pretext.

The final document shows some concern for privacy, and involves some questions about control and minimising the collection of personal data. Nevertheless, the overall impression remains that the drafters seem to have ignored the core of the advice of the Article 29 WP. Among the indicators of negligence are the aforementioned purpose of the DPIA and the absence of the category of 'actual impacts' therein. Second, nothing is mentioned about centralised or decentralised (on the meter) processing of personal data.[90] The largest flaw, however, is the point of departure of this Template. It mistakenly leaves discretion to private stakeholders to make decisions which impact upon fundamental rights and belong to the essential elements of the legislative act.[91]

[86] ibid 4, footnote 5.

[87] The DPIA only mentions 'PET' once on page 17, without even writing out what the abbreviation stands for.

[88] Jacobs (n 84).

[89] EU Commission Task Force for Smart Grids Expert Group 2, 'Regulatory Recommendation for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment: Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection' (Recommendation to the European Commission, The Publications Office of the European Union 2011) 28, 29 and 36.

[90] Best Available Techniques are discussed in the section on assessment of implemented and planned controls.

[91] More on this in section 5.

4.3 The impact assessment & Explanatory memorandum revisited

Taking the mandatory meter in its current form as the point of departure, the logical next step for the Commission would have been to assess the impact on fundamental rights that follows from it. Since the original impact assessment did aim to support 'the establishment of "smart grids" that encourage energy efficiency improvements', considerations with regard to smart meter functions would have to follow from this.[92] The Commission staff should have been or was aware of how these functions might be executed, since DG ENER was both responsible for drafting the impact assessment as well as drafting the 'Set of common functional requirements of the smart meter' (the latter together with DG INFSO). These functional requirements should have been taken as the point of departure for the question of whether the smart meter constituted an interference with the right to privacy and data protection. The monitoring feature of the meter (by collecting data) and the controlling feature (by allowing remote on/off switching) are the most obvious functions which impact the private character of the meter holder's domicile.

First, function 7, the remote on- and off-control of the power supply, is assessed. The main benefit of this function is that it allows electricity suppliers to shut down remotely the supply for customers that do not pay their bills. In Italy, the deployment of smart meters with this function was mandatory, so that people who did not pay their bill could be disconnected. In a number of countries, the remote-switch was scrapped from the meter design, due to numerous reasons such as costs,[93] or cybersecurity. The off-switches can be used to enforce targets of government savings, therefore, it could be argued that this function is politically charged.[94] It was demonstrated at the US Black Hat conference in 2009 through a proof of concept that hackers could get remote control of about 15 000 out of 22 000 homes in 24 hours.[95] It could be argued that choices about the function which allows remote on and off control of the meter do not even belong to the realm of the EU legislator. Given the considerations of national security, decisions about this function fall under the sovereignty of Member States.

Secondly and more importantly, the impact of the communication function is assessed. To get a fair view of the *likelihood* and *magnitude* of this impact, the staff should have assessed this

[92] SEC (2011) 779 (n 30) 15.

[93] In the Netherlands this function was also scrapped after complementary research was executed which showed that the net extra value was only marginally positive. Fred Koenis and John van Steen, 'Schakelfunctie onder loep: Nadere verkenning van de maatschappelijke kosten en baten van de schakelmogelijkheid in de slimme meter' (Rapport in opdracht van het Ministerie van Economische Zaken, KEMA Nederland BV 2013) 32.

[94] Ross Anderson and Shailendra Fuloria, Who controls the off switch? (Published conference paper from the 1st IEEE International Conference on Smart Grid Communications, IEEE 2010).

[95] ENISA, 'Smart Grid Security' (Annex II to the ENISA study Smart Grid Security: Recommendations for Europe and Member States, ENISA 2012) 5. See also Nick Hunn, 'What's the difference between Sir Philip Green and the GB Smart Metering Program?'(Creative Connectivity, 28 November 2016) < http://www.nickhunn.com/whats-the-difference-between-sir-philip-green-and-the-gb-smart-metering-program/> accessed 5 June 2018; Nick Hunn, 'Squirrels, Grid Security and a Stuffed Rudd'(Creative Connectivity, 2 May 2016) http://www.nickhunn.com/squirrels-grid-security-and-a-stuffed-rudd/ accessed 5 June 2018; Nick Hunn, 'When Smart Meters get Hacked' (Creative Connectivity, 8 June 2014) <http://www.nickhunn.com/when-smart-meters-get-hacked/> accessed 5 June 2018.

function against the background of the Commission's communications, including on 'Future networks and the internet' adopted in 2008.[96] In this context, the smart meter starts to function as yet another extension of the ICT infrastructure that serves the interest of a range of commercial and government parties. For instance closer attention could have been paid to reports financed by the Commission. An example from Denmark, where authorities cooperate with the banking sector, might have led to a conclusion that smart meter data kept in the private sector might be accessed by public authorities, e.g. to combat social security fraud, marijuana growing or other misdemeanours.[97] The relation between information that can be inferred from smart meter data and the relevance of this information for third parties, such as public authorities, denominates the likelihood that this information will actually be used. Governments have an interest in the evolution of these smart meters into surveillance systems that can be used by local as well as national authorities for a wide range of purposes, such as taxation, fraud prevention, risk profiling etc.[98] The Article 29 Working Party also confirmed the existence of these risks.[99] Given the Commission's involvement in contiguous policies it is difficult to understand how they could have missed these relevant possibilities.

The magnitude of the interference can be established by using the most important criteria the ECtHR has formulated in its extensive case law on the right to respect for private life and the home: the nature of the interference and the interest to be protected from interference.

The intrusiveness of the initial interference — the metering of electricity consumption — depends largely on the granularity of the data recorded, and whether that data is stored locally or communicated to a central server. When the data is detailed and is used for secondary purposes, the interference can become severe. The Article 29 WP had previously warned that the increase in the amount of data processed in conjunction with making it 'more readily available to a wider circle of recipients than at present' might generate a serious backlash.[100]

[96] Commission, 'Communication on future networks and the internet' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2008) 594 final.

[97] Graham Vickery, 'Review on recent studies on PSI reuse and Related Market Developments' (final version) <https://ec.europa.eu/digital-single-market/en/news/review-recent-studies-psi-reuse-and-related-market-developments > accessed 5 June 2018; Dean Narciso, 'Police seek utility data for homes of marijuana-growing suspects'(The Columbus dispatch, 28 February 2011) <http://www.dispatch.com/content/stories/local/2011/02/28/police-suspecting-home-pot-growing-get-power-use-data.html> accessed 18 June 2014.

[98] Joseph Savirimuthu, 'Smart meters and the information panopticon: beyond the rhetoric of compliance' (2013) 27 International Review of Law, Computers & Technology 161, 161. Eoghan McKenna (n 55).

[99] WP205 (n 81) 5.

[100] Article 29 Data Protection Working Party, 'Opinion 12/2011 on smart metering' (Adopted on 4 April 2011 00671/11/EN WP 183, The Article 29 Working Party 2011) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf> accessed 5 June 2018 3.

In addition, the remote control over the electricity supply increases the intrusiveness of the interference in the primary relationship between the provider and the consumer.[101]

The frequency of the measurement intervals will also make a difference with respect to intrusiveness. The initial interference enabled through the collection of data at a 15 minute interval consists of the monitoring of indoor activity or absence thereof.[102] The registration of the 15 minute interval allows a detailed insight into the activities within the home, up to the level of which appliances are used at what time.[103] The degree of accuracy in these registrations, and thus the severity of the interference, is expected to rise when more signatures of devices become available.[104] The scope of this recording system, always monitoring every 15 minutes how much electricity has been used, amounts to the mass collection of intimate data.[105]

The nature of the data recorded by the smart meter is not what primarily determines the intrusiveness of the interference with the right to privacy. Instead, it is the nature of the information that can be inferred from the collected data. This is particularly troublesome in a context in which this data can be distributed to systems that can cooperatively profile citizens and share information with other government institutions in the course of their duties, including bureaucratic processes in which decisions concerning citizens' rights are taken. The smart meter has to be assessed against the background of a highly invasive society in which the nature of the interference is magnified by the interconnection with other nodes in a network of public and private actors who seek information about citizens and customers.[106] What is at stake is the right to be free from external interference in the confines of ones' own home; a freedom historically most threatened under totalitarian rule in which the distinction between the private and public sphere is blurred. Again, once these smart meters are utilised by opportunistic governments or corporate parties, chances become very slim that the flaws in their design will be reversed.[107]

---

[101] Use of this remote control by government for other purposes will not be treated. It should be noted, however, that remote control through ICT-systems installed on a mandatory bases for commercial purposes is not unimaginable, as will be revealed in Chapter 6.

[102] Eoghan McKenna (n 55).

[103] Victoria Y Pillitteri and Tanya L Brewer, 'Guidelines for Smart Grid Cybersecurity'(A Three-volume report, NIST Interagency/Internal Report (NISTIR) - 7628 Rev 1 2014) <https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf> accessed 4 July 2014, volume 2.

[104] Signatures of devices allow to establish what plugin-devices are used at what time through the data collected. Eric D Knapp and Raj Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure* (Elsevier 2013) ch 4, 87.

[105] *MM v The United Kingdom* App no 24029/07 (ECtHR, 13 November 2012) para 200.

[106] WP205 (n 81) 5.

[107] See section 5.3 of this chapter. In the Netherlands meter data is already used to fight welfare fraud. Even worse, in the Netherlands the data might end up in a new instrument of public bodies known by the acronym SyRI, which stands for System Risk Indication. This instrument is used to control labour and tax laws, and fight welfare fraud. The operation of this instrument involves pooling data from numerous public authorities at a private organisation that mines the data through an algorithm to come to risk indications ('risicomeldingen'). These risk indications are then stored for two years in a registry ('register risicomeldingen') where they can be

The nature of the activities restricted could be anything. The aim pursued by the restriction could be as trivial as the correct levying of taxes, combating social security fraud for which it might be relevant if individuals live together, spend most time outside of the house or display any form of behaviour which departs from the norm. Citizens aware of these type of mechanisms in place could feel monitored in their own home, where every exceptional situation that would normally stay below radar — such as the separation of partners, the distant family member that stays over for a while, the new lover that is frequently visiting, taking care of the grandchild and basically anything that affects the number of people living in the house — will now be noticed and might even require justifying if someone is in receipt of state benefits. The Dutch parliament adopted legislation granting access to the data held by the parties responsible for energy and water supply to a number of public authorities for a wide range of administrative purposes.[108] The nature of activities taking place in the home varies from private to deeply intimate.[109] The nature of the measures subsequently taken by the government and the extent to which these may intrude into a person's life should not be underestimated, as it can relate to anything that happens once the meter data triggers a government algorithm to flag a household as a risk, including the remote shut down of the electricity supply. The expectation that data will be used outside of its original context heralds the chilling effect of smart meters on behaviour inside the home, transforming the sacred precincts of domestic life into Bentham's panopticon.

This infringes on the interest to be protected from interference, to dwell in ones' home freely and uninterrupted; that is, unmonitored and unrestrained. The first two out of four stages of privacy developed by Westin, solitude and intimacy, correspond to the sort of privacy interests in need of protection.[110] The home is the place where the citizen may retreat from the 'refining influence of culture', alone (solitude) or with others (intimacy).[111] Linked back to the likelihood of an interference and against the background of a data-sharing society in which public-private partnerships are used to conjure repressive surveillance mechanisms, the meter is likely to function as a government agent and the nature of the subsequent interference can be severe and far reaching.[112]

Provided for by law & Essential elements of design as adequate safeguards

Directive 2012/27/EU does not provide sufficient clarity about the scope and the manner in which the smart meter will interfere with the right to privacy. Moreover, the prospect of

consulted by these public authorities and even the police. Smart meter data could be provided to this system, effectively subjecting people their behaviour behind the door to the scrutiny of government algorithms.

[108] Artikel 54 lid 8 Wet structuur uitvoeringsorganisatie werk en inkomen, Staatsblad 2013, 405.

[109] *Dudgeon v The United Kingdom* App no 7525/76 (ECtHR, 22 October 1981) para 52.

[110] On the state using technology to monitor the mundane see Big Brother Watch, 'Lifting the lid: The rising number of microchips in our bins and why it matters' (Report, Big Brother Watch 2009) <https://www.bigbrotherwatch.org.uk/liftingthelid.pdf.> accessed 5 June 2018.

[111] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1891) 5 Harvard Law Review 193, 194.

[112] See next paragraph.

involuntary processing of personal data concerning detailed electricity usage and remote control over a household's electricity supply for all the households in the EU, requires these interferences to be spelled out in detail. What data is processed, for what purposes, by which parties, retained for how long etcetera. The obligation for the legislature to provide these type of indications follows from the foreseeability requirement. The law does not provide an indication to citizens enabling them to foresee how the smart meters will interfere with their right to respect for privacy.

The Commission should have made demands on the *essential elements of the smart meter design*; most notably on the condition that the meters do not allow centralised processing of detailed consumption data. By leaving this space to the Member States (which in practice is utilised by the ESOs), the Commission effectively created a situation in which it was highly likely that detailed data on electricity consumption would be stored centrally and therefore become accessible to energy suppliers and governments. This discretion does not belong to the Commission, or the Member States, because it results in a general, continuous breach of the right to respect for private life and the home against the will of its occupants. Even if this breach would be mistakenly deemed not to interfere with the essence of Article 7 of the Charter, then the existence of lighter alternatives still makes it impossible for the infringing smart meter functions to pass the necessity test. Furthermore, even if it was deemed to be necessary, the severity of this breach requires at the very least a basis in the Directive which is foreseeable. The legislature should have clarified the functions and their specificities, which could be considered *essential elements of design*,[113] since choices about them determine the extent to which an interference with the right to privacy takes place. The lack of determination on these matters in the legislative act itself displays the EU legislature's lack of awareness that equipping these meters with privacy-invasive functions without a legal basis constitutes an illegal act. The result is that EU law mandates the installation of an undetermined device which can be subsequently equipped by private parties with privacy-infringing functions, thereby circumventing the protection of the Charter. A correct impact assessment, in line with the Commission's policy statements, would have ensured that adequate safeguards were put in place.[114] The advice received from the Working Party and earlier constitutions of EG2, emphasises the failure of the Commission to address fundamental rights in its smart meter policy. The Commission's failure is also evident in the absence of justifications or explanations regarding the safeguarding of the Charter rights in the explanatory memorandum of Directive 2012/27/EU.[115]

Proportionality test: necessity (other policy options) and balancing

The impact assessment does not contain an assessment of the impact of the smart meter functions on the right to private life, the home and the protection of personal data. It also

[113] See Chapter 4, section 4.1.

[114] Commission, 'Operational Guidance on Taking Account of Fundamental Rights in Commission Impact Assessments'(Commission Staff Working Paper) SEC(2011) 567 final 18.

[115] COM (2010) 573 (n 63) 8.

lacks an investigation into various policy options regarding the design of the smart meter. This investigation is inherent to an impact assessment in general and follows from testing the proportionality of the measure considered. Voluntary and mandatory measures were mentioned, but the measures themselves lacked nuances. The rationale of both the right to privacy and data protection clearly favour a least infringing alternative and are highly relevant for the design choices of the smart meter.

On the other hand, industry argues that balancing the electricity supply and demand through the smart grid requires the input of personal data. Despite this view, or perhaps *because* of this view, the Commission was required to perform 'a proper and complete investigation and study with the aim of finding the best possible solutions' in order to 'find alternative solutions and generally seeking to achieve their aims in the least onerous way as regards human rights'.[116] Without this information it is impossible to assess whether the mandatory rollout of smart meters results in a justifiable breach of the right to privacy. The Commission has failed to undertake this investigation. By neglecting fundamental design choices in the impact assessment the Commission staff waived its responsibility to take conscious, informed decisions on these matters. It is widely recognised that the effective protection of fundamental rights requires designing them into the architecture of the system.[117] The foundations of the design, therefore, should be adopted in the legislative proposal. As commented by the civil society experts on the incorporation of PbD-principles in the smart meter programme by industry:

> 'it became a buzzword, but in practice we have not seen much evidence of it. Suppliers ridiculed [genuine privacy-enhancing approaches] because they were so far away from existing processes. Throughout the process there has been no vision of how privacy by design could have been implemented. Working groups were dominated by incumbents who are only willing to go one or two steps further than where they are. Therefore, we have a sticking plaster solution on what is fundamentally not the best approach.
>
> …….
>
> Industry was directly interested in getting personal data and just not interested in privacy enhancing technologies. They also argued [PET designers such as Danezis et al.] didn't understand the industry.'[118]

The industry's sense of feeling misunderstood displays a severe lack of understanding of their responsibility, the importance of the right to privacy and its centrality to democratic society. Their nonchalance towards PET-designers, sacrificing hard won liberties to a smart meter design for their narrow interests, demonstrates their contempt for civil rights.

[116] *Hatton and Others v The United Kingdom* App no 36022/97 (ECtHR 2 October 2001) para 97.

[117] Mireille Hildebrandt, 'Legal Protection by Design in the Smart Grid' (Report commissioned by the Smart Energy Collective, Bepress 2013) <http://works.bepress.com/mireille_hildebrandt/42> accessed 5 June 2018 14.

[118] As quoted in Ian Brown, 'Britain's smart meter programme: A case study in privacy by design' (2014) 28 International Review of Law, Computers & Technology 172 10-11.

The impact assessment could have contributed to the effective protection of fundamental rights if it was used to test alternative design choices against the requirements of *proportionality* and *necessity*. This could have helped establishing the best alternative, a design choice which minimises the interferences with the right to privacy, whilst retaining its functionality within the smart grid. The existence of a large body of hard and soft law on privacy and data protection implies the legislature only enjoys a narrow margin of appreciation. [119] The legislature, in turn, should have adopted strict limits on smart meter functions in the legislative act in order to narrow the margin of appreciation of the Commission.[120]

Key to a meaningful assessment is the recognition that smart meters can be designed in a way they serve their stated aims (energy efficiency), without transmitting detailed personal data to third parties. The technical aspects of safeguarding privacy in the smart grid received some scholarly attention.[121] McKenna and others established that the smart meter can function in the smart grid whilst minimising or even avoiding the use of personal data.[122] Both the Article 29 Working Party and the EDPS confirmed the existence of a privacy-friendly alternative, the former in an opinion in which it explicitly held that it was not necessary to share the detailed data on the smart meter with third parties:

> 'In particular, innovative PETs exist, currently in different phases of research and development, which may make it possible to achieve the basic objectives of the smart metering system (billing, energy-efficient maintenance of the grid (forecasting and settlement) and security assurance (including prevention of fraud)), in such a way that it could be altogether avoided — for such basic purposes at least — that fine-grain meter readings would need to leave the smart meter or the household where the smart meter is installed.'[123]

This was long after the Article 29 Working Party had taken the position that data collected by default should remain within the household. It, also, advised to design the system in a way that data elements unnecessary to fulfil the purpose of the transmission are removed. [124] The existence of a privacy-friendly alternative was also confirmed in an interview with Bram Reinders, former head of the EG2. In an earlier report EG2 acknowledged the option for

[119] Chapter 2, section 2.2. *Roemen and Schmit v. Luxembourg* App no 51772/99 (ECtHR, 25 February 2003).

[120] Lee A Bygrave, 'Data protection pursuant to the right to privacy in human rights treaties' (1998) 6 International Journal of Law and Information Technology 247, 273. Eg Directive 95/46/EC, Article 8 ECHR, Article 7 and 8 Charter.

[121] Klaus Kurasawe (n 56); Information and Privacy Commissioner of Ontario and The Future of Privacy Forum (n 56); Eoghan McKenna (n 55).

[122] Eoghan McKenna (n 55).

[123] WP205 (n 81) 16. European Data Protection Supervisor, 'on the Commission Recommendation on preparations for the roll-out of smart metering systems' (8 June 2012) <https://edps.europa.eu/sites/edp/files/publication/12-06-08_smart_metering_en.pdf > accessed 7 June 2018, para 52.

[124] WP 183 (n 100) 16-17.

privacy-friendly billing and recommended decentralised storage at the customers as the best measure to protect personal data.[125]

In fact, the choice between centralised and decentralised storage of consumption data is pivotal to the question 'who can get access to what type of data and in what form?' Choosing centralised storage of detailed consumption data exposes citizens to the risk of the further processing of data for a number of purposes; some of which are detrimental for competition; some of which are detrimental for incentivising people to produce electricity themselves; yet all of them are bad for privacy and personal freedom (see also section 5.2.2). [126] Providing the customer with such a means of control would be a good step towards a design that respects the right to privacy and data protection legislation (purpose limitation). Smart meters which process more personal data than necessary result in a disproportionate processing of personal data that goes beyond the scope of what is necessary to attain the goal of the smart grid and is in conflict with the ECHR, Charter and data protection legislation. In short, the Commission staff has failed to recognise the different policy options and the subsequent deliberations on the right choice.[127]

Determining the essential architectural choices of the smart meter is also necessary to engage in the final sub-test of proportionality, balancing the competing interests (proportionality *stricto sensu*). With the current design-choices the Commission allows the right to privacy to compete with energy efficiency. The smart grid can be, and in some Member States is already, realised on the neighbourhood level (see 5.2.2). On this level the right to privacy is not under threat. To assess whether the installation of smart meters can be justified the estimated difference in energy efficiency of a smart grid on the neighbourhood-level should be compared with the household-level, and this difference should be weighed against the interference with the right to private life, the respect for the home and the protection of personal data of all EU citizens. If the necessary functions for a fully functioning smart grid have grave consequences for privacy these could outweigh the benefits.[128]

[125] EU Commission Task Force for Smart Grids Expert Group 2 (n 89) 32, 33, 36.

[126] Ross Anderson explained it plain and simple:

'It is time for this debate to start. We have no objection to meters being able to support contracts with finer time granularity of pricing; but if I contract with an energy company to buy electricity for 4p per unit from midnight to 6 am, 24 p per unit from 4pm to 7pm, and 8p the rest of the time, then all my meter needs to tell the company is how many KWh I consume in each of these price bands in each billing period. It is not necessary for my meter to tell the power company, let alone the government, how much I used in every half-hour period last month.'

Ross Anderson, 'Consultation response on Smart Meters' (Foundation for Information Policy Research 2010) <http://www.fipr.org/100110smartmeters.pdf> accessed 5 June 2018 3.

[127] Later it will be argued why a correct application of the proportionality principle necessitates a choice for decentralised processing.

[128] This is notwithstanding the fact that all evidence points in the direction that the smart meter can be designed in a way to respect the right to privacy and function within the smart grid.

5. Privacy infringing functions and implementing acts

The wide range of potential functions of the smart meter and ways in which they may be executed raise many questions over technical details. Throughout the legislative process decisions on these matters were left to the Commission, which in turn gave a mandate to the ESOs in 2009 to develop standards for the smart meters. The underlying rationale is that the latter are better positioned to facilitate the evolution of technology in comparison with the EU legislature. Since the ratification of the Treaty of Lisbon in 2009, the relation between the Commission and the EU legislature in non-legislative acts is governed by Article 291 TFEU. As established in Chapter 4, the EU legislature needs to respect the specificity principle and the non-delegation doctrine. The Commission should respect the part of the non-delegation doctrine which concerns the reservation of the essential elements for the legislative act, moreover, it is not allowed to act outside of its competence. The EU legislature and the Commission should both respect the boundaries imposed by the Charter. This body of rules will be referred to as the constitutional requirements. As a result, the essential functions of the meter, i.e. the functions which are politically sensitive and/or limit fundamental rights, should be provided by the Directive and should be proportionate and necessary in relation to their goal. After the adoption of Directive 2012/27/EU, which amended Directive 2006/32/EC, the mandate that the Commission provided to the ESOs in 2009 did not change. In 2012, a report of the ESOs indicated that the mandate given by the Commission in pursuance to Directive 2006/32/EC was still used to issue standards.[129] Article 26 of Directive 2012/27 provides that the Commission will be assisted by a committee within the meaning of the Comitology Directive.

The Directive's gaps with regard to the design of the meter, the lack of specification of the functions and the manner of their execution, as well as the absence of substantial demands on the design regarding privacy, is, therefore, regarded as non-essential and consequently left to the Commission to decide on. This part of the design should be limited to functions neither of a highly politically conflictive nature, nor interfering with fundamental rights.[130] For the same reason, and in line with the doctrine of the effective protection of fundamental rights, decisions substantially increasing the risk of interference occurring downstream also should be outside of this mandate.

5.1 Essential elements of smart meter design

The decision as to what qualifies as 'essential elements' is not solely up to the Commission and Council; it also must have its basis in objective factors amenable to judicial review.[131]

[129] CEN-CENELEC-ETSI Smart Grid Coordination Group, 'First Set of Standards' (CEN CENELEC 2012) <ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/First%20Set%20of%20Standards.pdf> 107.

[130] See Chapter 4 section 4.1 for further elaboration.

[131] See Chapter 4, section 4.1. In 2011 Voermans wrote that what is essential is 'essentially a question to which there is only a political answer'. He considered the CJEU unlikely to render a substantive opinion on this

The two most controversial functions are the remote reading of the meter and the remote on/off control. These functions are beneficial to electricity providers, network operators and public authorities, but demonstrably at odds with the interests of citizens (see section 4.2). The process which led to the formulation of these functions was attended only by parties with specific economic interests. The Commission should have paid close attention to the relation between the interest of these companies — making profit for shareholders — and the interest of their clientele (which consists of the entire EU population) which is to be protected against the abuse of power of parties capable of imposing their will.

If the impact assessment had been executed properly and standards of proportionality and necessity as developed in ECtHR and CJEU case law would have been used as a standard, the significance of design choices would have been recognised before the drafting of Directive 2012/27/EU. The pivotal choice discussed earlier, between centralised and decentralised storage of detailed consumption data produced by the smart meter (illustrated in section 4.2), was never recognised by the EU legislator. The controversial political nature of this decision is indicated by the conflict highlighted earlier between industry and PET designers. Moreover, the choice for central storage of the meter data constitutes a severe interference with the right to private life and respect for the home. This opens the door for secondary uses of these data and consequently subjects private activities of citizens to state and commercial surveillance. The mandatory installation of smart meters has sparked civil disobedience and dissent in countries such as France, Britain, Spain, Belgium and the Netherlands, exactly because it is viewed as a socio-technical object that benefits industry, whilst increasing social control through the data it processes.[132] Since the centralised or decentralised storage constitutes an *essential element of smart meter design*, this choice belongs to the realm of the legislator. Based on the requirements to interfere with fundamental rights, this choice could have only been decided in favour of citizens, namely by opting for a decentralised storage on the meter which only communicates the total of the consumption data to the electricity provider.

By omitting to specify the limits of the Commission's power with respect to the essential elements of the smart meter design, the EU legislature has acted in contravention of the specificity principle and has failed to provide a foreseeable legal basis for the functions of the smart meter interfering with the fundamental rights to privacy and the protection of personal

---

subject. Although this was in line with previous case law, the CJEU changed its course in 2012 in case C-355/10 *Parliament v Council* ECLI:EU:C:2012:516, [2012].

[132] Stéphane Lhomme, 'Compteurs communicants: pourquoi il faut resister au diktat des politiques et industriels'(L'obs, 17 April 2016) < http://leplus.nouvelobs.com/contribution/1505932-compteurs-communicants-pourquoi-il-faut-resister-au-diktat-des-politiques-et-industriels.html > accessed 7 June 2018; Patrick Criqui and Stéphane La Branche, 'Compteur électrique Linky: comprendre la polémique' (The Conversation, 23 May 2016) <http://theconversation.com/compteur-electrique-linky-comprendre-la-polemique-59769> accessed 7 June 2018; Bart Tommelein, 'Overheid gaat fraude opsporen via onze energie- en waterfacturen', (MoneyTalk, 18 Februari 2016) <http://moneytalk.knack.be/geld-en-beurs/belastingen/overheid-gaat-fraude-opsporen-via-onze-energie-en-waterfacturen/article-normal-666995.html?utm_campaign=Echobox&utm_medium=social&utm_source=Facebook#link_time=1455789795> accessed 7 June 2018.

data. The recognition of the essential features of smart meter design is a key notion for the Commission to formulate a mandate limiting the discretion of ESOs and the (risk to abuse of) power that comes with it. Unfortunately, no such notion was recognised in advance of the Commission's instruction to the ESOs.

5.2 Instructing the ESOs

In 2009 the Commission offered a standardisation mandate to the ESOs, the purpose of which was to 'create European standards that will enable interoperability of utility meters (water, gas electricity, heat), which can then improve the means by which customers' awareness of actual consumption can be raised in order to allow timely adaptation to their demands (commonly referred to as "smart metering").'[133] This phrase contains an implicit referral to the function of smart meters within the smart grid, i.e. to communicate to customers peak demand times so that they reduce their consumption in order to save money by refraining from using electricity against higher prices. Although the Charter was not yet in force, the Commission communicated already in 2005 that it would use the latter to test the legality of its own actions: the DG of Industry and Enterprise seemed unaware of this new work ethic. According to the Commission, only the Directive 2004/22/EC on measuring instruments (hereinafter MID) provided restrictions: [134]

> 'It allows all functionalities that do not interfere with the metrological characteristics of the instrument. Most of these functionalities are not subject to any other limitations, i.e. MID allows any specification to be put into use.'[135]

The Commission ignores the relevance of the limitations following from the Charter and Article 291 TFEU for the smart meter functions. In the mandate, the Commission formulates a set of demands for the meter, which includes one of the functions that pose a risk to the right to privacy. The architecture should support secure bidirectional communication upstream and downstream, which can be seen as a demand that facilitates the remote reading of the meter, i.e. upstream communication. This is further elaborated on in the demand that standards should 'permit innovation in the protocols that enable remote reading of utility meters'.[136] Whether the data are computed on a central or decentralised level is left open. It contains no instructions about the remote on/off-control, yet this is a function that smart meters in Europe are equipped with on the basis of the 'Set of common functional requirements of the smart meter'. This highly invasive function is thus not required by law,

[133] Commission, 'Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability' (Enterprise and Industry Directorate-General , Consultation date: 21 January 2009) M/441 EN.
[134] Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments [2004] OJ L 135/1.
[135] Commission, 'Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability' (Enterprise and Industry Directorate-General, Consultation date: 21 January 2009) M/441 EN.
[136] ibid 3.

but is adopted in agreements which sideline the EU and national legislators. It goes against the case law of the ECtHR to view this interference as proportionate on grounds of protecting the economic wellbeing of the country: the Court allows a wide margin of appreciation if the right interfered only falls under the scope of Article 8 ECHR remotely.[137] Here the rights that are interfered with do fall explicitly within the scope of Article 8 ECHR.

The Commission does instruct the ESOs that 'deliverables should take into account applicable legal requirements concerning the confidentiality of personal data protected under Directive 95/46/EC and Directive 2002/58/EC'. What is notable is the Commission's choice of words on the applicable legal requirements which should be '*taken into account'*, instead of *being complied with.* The Commission focuses on the confidentiality of data which invokes restricting access to data, rather than limiting or minimising its collection. Moreover, it does not address whether the initial generation of data is necessary. Generally, no specification, or explanation is given on substantive norms adopted in this legislation. Consequently, their interpretation is left to the ESOs which mainly serve corporate interests, as noted above. The Commission leaves plenty of room for the ESOs to disregard the substantive demands that follow from data protection legislation, resulting in the freedom to drill for intimate data. The substantial protection that could follow from a strict interpretation of these norms is undermined, due to the constituency of the ESOs which favours a loose interpretation. Furthermore, the ESOs do not have to comply with the Charter as they operate outside of the accountability mechanisms which intend to curb the power of EU institutions.

In its 2011 Communication on smart grids, the Commission stated that a PbD-approach would be integrated in the standards developed by the ESOs.[138] In a 2012 report the ESOs indicated, however, that they still based their new standards for the smart meter on a mandate from 2009.[139] There is no indication whatsoever that this PbD-approach had a substantive impact on the design of smart meters. The earlier findings on industry's approach to PbD (section 5.4.2) also hint towards the use of PbD-language as window-dressing. All of the above underlines the previous observations in that the Commission contributes to the misunderstanding of data protection as data security. In this lax instruction it excluded the right to private life and the home and failed to address essential features of the smart meters design. By omitting to formulate concrete restrictions on the development of these functions, the Commission indirectly delegated discretionary power to the ESOs on the development of privacy-infringing functions, arguably in contravention of the non-delegation doctrine.

[137] *Hatton and others v The United Kingdom* App no 36022/97 (ECHR, 8 July 2003) para 96.

[138] Commission, 'Smart Grids: from innovation to deployment' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2011) 202 final 2.

[139] 'First Set of Standards' (n 129) 100, 107.

5.3 The approach to privacy in the Smart Meters-Coordination Group

With the lax instruction of the Commission the approach to privacy by the ESOs becomes all the more relevant. The Smart Meters Coordination Group (SM-CG) was formed in a concerted response by the ESOs to Mandate M/441. The aim of this joint advisory body is to combine the expertise and resources to focus on smart metering standardisation issues.[140] In the aftermath of the mandate this group produced two reports: the first will be referred to as the Technical Report and the second as the Summary Report.[141]

The Technical Report focuses on the architecture of the meter. It also dedicates a chapter to privacy and data security. The report acknowledges the relation between the purpose, design, functionalities and implementation of the metering system and its compliance to EU privacy and data protection legislation.[142] It states the importance of implementing privacy-requirements into the design, and also mentions that privacy-enhancing technologies should be considered. Standardisation is accorded the role to protect privacy in order to support the smart meter deployment. Yet, there are clear indications that privacy is not understood as non-interference or minimal interference or control of a meter holder over data produced by the meter. The chapter opens with the following sentence: 'For public acceptance of smart metering, suitable privacy and data protection safeguards need to be in place so that consumers can be confident that their data is treated securely and their privacy is not infringed.'[143] This exposes the biased approach resulting in the conflation of privacy and data security.

The Summary Report preserves this conflation. There was a 'private circulation' of this report which could be found through the use of a search engine. One of the headers in this report read 'Security issues'.[144] In the final version, this was changed into 'Security and privacy issues', yet no text was added about privacy.[145] This section also mentions the report on privacy and security produced by the SM-CG.[146] This report is highly technical and is concerned with questions of security and along that line privacy. This, too, does not address

[140] 'Smart metering' (Online index, CEN and CENELEC) <http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartMeters/Pages/default.aspx> accessed 5 June 2018.

[141] The full names of these reports are respectively: CEN, CENELEC and ETSI, 'Functional reference architecture for communications in smart metering systems' (CEN/CLC/ETSI/TR 50572:2011); CEN, CENELEC and ETSI/Smart Meters Coordination Group, 'Introduction and Guide to the work undertaken under the M/441 mandate' (A report by the CEN-CENELEC-ETSI Smart Meters Coordination Group).

[142] Functional reference architecture for communications in smart metering systems (n141) 14.

[143] ibid.

[144] CEN, CENELEC and ETSI/Smart Meters Coordination Group, 'Introduction and Guide to the work undertaken under the M/441 mandate' (SM-CG report at end 2012 – Final draft, Private circulation PEL/13_12_0105) 7.

[145] ibid 9.

[146] CEN, CENELEC and ETSI/Smart Meters Coordination Group, 'Task Force Privacy and Security of the Smart Meters Coordination Group, 'Privacy and Security approach – part I' (Version 1.02, CEN-CENELEC-ETSI 2013) <ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/Management/SmartMeters/SMCG_Security_and_Privacy_Report_PartI.pdf > accessed 5 June 2018.

privacy as a right, but instead discusses it as a matter of confidentiality of data handling. This shows that the ESOs make the same mistake as the Commission by conflating two separate concepts of data security and privacy. The ESOs, thus, do not even commence a genuine exploration of the existing lighter alternatives, which could safeguard privacy.

In conclusion, decisions impacting the right to privacy as enshrined in the Charter and the ECHR and the requirements that need to be met to justify interferences with it are not only wrongfully delegated to the ESOs, but also are not given any consideration by them. Although unsurprising, it is problematic that the mandate the ESOs receive directly from the Commission and indirectly from the EU legislature does not impose any substantive demands on them. The reality is that due the role played by the ESOs in EU law, smart meters which comply with standards carry the presumption of conformity with the mandatory basic legal requirements and can circulate freely on the EU's internal market.

6. Conclusion

The rules which govern the design of smart meters are embedded in a complex (quasi-) legislative landscape demonstrably favourable towards narrow sectoral-bound industry and government interests. In this dossier, the Commission's actions run counter to its fundamental rights ambitions. It paid lip-service to its role as *guardian of fundamental rights*, but in practice heavily neglected this role in pursuing its policy. It established privacy-infringing functions without involving the EU legislature. It left the execution of these functions to the ESOs in a mandate with only a general reference to data protection legislation. In the legislative process towards the introduction of these systems, it did not mention a single word on fundamental rights. In combination, this led to the serious undermining of the protection of the right to respect for private life and the home. The choices made were not explained nor accounted for in either the relevant legislation or the preparatory process.

The smart grid is one of the biggest public-private projects of our time, which embodies opposing interests, yet is governed and driven by parties with a homogenous constituency. The design of the smart meter and the way its functions are executed within this architecture is a politically sensitive matter, which, nonetheless, does not receive due attention. It could even be depicted as a battlefield between industry and government interests on the one side and citizens' fundamental rights on the other. The fact that this politically supercharged process took place outside of the democratic arena is a textbook example of common observations in EU law that the democratic process in the EU is hijacked by elitist decision-making.[147]

On the level of Member States, exceptions aside, the peculiar situation is created in which they have the duty to pursue the rollout of smart meters, without having control over the design, whilst ensuring 'the privacy of final customers, in compliance with the relevant

[147] Paul Craig and Gráinne de Búrca, *EU Law: text, cases and materials* (5th edition, Oxford University Press 2011) 137.

Union data protection and privacy legislation'.[148] This raises the question whether Member States can ensure compliance with legislation and observe the respect of the fundamental rights of privacy and data protection, without exercising influence over the design of the meters which is essential for their impact on the aforementioned rights. A positive answer would wrongfully assume that these rights can be effectively safeguarded by nothing more than law. The EU legislature and the Commission have a duty to address the features of smart meter design which (risk) impact on the right to privacy.

Of course, one should not mistake ideals for reality and law in the books will never be the same as the law in practice. In the policy and rulemaking on smart meters, however, the law in the books is absent in practice. The plaster used to restore this fundamental breach of the right to privacy is the application of a deformed, watered down version of data protection legislation. The lack of any substantial results on privacy in the design of the meter, other than data security, reveals the inadequacy of leaving the interpretation of substantive legal norms to the parties benefitting from the processed data. This *data protection light*, however, does resonate with the approach to privacy the Commission advances through its communications.

Citizens are forced to accept through legislation the installation of smart meters with functions serving the interest of business and government, subjecting the private sphere to corporate motives. From the perspective of fundamental rights, the process concerning privacy, data protection and the design of the smart meter can be considered an historical error on literally continental scale. The nature of the interference enabled through the smart meter strikes at the heart of personal freedom and permanently breaches the right to respect for the home that is fundamental to people's personal security and well-being. The smart meter in its current form, therefore, is not only disproportionate, unnecessary and illegal – it is irreconcilable with the essence of the right to respect for private life and the home.

[148] Art 9 2 (b) Directive 2012/27/EU.

Chapter VI
Regulatory framework of eCall: case study II

1. Introduction

The Intelligent Transport Systems (ITS) agenda of the Commission is nothing less than the coordinated colonisation of the existing road transport infrastructure and the vehicles by information and communication technology.[1] Cars that communicate are usually associated with navigation systems or sci-fi on-board Artificial Intelligence, such as K.I.T.T. in the TV series *Knight Rider*. A future, in which our cars start communicating autonomously, might sound promising, but it also raises a number of questions, including what information will be communicated, to which parties and how much control motorists would have over this. Will motorists be able to choose the data their cars are transmitting or will ITS turn their car against them: 'Good morning, Michael! The tax service has just been informed that you have driven more kilometres than submitted on your tax form.… Oh, and, please, be aware that the police has sent a fine to your eGovernment portal for speeding yesterday.'

In the 2009 Internet of Things action plan reference is made to the 2008 ITS action plan.[2] The latter plan covers a number of areas in which the uptake of ICT is estimated to have a positive effect on the mobility and safety of EU road users through the coordinated deployment of ITS. These technologies should be installed in the road infrastructure as well as vehicles, allowing an integration of cars and the digitised highway. On the 7th of July 2010, Directive 2010/40/EU for ITS[3] (hereinafter the 'ITS Directive') was adopted. This Directive sets out four priority areas and six priority actions. One of the priority areas is ITS road safety and security applications, which is linked in the annex to the eCall system. One of the priority actions is the 'harmonised provision for an interoperable EU-wide eCall'.

On the 29th of April 2015, Regulation 2015/758 was adopted (hereinafter the 'eCall Regulation').[4] The objective of this Regulation is to increase road safety through the mandatory installation of the so-called eCall in-vehicle system (the 112-based eCall in-

[1] Borrowing the beautiful metaphor of Adam Greenfield: 'The project of everyware is nothing less than the colonization of everyday life by information technology'. Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (1st edition, Pearson Education 2006).

[2] Commission, 'Internet of Things – An action plan for Europe' (Communication from the Commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions) COM (2009) 278 final.

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

[4] Regulation (EU) 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 [2015] OJ L 123/77.

vehicle system, hereinafter the '112 system'). From the 31st of March 2018 every car certified for the European market is equipped with eCall. Before this date, certain car manufacturers already installed a proprietary eCall-system (hereinafter 'TPS eCall'). The function of the 112 system is to automatically dial emergency-services when a car is in a serious accident and to communicate a minimum set of data (MSD), including the exact location of the car, the direction it was driving and the unique Vehicle Identification Number (VIN). After this data has been transmitted an audio channel is opened between the Public Safety Answering Point (PSAP) where the call is received and the system within the car. A number of benefits are expected from the introduction of this system. The time saved by automatically dialling emergency services should result in fewer fatalities, a reduction in the severity of injuries and a decrease in the congestion caused by the accident (recital 7).[5] Particularly in rural areas, with a significant chance of no witnesses to an accident, this service can make the difference between life and death. In sum, the in-vehicle system is expected to bring major benefits to road safety.

The 112 system integrates four categories of technology. First, sensors register when the car is in a severe crash, e.g. the ones that activate the airbag. Second, Galileo and the European Geostationary Navigation Overlay Service (EGNOS, a regional satellite navigation system) provide satellite receivers compatible with positioning services. These receivers track the last three positions of the car.[6] Third, a GSM modem transmits the satellite data and establishes the audio channel between the PSAP and the car. Fourth, the microphone and loudspeaker enable communication with the PSAP.

The same system is expected to bring benefits for the relevant industry because it offers a platform for the provision of added value services, e.g. insurances and the tracking of stolen cars.[7] The Regulation explicitly introduces these added value services building on the eCall in-vehicle system.[8] Stakeholders, such as car manufacturers and independent operators, are allowed to utilise the GSM and satellite technology of eCall in order to provide these services.[9] This implies that the future cars for the European market are equipped with sensors and these can be used to collect data, communicate both ways and thus create value. Car data monetisation is said to depend on three enablers: 'in-car technologies, infrastructural

[5] The estimation is the prevention of 2 500 (6.4% of 39 000) traffic deaths per year, mitigate the consequences of severe accidents in 5850 cases (15% of 39 000), see European Commission, 'Emergency calls: Commission welcomes growing Member State endorsement for eCall in-car system' (IP/ 10/488 Press Release, Brussels, 4 May 2010) <http://europa.eu/rapid/press-release_IP-10-488_en.htm> accessed 7 August 2015.

[6] Recital 10 and Article 5 (4) eCall Regulation.

[7] See European Commission, 'eCall: automated emergency call for road accidents mandatory in cars from 2015' (IP/13/534 Press Release, Brussels, 13 June 2013) <http://europa.eu/rapid/press-release_IP-13-534_en.htm> accessed 5 June 2015.

[8] 'eCall' refers to both services. They both run on the same device.

[9] There are indications in the Regulation that this is so, e.g. Recital 15, Article 3(10), and was also confirmed by a senior manager of ERTICO ITS Europe (Europe's Intelligent Transportation System organization that promotes research and defines standards).

technologies, and back-end processes'.[10] Regulation 2015/758/EU establishes the mandatory installation of the first of these enablers.

Notwithstanding the benefits, the eCall system undermines the right to privacy and the protection of personal data (Article 7 and 8 of the Charter) and might conflict with the GDPR. Equipping every car with an individual system allows mass surveillance of car movements on the level of a single car. Moreover, this system allows the targeting of vehicles and using the system against the citizen in a number of ways. Some of the challenges to fundamental rights follow from eCall's design which introduces the risk that eCall will be used to perform functions and serve purposes it was not originally intended for (*purpose and function creep)*.[11] When the collection of personal data brings value to other parties against the data subject's will the challenge to the right to privacy is evident. This chapter analyses, within the broader ITS framework, the Commission's groundwork leading to the mandatory introduction of eCall. It discusses the relevant impact assessments with an emphasis on the right to privacy to identify the challenges introduced by the eCall system. The chapter makes an inventory of the way privacy and data protection are addressed in the eCall legislation. Finally, it analyses the powers conferred to the Commission in this legislation against the constitutional limits provided in the Treaties and the Charter.[12]

2. Groundwork by the Commission: making eCall mandatory

Prior to the adoption of the ITS Directive and Regulation 2015/758/EU the Commission prepared the ground thoroughly for the compulsory introduction of the eCall system. It performed its role of policy entrepreneur through a range of activities, such as funding important platforms (eSafety Forum), financing studies to estimate 'the socio-economic benefits' of eCall, organising 'high-level meetings' with Member States and industry, bringing these parties together in the eCall Driving Group, setting agendas (amongst others through communications), proposing legislation and adopting quasi-legislation (delegated acts).

2.1 Communications framework

The Commission issued four communications and an action plan before it adopted the ITS Directive in 2010. In its 2003 Communication on *Information and Communications Technologies for Safe and Intelligent Vehicles*, it established the relation between car safety and services for the automotive market. Although the Commission claims that 'this Communication deals only with the application of these technologies for road safety', this

[10] McKinsey & Company, 'Monetizing car data: New service business opportunities to create new customer benefits' (Advanced Industries September Report, McKinsey & Company 2016) 32.

[11] Tijmen HA Wisman, 'Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things' (2013) 4(2) EJLT < http://ejlt.org/article/view/192/379> accessed 5 June 2018.

[12] 'eCall legislation' refers to the ITS Directive and the eCall Regulation.

'safety' is firmly placed in the key of economic growth. ITS are mentioned a few times and linked to Intelligent Infrastructure and co-operative systems. The coordinated integration of the automotive market with mobile communications and ICT is the Commission's goal:

> 'As the car parc of vehicles with telematics grows, the market will shift towards services, further integrating the automotive market with two other key industrial sectors in Europe: Mobile Communications and Information Technology.'[13]

The markets identified are 'safety and security', 'vehicle oriented telematics', 'navigation and routing', 'fleet management and infotainment'. The key ICT technologies identified are 'mobile telecommunications, location/positioning technologies, intelligent sensors, actuators and interfaces, automotive-grade high-performance in-vehicle communications networks', enough to turn a rust bucket into an intelligent vehicle cruising the digital highway in an Internet of Things vision.[14] Despite the Commission's praise for these technologies it claims that leaving the introduction of these technologies to the market would probably take a very long time, admitting that the introduction of all these technologies will lead to an increase in complexity and thus maintenance and repair costs of vehicles.[15] The Commission introduces the idea that the 'public and private sectors must agree to co-operate' and 'full support of the public sector' should contribute 'to a positive public/private business case'.[16]

The Commission then sums up certain mechanisms for public sector intervention, such as promoting standardisation and introducing financial incentives, before it reveals statutory force as its ultimate remedy: '[t]he vehicle type approval legislation should be adapted, when necessary, to permit these systems, or even mandate them, if appropriate.'[17]

This communication form 2003 shows an interesting and incoherent chronology. First, the importance of car safety systems is brought to the fore following a discussion of a whole body of technologies for a great variety of purposes other than safety. Then, these technologies serving diverse purposes are lumped together under the term 'Intelligent Vehicle Safety Systems' and brought under the heading '**A prerequisite: a positive business case**'. Under this heading, market mechanisms are considered unreliable and the option to make these Intelligent Vehicle Safety Systems mandatory through law is advanced.[18] The lack of a positive business case did not halt the Commission's ambitions.

---

[13] Commission, 'Information and Communications Technologies for Safe and Intelligent Vehicles' (Communication from the Commission to the Council and the European Parliament) COM (2003) 542 final 5.

[14] ibid 7.

[15] Something which is missing in the studies to economic benefit-analysis studies I found, which might be explained by the one-dimensional focus on benefits.

[16] COM (2003) 542 (n13) 13. The parties to cooperate are 'the automobile manufacturers, equipment suppliers, motorway operators, telecommunication operators, service providers, automotive after-sales players, insurance industry, road safety and user organisations, road authorities, emergency service providers, Member States and the European Commission.

[17] ibid.

[18] ibid.

In the next communication from 2005 it becomes clear that the Commission is leveraging the political will to reduce traffic fatalities to advance the broader oriented pan-European eCall. It refers to eCall as 'the first building block of the Intelligent Car initiative', which reveals the Commission envisions the use of eCall for a plethora of purposes exceeding the limits of emergency situations.[19] This Intelligent Car Initiative was presented by the Commission '**as a policy framework for actions in this area**', deemed 'important to maintain European industry competitiveness' and perpetuates the link between safety and commercial services. [20] In the second eSafety communication, the Commission pressed the Member States to upgrade their PSAPs to handle location-enhanced eCalls and provide adequate location-enhanced emergency services and language support. It also announced that the 'eSafety partners' (European Commission, industry, public authorities and other stakeholders) established a road map, the most important milestone of which was the introduction of 'eCall as standard equipment in all vehicles entering the market after September 2009'.[21] In the conclusion the Commission repeats the urge for action by the Member States with a final note that it will 'consider further measures' if the roll-out of eCall fails to progress in lock step with the proposed road map.[22]

In the third communication from 2006 the Commission also addressed the European, Japanese and Korean associations of car manufacturers (ACEA, JAMA and KAMA respectively). The Commission announced it would start negotiations with these associations in 2007 and modestly proposed that 'automotive industry should work together with the Commission in defining the terms of the voluntary agreement'; that is the 'voluntary agreement of introducing an eCall in-vehicle device'.[23] In an attempt to make an offer industry could not refuse, the Commission reiterated its determination to 'propose further measures' if the automotive industry failed to conclude this 'voluntary' agreement.[24]

Besides the threat of statutory force the Commission brought together stakeholders, first through the eSafety Forum and later by setting up a 'High Level Group', established in Directive 2010/40 as the 'European ITS Advisory Group'. The Commission introduced this idea in the impact assessment of the Directive, calling for an effective cooperation between

[19] Commission, 'The 2nd eSafety Communication: Bringing eCall to Citizens' (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions) COM (2005) 431 final 2.

[20] Commission, 'On the Intelligent Car Initiative "Raising Awareness of ICT for Smarter, Safer and Cleaner Vehicles"' (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions), COM (2006) 59 final 1, 5. Bold in original text.

[21] COM (2005) 431 (n 19).

[22] This can be viewed as an implicit referral to the option of statutory force.

[23] Commission, 'Bringing eCall back on track – Action Plan (3rd eSafety Communication)' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2006) 723 final 8, 9.

[24] ibid 9.

public and private stakeholders 'with synchronised investments'.[25] It noted that industry struggled 'with a non-obvious business case and reluctant consumers' and the public sector was 'not (or not sufficiently) aware of the potential of ITS to help achieve policy objectives'.[26] The ITS Advisory Group was needed to 'provide a clear vision of the future of European transport policy and the role of ITS in this'.[27] The Commission already undertook an effort to form such a group in 2001 through a recommendation, but this group failed to agree on clear actions. The reliance on a voluntary group was considered, therefore, to be a risk.

In 2008 the Commission launched the 'Action Plan for the Deployment of Intelligent Transport Systems in Europe'.[28] Here, eCall is positioned within the broader framework of ITS and set policy goals for establishing a legal framework for ITS deployment in addition to funding and other soft measures. The 'open in-vehicle platform' is presented as the way to integrate the vehicle in the transport infrastructure, which together form the 'open system architecture'.[29] In this action plan, certain benefits of ITS are summarised as follows: greening of transport through toll collections and dynamic in-vehicle navigation, improving transport efficiency amongst others through 'Real-time Traffic and Travel Information' (RTTI) services, improving road safety and security through eCall and other systems. The Commission takes the position that the 'potential of ITS can only be realised if its deployment in Europe is transformed from the limited and fragmented implementation that is observed today into an EU-wide one'; therefore 'the removal of existing barriers to ITS deployment will be pivotal'.[30] These words resonate with the IoT vision of the Commission in the 2009 Action Plan on the IoT, where it takes on the responsibility to transform policy areas through the adoption of ICT. It also indicates a number of 'priority areas for action', including data security and protection (in that order). The Commission limits itself to data security, addressing 'data integrity, confidentiality and availability' and leaving out explicit consideration on substantive requirements, such as the necessity of the collection of data in the first place.[31] Data protection is identified as an issue that can turn out to be a 'major barrier to wide market penetration of some ITS services if citizens' rights are not shown to be

[25] Commission, 'Impact Assessment accompanying the Communication from the Commission Action plan for the deployment of Intelligent Transport Systems in Europe and the Proposal for a Directive of the European Parliament and of the Council lying down the Framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes' (Commission Staff Working Document) SEC (2008) 3083, 47.
[26] ibid.
[27] ibid.
[28] Commission, 'Action Plan for the Deployment of Intelligent Transport Systems in Europe' (Action plan) COM (2008) 886 final.
[29] ibid 2, 11.
[30] ibid 2, 5.
[31] ibid 2, 12.

fully protected'.[32] This concern is rooted in market considerations, rather than in the protection of fundamental rights.[33]

In its 2009 Communication, the Commission builds up the pressure by noting in the introduction that it will consider a number of options, one of which entails setting up a regulatory framework.[34] It reports on the progress on the commitment of different stakeholders and notices in bold that:

> **'The automotive manufacturers also took the position that making eCall standard factory-equipped equipment in all vehicles would be possible only through regulation** …. The automotive industry is also interested in using the eCall platform to offer **added-value services** to boost their business.'[35]

The first sentence demonstrates that reaching a voluntary agreement with automotive industry failed. Apparently, not all manufacturers were willing to make eCall standard equipment. According to the second sentence, automotive manufacturers expressly indicated an interest to use eCall for their own profit if eCall became mandatory. The technical components could also be used as the basis for in-vehicle applications 'required by existing or planned regulation applicable to commercial or private vehicles, such as the digital tachograph, electronic toll collection or provisions on the transport of dangerous goods and live animals'.[36] The alignment and integration of

> 'these applications within a coherent, open-system architecture could yield better efficiency and usability, reduced costs and enhanced extensibility (…) 'that address road safety, personal mobility, logistics support or access to multimodal information. The definition of an "open in-vehicle platform" concept is part of the ITS Action Plan and the introduction of eCall based on this concept would positively contribute to its momentum.'[37]

This sheds light on the Commission's envisioned shift from the initial purpose of eCall as a public technology saving lives to a private technology making profit, or more euphemistically enabling 'the wider deployment of ITS'.[38] It raises the question how these newly introduced purposes affect considerations on the design of eCall. Do these envisioned purposes necessitate a more privacy-intrusive design and if so, how does this relate to the possibility of making the eCall system mandatory? The Commission does not address these questions. Instead, it simply turns to the argument in favour of making the installation of eCall mandatory. Under the heading 'Recommendations', the Commission introduces three policy

[32] ibid.
[33] There is an interesting parallel between this worry and the concerns of the OESO in the seventies about privacy becoming an obstacle to the free flow of data.
[34] Commission, 'eCall: Time for Deployment' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2009) 434 final 3.
[35] ibid 6.
[36] ibid 7.
[37] ibid.
[38] COM (2003) 542 (n13) 13.

options. The way these options are formulated leaves little doubt about the Commission's preference. The first option is non-interference: the Commission argues that this will bring complexity in the relation between emergency response services and TPS eCall. The saving of lives is at stake, and therefore 'this option is unacceptable' for the Commission.[39] The second option is the voluntary approach, which 'would lead to the introduction of the eCall service in Europe, but too slowly'.[40] In addition, this would lead to missing the benefits of economies of scale, increasing the price and reducing demand. This is also presented as an option which is not viable. The final option is the regulatory approach, which implies 'making eCall standard equipment in all new vehicles in Europe' to 'unlock the full potential of eCall to save lives and mitigate the severity of injuries' and to 'at the same time stimulat[e] the telematics service market in Europe'.[41] In short, the Commission only presents one viable option which is mandating eCall:[42]

> '**The final aim is to fully roll out the pan-European eCall service and make it standard equipment in all new type-approved vehicles in Europe. The Commission will monitor the effectiveness of the voluntary approach described above. If significant progress is not made by the end of 2009, both in the availability of the eCall device in vehicles, and the necessary investment in the PSAP infrastructure, the Commission will plan to take the following regulatory measures in 2010'.[43]**

It should be noted that the deadline was set at the end of 2009, rather unrealistic keeping in mind that this Communication was adopted on the 21st of August 2009.

It is particularly interesting how the Commission, after considering legislative intervention, arrives at a conclusion that '[c]itizens recognise [eCall's] value and want an affordable eCall with their next vehicle.'[44] These are the same citizens who were indicated only a year earlier as 'reluctant consumers' in the Commission's action plan, who will be forced to 'welcome' a deeply intrusive device in their car for which they have to pay and which offers industry a 'platform to offer added value services to boost their business'.[45] This patronising approach rings reminiscent of the way colonisers forced religion on native people who had to be taught that they wanted to be civilised.[46] Now this approach is used on Europe's natives to get them ready for the civilised perspective of driving a car equipped with a system serving a corporate agenda.

---

[39] COM (2009) 434 (n 34) 9.
[40] ibid 9.
[41] ibid.
[42] The option it already expressly considered in its 2003 Communication, COM (2003) 542 (n13).
[43] COM (2009) 434 (n 34) 10.
[44] ibid 10.
[45] ibid 6. This is similar to what Adam Greenfield refers to in his book 'Everyware', in which he describes an interview with a Motorola executive for the Economist, where the executive 'asserted the rather patronizing viewpoint that if customers didn't want these conveniences, they'd simply have to be "educated" about their desirability until they did manage to work up the appropriate level of enthusiasm. In other words, "the floggings will continue until moral improves."' Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (1st edition, Pearson Education 2006) 92.
[46] Noam Chomsky, *Profit over People: Neoliberalism and Global Order* (1st edition, Seven Stories Press 1999).

2.2 Legislative framework

The ITS Directive was adopted under Article 91 TFEU on the common transport policy. It establishes priority areas, priority actions, and confers to the Commission the power to adopt delegated acts with respect to specifications necessary to ensure compatibility, interoperability and continuity (technical aspects) for the deployment and operational use of ITS with respect to the priority actions. It further instructs the Commission to request the ESOs to develop the standards on these technical aspects, after consulting the European ITS Committee (EIC) which consists of representatives of Member States (advisory procedure of comitology). It instructs the Commission to establish a European ITS Advisory Group 'to advise on business and technical aspect of the deployment and use of the ITS in the Union' which will be composed of all the other relevant stakeholders. In order to enable the Commission to monitor the progress made at national level, the Member States are obliged to report to the Commission on the progress made on the various priority actions.

Cascading from the ITS Directive are five delegated regulations linked to five out of six priority actions.[47] In the initial proposal Member States were required to 'take necessary measures to integrate safety and security-related ITS systems into vehicles and road infrastructure'. [48] In its opinion on Directive 2010/40/EU, the EDPS noted that the Commission did not 'define what "safety and security-related ITS systems" and it should therefore be further clarified what the specific ITS applications and systems are which must be embedded in vehicles'.[49] In the final version of Directive 2010/40/EU, 'safety and security-related ITS systems' was removed, but 'the harmonised provision for an interoperable EU-wide eCall' was introduced as a priority action, similarly without a definition of this system.[50] This is the only time eCall is mentioned in the main text of the Directive.[51] These delegated regulations cover a variety of matters in which data transmitted

[47] Eg the Commission Delegated Regulation (EU) 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an interoperable EU-wide eCall [2013] OJ L 91/1 provided the specifications for the Decision 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall Service [2014] OJ L 164/6. The Commission did not follow up on the sixth regarding 'the provision of reservation services for safe and secure parking places for trucks and commercial vehicles'. After consultations with Member States experts it appeared that the parking areas which could offer reservation services in 2014 was only 2%.

[48] Commission, 'Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes' COM (2008) 887 final.

[49] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes' (OJ 2010 C 47/02) para 17.

[50] Article 3(d) Directive 2010/40/EU.

[51] The other time is in Annex I, priority area III.

by cars could play a vital role, such as EU-wide real-time traffic information services' and call into question how these relate to the functioning of eCall.

In 2011, the Commission adopted the Commission Recommendation on support for an EU-wide eCall service in electronic communication networks for the transmission of in-vehicle emergency calls based on 112.[52] This Recommendation establishes that the 'harmonised EU-wide interoperable eCall service requires that the voice-audio call, along with the minimum set of data generated by the in-vehicle system on the incident, is transmitted automatically to any appropriate public safety answering point that can receive and use the location data provided' and that the arrangements between mobile network operators and PSAPs are 'established in a transparent and non-discriminatory' manner.[53] Member States need to establish the detailed rules for the public mobile network operators in their countries on handling eCalls and these rules should comply with Directives 95/46/EC and 2002/58/EC.[54]

Regulation 2015/758/EU which mandates the installation of eCall was not adopted under the common transport policy, but under Article 114 TFEU, which is a residual provision that sees to the establishment and functioning of the internal market.[55] The difference in the legal basis can be explained by the fact that this Regulation is an amendment of Directive 2007/46/EC which established a comprehensive Union type-approval system for motor vehicles.[56] The Regulation is aimed at increasing road safety through the mandatory installation of the '112-based eCall in-vehicle system' in every car certified for the European market from the 31st of March 2018 onwards.[57]

The eCall Regulation coins a great number of terms. With respect to services, the Regulation uses terms such as 'eCall service' (Recital 3), 'the public interoperable Union-wide eCall service' (Recital 13), 'TPS eCall service' (Recital 13, Article 6 (11)), 'public 112-based eCall service' (Recital 13 mentioned three times), '112-based eCall service' (Recital 14), '112 service' (recital 5 and 6), pan-European eCall service (Recital 26). All of these terms for services do not reoccur in the definitions provided in Article 3. This Article only provides a definition for 'third party services supported eCall' or 'TPS eCall', which is an emergency call to a third party service provider; and 'third party service provider' which is an organisation officially allowed to receive the TPS eCall. With respect to systems the

[52] Commission Recommendation 2011/750/EU on support for an EU-wide eCall service in electronic communication networks for the transmission of in-vehicle emergency calls based on 112 ('eCalls') [2011] OJ L 303/46.

[53] Recital 6 and 7 Recommendation 2011/750/EU.

[54] Article 3 Recommendation 2011/750/EU.

[55] For more background to this provision I refer to Paul Craig and Gráinne de Búrca, *EU Law: text, cases and materials* (5th edition, Oxford University Press 2011) 590.

[56] Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (hereinafter 'Framework Directive') [2007] OJ L 263/1.

[57] Article 5 eCall Regulation establishes the obligation for manufactures to build in a '112-based eCall in-vehicle system, components and separate technical units designed and constructed for such vehicles….approved in accordance with this Regulation and the delegated and implementing acts adopted pursuant to this Regulation'.

Regulation uses terms such as 'comprehensive Union-type approval system ('Recital 1'), 'Union eCall System' (Recital 7), 'third party service supported eCall systems' (Recital 13), 'TPS eCall system' (Recital 14, 24, Article 6(10)), 'the system providing private or added-value services' (Recital 15), 'free public eCall system' (Recital 24). All of these terms for systems do not reoccur in the definitions provided in Article 3. This Article only provides a definition for '112-based eCall in-vehicle system' and 'third party services eCall in-vehicle system'. In conclusion, the terminology of the Regulation creates much confusion and fails to provide clarity with respect to the matter it governs.

The lack of clarity with respect to the system mandated by Regulation 2015/758

The Regulation focuses on safety, seen in the inclusion of 'the 112 service' in its title, however, the scope is extended to 'added value services'.[58] According to Recital 15:

> 'The mandatory equipping of vehicles with the 112-based eCall in-vehicle system should be without prejudice to the right of all stakeholders such as car manufacturers and independent operators to offer additional emergency and/or added value services, in parallel with or building on the 112-based eCall in-vehicle system. (…) Where provided, those services should comply with the applicable safety, security and data protection legislation and should always remain optional for consumers.'

The first sentence provides that added value services can be 'build on' the 112 system, meaning that it can be used to offer added value services. [59] This means that the eCall system is mandated for the purpose of saving lives, but can be used as a platform to offer commercial services. Recital 15 does establish that these services should comply with data protection legislation and 'always remain optional for consumers', however, there seems to be an interesting bent to this formulation which will be discussed further in section 3.2 (subsection C-ITS). The EDPS responded to this proposal by stating that services utilising the eCall system 'create considerable additional risks for privacy, comparable with those of mobile apps on smart phones'.[60]

Recital 16 continues this commercial turn and even broadens the perspective:

> '(…) the eCall in-vehicle systems should be based on an interoperable, standardised, secure and open-access platform for possible future in-vehicle applications or services. As this requires technical and legal back-up, the Commission should assess without delay, on the basis of consultations with all stakeholders involved, including vehicle manufacturers and independent operators, all options for promoting and ensuring such an open-access platform and, if appropriate, put forward a legislative initiative to that effect. (...)'

[58] Recital 15 Regulation 2015/758/EU.
[59] COM (2009) 434 (n 34) 6.
[60] European Data Protection Supervisor, '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/EC' (EDPS) 29 October 2013, 4.

In order to save lives, vehicles are equipped mandatorily with the 112-based in-vehicle system based on an 'open-access platform', which can be used to provide 'for possible future in-vehicle applications or services'. The text of the Regulation appears to suggest there is a difference between the 112-based in-vehicle system and the open-access platform. The definition of an 'open-access platform' is, nonetheless, missing. This term reoccurs only once in Article 12(2), whereby the Commission will assess the need of requirements for an interoperable, standardised and secure platform after a broad consultation with all relevant stakeholders and a study assessing the costs and benefits.[61]

This part of the Regulation overlaps with a report of the Platform for the Deployment of Cooperative Intelligent Transport Systems in the EU (hereinafter C-ITS Platform),[62] launched by the Commission in July 2014.[63] C-ITS reflects the idea of autonomous communication from vehicles to vehicles (V2V), vehicles to infrastructure (V2I) and infrastructure to infrastructure (I2I). In this report, the open-access platform is linked to priority area IV of the ITS Directive.[64] The mandatory system which is justified for emergency purposes is perceived as the seed for C-ITS, also popularly referred to as 'eCall on steroids'.

The '112-based eCall in-vehicle system' is defined as an emergency system, comprising in-vehicle equipment and the means to trigger, manage and enact an eCall.[65] 'eCall' is defined as 'an in-vehicle emergency call to 112'.[66] This definition does not cover added value services. It also provides a definition for 'in-vehicle equipment' meaning 'equipment permanently installed within the vehicle that provides or has access to the in-vehicle data required to perform the eCall transaction via a public mobile wireless communication network'.[67] The relation between the open-access platform, the 112-based in-vehicle system and the in-vehicle equipment is not clarified. The text of the Regulation also remains silent on definitions for added value services and 'future in-vehicle applications and services'. A legal vacuum is, thus, created with respect to the applications and services and the functioning of the mandatory in-vehicle system.

This lack of clarity with respect to the dual or even triple purpose (if a distinction is made between added value services and C-ITS services) of the system raises fundamental questions on its design. Everyone comprehends the rationale behind making seatbelts mandatory: it is a

[61] It also provides that the Commission will adopt a legislative initiative on the bases of those requirement 'if appropriate', which probably depends on the outcome of the study. On 15-12-2017 such a legislative initiative could not be found by the author.

[62] C-ITS Platform/Working Group 6, 'Access to in-vehicle resources and data'(Report, European Commission 2015).

[63] C-ITS Platform, 'Final Report' (Report, European Commission 2016) 17.

[64] C-ITS Platform/Working Group 6 (n 62) 4.

[65] Article 3(1): '112-based eCall in-vehicle system' means an emergency system, comprising in-vehicle equipment and the means to trigger, manage and enact the eCall transmission, that is activated either automatically via in-vehicle sensors or manually, which carries, by means of public mobile wireless communications networks, a minimum set of data and establishes a 112-based audio channel between the occupants of the vehicle and an eCall PSAP'.

[66] Article 3(2) Regulation 2015/758/EU.

[67] Article 3(7) Regulation 2015/758/EU.

measure which infringes personal freedom to a small extent with an obvious direct safety benefit. The benefits of making Intelligent Vehicle Safety Systems mandatory have been researched, but it is not evident these justify a mandatory roll-out. It is telling that the Commission repeatedly cites the numbers of deaths and injuries (except for 2005) per preceding year in its 2005, 2006, 2009 communications without differentiating the number of those affected by long waits for emergency services. Surely the number of bicycles, mopeds, pedestrians and instant deaths in cars do not count for the life-saving argument. One of the most significant drawbacks of the relevant assessments is their focus on the benefits. While these include the financial costs in their analysis of potential disadvantages, no reference is made to considerations about the impact on fundamental rights.[68]

The Commission does not engage in an analysis of the parts of the system that are necessary for safety, considering instead a package-deal without advancing a proper argument on its necessity. Given the Commission's claim that these systems will bring together ICT, mobile communications and satellite navigation, it should have been at least aware of the possibility that these systems could interfere with fundamental rights. Consequently, the Commission should have raised the question whether this would have consequences in the face of its earlier considerations to obligate the installation of eCall through legislative intervention. Using the law to force a system into private property, which serves a variety of collective private and public interests, can be seen as a legislative version of 'detournement de pouvoir'. Already in the 2006 recommendation of the eCall Driving Group, four large constituencies were introduced, of which the fourth consisted of 'public social security organizations, private insurance companies and Automobile Clubs'.[69] In this respect, it should be noticed that Article 6(9)(i) Regulation 2015/758/EU provides that 'differences may exist between the data processing carried out through the 112 system and the TPS systems or other added value services'. This implies that the provision of added value services, which builds on the in-vehicle system, allows for the processing of more personal data than the provision of the 112 service. This in turn implies that the system installed in the car is able to perform more functions than those strictly necessary for the emergency service. In short, the commercial ambitions facilitated by the Commission lead to the installation of a device more intrusive than necessary for the provision of the 112 service.

[68] COM (2005) 431 (n 19) 5. They are referred to in the slides on implementation status from 2009 as: "Exploratory study on the potential socio-economic benefits of the introduction of Intelligent Safety Systems in Road Vehicles".

[69] eCall Driving Group, 'Recommendations of the DG eCall for the introduction of the pan-European eCall' (Version 2.0, eCall Driving Group 2006) 2.

3. The Impact Assessment and Explanatory Memorandum

The aim of this section is to evaluate the impact assessments of the Commission, in particular their catering for the right to privacy and data protection in the process leading towards the legislative proposal. The second part is normative and performs an analysis of the impact assessment against the Commission's official position on the case law of the ECtHR and CJEU. The aim is to assess the options which would have allowed the Commission to ensure effective protection of the Charter's rights, particularly the right to privacy, in accordance with its rhetoric.

3.1 The Impact Assessment and Explanatory Memorandum of the Commission

The European Commission executed three impact assessments: one accompanying the 2008 Action Plan and the Proposal for the ITS framework Directive; another accompanying the Commission Recommendation for an EU-wide eCall service; and the final assessment included in the proposal for the Regulation concerning type-approval requirements for the deployment of the eCall in-vehicle system. They are discussed in chronological order.[70]

The first impact assessment, accompanying the ITS Action Plan 2008 and the Proposal for the ITS Directive, introduces the problems, stating that the benefits of ITS 'seem to be generally recognised [and] that **the uptake of ITS in road transport has been rather slow and** fragmented, mainly because of lack of cooperation among stakeholders, a low level of interoperability and unsolved privacy and liability issues'.[71] According to the Commission this results in ITS not being 'used to its potential to address societal problems of congestions, safety and pollution'. Classifying the slow and fragmented uptake of ITS as 'the problem' is conditional upon the assumption that a successful uptake of ITS will solve, or contribute to solving, societal problems of congestion, air quality, environment and accidents. The 'problem' is framed as the non-realisation of an unproven solution. In contradiction to its own impact assessment guidelines, the Commission provides no evidence to support the position that the fast and coordinated uptake of ITS will contribute to solving these problems.[72] In response to the posed problems, the Commission sets the following general objective:

> 'The general objective of the present initiative is to create the conditions and, in particular, to put in place the necessary mechanisms to foster the uptake of ITS services and applications

[70] It was stated in the Impact Assessment accompanying the action plan that 'Concrete legislative proposals to be decided by the Commission using the comitology procedure will however be underpinned by an additional and specific impact assessment.' SEC (2008) 3083 (n 25) 38. This referred to the delegated regulations providing the specifications. Also Article 6(7) Directive 2010/40/EU established that the Commission would conduct an impact assessment including a cost-benefit analysis prior to the adoption of the specifications, which were adopted through the delated regulations. In the end there was no impact assessment executed for these regulations.

[71] SEC (2008) 3083 (n 25) 12.

[72] Commission, 'Impact Assessment Guidelines' SEC(2009) 92, 21.

> for road transport and their interconnections with other modes of transport in order to have ITS contributing at its full potential towards the various EU policies.'[73]

'Unsolved privacy and liability issues' are identified as one of the 'problem drivers hindering ITS take up'.[74] The collection and exchange of privacy sensitive (traffic) data is presented as a requirement for ITS, such as pay-as-you-drive insurances, eCall, road charging.[75] It is highlighted that this will be 'partly sensitive in terms of privacy policy', however, there is no indication that the way in which this data will be processed depends on the design of ITS and is key to the extent to which privacy issues will arise. Legal certainty on privacy issues is presented as a precondition for the exchange of traffic data. Fundamental rights, recognised as imposing legal limits to the EU's right to take action, 'will be fully respected and attention will be paid to the protection of individual privacy in the different ITS applications, as this specifically constitutes one of the issues identified as needing to be addressed'.[76] Solving privacy and liability issues are set as a specific objective, yet solving the privacy issue is identified as a specific objective 'related to the provision and sharing of data, and to the deployment of novel safety-enhancing applications and value-adding services'.[77] The privacy issue is linked to the sharing of data. Linking the privacy issue to the sharing of data seems to be based on the presumption that interests served through the sharing of data automatically outbalance the interest of not sharing data – one protected by the right to privacy. The formulation of this objective contains an implicit assumption that the right to privacy of all EU motorists is outweighed a priori by the ITS ambitions of the Commission. This is in dire contrast to one of the goals of the impact assessment, which is to enable the Commission departments to make a systematic and thorough assessment leading to a legislative proposal in which the fundamental rights are respected.[78]

In the impact assessment, different policy options are considered ranging from Option A of 'no additional new action', Option B of 'overcoming specific problems by concentrating on enabling actions and application fields', to 'Option B extended with a comitology procedure' (hereinafter also referred to as 'Option B+'). All of these options have a different impact on the specific objective of solving privacy issues. According to the Commission, Option A 'will hardly improve owing to an insufficient penetration rate of personal safety devices and services', resulting in little to no direct impact on interoperability, cooperation and privacy and liability and no indirect impact on economic, societal and environmental matters.[79] The

[73] SEC (2008) 3083 (n 25) 29.
[74] ibid 17.
[75] ibid.
[76] ibid 29. Among these applications that are identified earlier are road charging (tolling systems), eCall, intelligent speed management and pay-as-you-drive insurance. In the comments on this last application it is even indicated that such a scheme had to be abandoned in the UK due to too little subscribers as a result of the fact that people did not want to have a tracking device installed in their car.
[77] ibid 31.
[78] Commission, 'Compliance with the Charter of Fundamental Rights in Commission legislative proposals: Methodology for systematic and rigorous monitoring'(Communication from the Commission) COM (2005) 172 final 3.
[79] SEC (2008) 3083 (n 25) 42, 60, 61.

Commission concludes that this is not the preferred option. Under Option B and B+ five 'priority action areas are indicated'. Three actions are particularly relevant with respect to their impact on fundamental rights and the assessment of the relevant impact by the Commission. The first action is as follows:

> 'the definition of a **functional open in-vehicle platform** allowing the re-use of crucial components (communication technologies, positioning, processing power and Human Machine Interface). Such a platform will permit synergies and reduce the cost of introducing and operating ITS services; it should also guarantee access for the public sector and applications of public interest. This action will facilitate the integration of the vehicle into the transport system and support the introduction of cooperative systems in the longer term, by standardising the exchange of data between the infrastructure and the vehicle, and between vehicles themselves. It includes further support for broader take-up of (autonomous) safety-enhancing in-vehicle applications.'[80]

This action establishes the building blocks for the in-vehicle system which enables 112 eCalls, but also allocates to the hardware and software the function to provide third party services and ultimately opens the perspective to link the car to the infrastructure (C-ITS). This action lays the foundation to fit the future car into the EU vision on the Internet of Things.[81] It can also be seen as the follow-up of the 2003 Communication statement on adapting vehicle type approval legislation to mandate 'Intelligent Vehicle Safety Systems' if appropriate, only here these systems are rebranded as the 'functional open in-vehicle platforms'.[82] In the impact assessment of the in-vehicle platform there is a section asking 'Who will benefit?'. In this section the analysis sticks to the lowering of basic costs through 'standardising and guaranteeing access for all parties involved', which includes public sector entities which 'with access to the platform will be able to address equipped users'.[83] In short, according to the Commission the answer to the question 'who benefits?' is simply: 'Everybody'. Under the 'Longer-term perspective' it is provided that this installation 'will support the development of cooperative systems, building on standardised data exchange between vehicles and 'communication portals along the roadside'.[84] Obviously such a standardised data exchange could carry great consequences for motorists' privacy on the road, but the Commission does not notice any implications for the right to privacy and even rates 'Privacy & liability' under this action with 0/+.[85] It is unclear why this indication is somewhat positive, since this action is likely to have the greatest impact on the right to privacy.

[80] ibid 34.
[81] COM (2009) 278 (n 2).
[82] COM (2003) 542 (n 13) 13.
[83] SEC (2008) 3083 (n 25) 49.
[84] ibid 46.
[85] This will be further treated in subsection on C-ITS.

The second relevant priority action is the following:

> 'Enhancing cooperation, defining responsibilities by the establishment of a framework for **optimised collection, exchange and integration of road and traffic data**, addressing the core of most ITS services.'[86]

Real-time traffic information transmitted by eCall can be used to deliver real-time traffic services.[87] The impact of this action on the right to privacy depends on a number of factors, such as the control the motorists have over the sharing of data, the format in which the data is shared and whether this format allows use for purposes which go against the interest(s) of individual motorists. The Commission does not make any consideration on this issue and sticks to general observations about developing new services and better data exchanges, ending still with a 0/+ for privacy, because 'the fact that stakeholders will discuss ITS-related issues will enhance understanding, and might indirectly support solving of privacy / liability issues'.[88] This seems to be founded on blind optimism.

The last relevant priority action is about 'addressing **privacy and liability issues** linked to ITS services'. This impact is addressed under a later priority action:

> 'the resolution of data security and protection, privacy and liability issues hindering the uptake of certain advanced ITS equipment and services. These issues have been identified as being core to the current slow uptake of ITS: in the absence of clear rules and responsibilities, neither providers nor customers are willing to invest or buy. Though the whole ITS ecosystem is affected, issues relating to deployment of in-vehicle applications and (autonomous) safety-enhancing ones in particular need to be addressed first'.[89]

This priority action perpetuates the presentation of privacy as a problem. Privacy 'issues' need to be solved in order to promote the uptake of ITS, or in this case the investment in it. Although the Commission is consistent in presenting fundamental rights as an obstacle,[90] it is unlikely this presentation contributes to their effective protection. Under Option B+, the Commission is indicated as the responsible party within the Comitology context to take action where necessary on data security, individual data protection and liability (one of the priority actions).[91] The analysis of this priority action's impact is only elaborated upon under Option B. The Commission asks certain questions about who owns the data and how shared data can be used or not. It mentions 'aspects of security and privacy of data (exchange of data being the core of ITS)', but fails to address key questions on respecting the right to privacy, such as the motorists level of control over sharing data and the form in which the data are

[86] SEC (2008) 3083 (n 25) 49.
[87] EDPS also brought this under the attention to the Director-General of DG MOVE in a letter from 12 March 2014.
[88] SEC (2008) 3083 (n 25) 49.
[89] ibid 35.
[90] COM (2009) 278 (n 2) 5.
[91] SEC (2008) 3083 (n 25) 38.

exchanged.[92] This does not stop the Commission from rating 'Privacy & liability' under this action a '+'.

In the explanatory memorandum attached to the proposal of Directive 2010/40/EU, the impact assessment is summarised and repeated. Only recital 9 addresses privacy and personal data with the perfunctory general instruction that the processing of personal data by ITS applications and services should comply with Directive 95/46/EC and Directive 2002/58/E. Article 6 adopts the same positon adding that Member States should 'ensure that ITS data and records are protected against misuse, including unlawful access, alteration or loss' and confirming the applicability of Directive 2003/98/EC on the re-use of public sector information.[93]

The Commission Recommendation on support for an EU-wide eCall service in electronic communication networks for the transmission of in-vehicle emergency calls based on 112 ('eCalls') is accompanied by an impact assessment which does provide a more accurate description of the nature of the problem involving road fatalities, severe injuries, delays in alerting emergency services and reaching the accident scene, long rescue time at the accident scene, and secondary accidents and traffic congestions.[94] For the scale of the problem reference is made to three other figures, and further in the assessment an in depth analysis of a number of countries is provided. It also provides three policy options largely similar to the ones advanced under the impact assessment accompanying the proposal for the ITS Directive. In evaluating the different options the impact on fundamental rights was not taken into consideration. Choices with regard to privacy features in the design of eCall were not involved in establishing policy options by the drafters of the impact assessment, despite the EDPS recommendation to adopt 'privacy by design' at an early stage of the design.[95]

Although the word 'privacy' is mentioned a few times, the 'right to privacy' is not mentioned once. There is a brief section dedicated to the protection of personal data.[96] This section remains quite general: 'eCall requirements comply with the Directives 95/46/EC on the protection of personal data', it 'follows the opinions of the Article 29 Data Protection Working Party', 'the in-vehicle device will be dormant' and when the platform is used for services other than emergency calls 'these should be covered by the appropriate contract between the user and the service provider'.[97]

The impact assessment accompanying Regulation 2015/758/EU is only one page long, in contrast to the 117-page impact assessment accompanying Recommendation 2011/750. While the title includes cost-benefit analysis in addition to impact assessment, the document

[92] ibid 50.
[93] COM (2008) 887 (n 48).
[94] Commission, 'Impact Assessment accompanying the document Commission Recommendation on Support for an EU-wide eCall service in electronic communication networks for the transmission of in-vehicle emergency calls based on 112 ('eCalls')' (Commission Staff Working Paper) SEC(2011) 1019 final 9.
[95] (OJ 2010 C 47/02) (n 49) para 28.
[96] SEC(2011) 1019 (n 94) 13.
[97] ibid 13.

assesses only financial costs.[98] Given the fact that this is the legislative act obligating the installation of this system, which in the long run permits 'synergies and reduce the cost of introducing and operating ITS services', guarantees 'access for the public sector and applications of public interest' and facilitates 'the *integration of the vehicle into the transport system*', the need for a more elaborated assessment on its impact on fundamental rights is self-evident.[99]

Already in 2011, the EDPS noted that 'the choice of a mandatory introduction of eCall will have to be properly justified in terms of data protection' and that it should be 'demonstrated why the mandatory introduction of eCall is necessary for the pursued purpose'.[100] These comments have been ignored and the impact assessment does not even attempt to demonstrate the necessity of the mandatory introduction. In line with the other assessments of the European Commission an assessment of the impact on fundamental rights is completely absent.

In the detailed explanations of the proposal, a reference is made to Article 6 of the Regulation 2015/758 in relation to the rules on privacy and data protection. This provision does establish a number of rules in which the advice of the Article 29 Working Party can be recognised, such as 'vehicles equipped with eCall in-vehicle system are not traceable and are not subject to any constant tracking in their normal operational status related to the eCall' and '(P)rivacy enhancing technologies shall be embedded in the in-vehicle eCall system'.[101] However, it only addresses the 'eCall in-vehicle system' which in the proposal is equal to the 112 eCall system, thus excluding the added value services building on this system. What PETs mean is left open. The Commission is granted power to decide on personal data and privacy enhancing technologies through delegated acts.[102]

These impact assessments reveal quite a disturbing picture in which fundamental rights impact assessments on eCall were hardly performed, despite the fact that this is an initiative where the concerns with regard to fundamental rights have been recognised years before the first impact assessment. Explanatory memoranda reveal a Commission with a preference for applying a watered down version of data protection legislation, which mainly concerns itself with procedural rules on safeguarding data, but fails to engage in genuine analysis of its

[98] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall in-vehicle system and amending Directive 2007/46/EC' COM (2013) 316 final 3.

[99] SEC (2008) 3083 (n 25) 34. Italics in original text.

[100] European Data Protection Supervisor, 'EDPS comments on the Commission Recommendation and the accompanying impact assessment on the implementation of the harmonised EU-wide in-vehicle emergency call ("eCall")' (European Data Protection Supervisor 2011) 1.

[101] See also Recital 14 on information requirements 'Consumers should be provided with a realistic overview of the 112-based eCall in-vehicle system and of the TPS eCall system, if the vehicle is equipped with one, as well as comprehensive and reliable information regarding any additional functionalities or services linked to the private emergency service, in-vehicle emergency or assistance-call applications' and Recital 15 'The 112-based eCall in-vehicle system and the system providing private or added-value services should be designed in such a way that no exchange of personal data between them is possible.'

[102] Article 6(4) proposal of Regulation 2015/758/EU.

proposals against such substantive rules as purpose limitation, proportionality and data minimisation.

The reasons for this omission are unclear. Did the Commission lack the technical as well as legal knowledge to execute the impact assessment in line with its own ambition to realise a fundamental rights culture, or can their omission be attributed to the fact that it has long recognised the business interests in a privacy-invasive in-vehicle platform? Taken into account that privacy was already recognised as a problem early in this policy process it is more likely that the Commission's omission can be attributed to the latter. It is, also, in line with the Commission's approach to privacy in IoT in general, as discussed in Chapter 4.

3.2 The Impact Assessment and Explanatory Memorandum revisited

The first concern in the execution of the impact assessment for the ITS Directive lies in the identification of the problem. The Commission frames the problem as the slow and fragmented uptake of ITS.[103] Given the fact that 'ITS' is an umbrella term for almost everything involving ICT and cars, this cannot qualify as a well-described problem. In line with its own guidelines the nature of the problem should be described in clear terms. Clarifying the nature of the problem is pivotal for the next steps: supporting the description of the problem with evidence, setting out the scale of the problem, identifying those most affected by it, identifying risks and uncertainties, justifying action on EU level etc.[104] An accurate description of the problem is also necessary in order to establish if and to what extent an interference with fundamental rights is justified, as a precondition for setting objectives and considering different policy options, which in turn can assist in establishing safeguards mitigating the impact on fundamental rights. Failing to identify the problem clearly makes it impossible to test the proportionality of the measures proposed and the necessity of the interference with the right to private life. In the context of data protection law, it can be viewed as the failure to establish a specified, explicit and legitimate purpose for the processing of personal data, making it impossible to apply data protection law principles such as data minimisation. In short, this impact assessment goes off the rails before it starts.

Second, the Commission should have produced evidence on the effects the fast and coordinated uptake of ITS will have on each individual challenge in road transport. In that respect, the case for ITS was pleaded for prematurely by the Commission in 2003, five years prior to the impact assessment which in the end does not produce evidence supporting the resolution of these challenges by ITS; it merely refers to some sources which indicate numbers on the challenges.[105] The causal connection between these challenges and 'the problem' is simply taken as the starting point. The 'problem' is presented as the solution to the social problems identified (see section 6.3.1). The impact assessment, however, does not provide any proof to demonstrate this. Therefore the objectives become mere steps towards

[103] SEC (2008) 3083 (n 25) 12.
[104] SEC(2009) 92 (n 72) 21.
[105] SEC (2008) 3083 (n 25) 13.

realising 'the solution' without linking them to the challenge they are supposed to meet. The lack of evidence is in stark contrast with the goal of the impact assessment which 'is a key tool to ensure that Commission initiatives and EU legislation are prepared on the basis of transparent, comprehensive and balanced evidence'.[106] Its political significance is seen in its ability to 'provide sufficient evidence to respond to concerns that are likely to arise in the decision-making process or the public reaction after the Commission adopts the initiative'.[107] This implies that the Commission can provide evidence to justify why it has made certain decisions and left others out. Following the indicators provided in the Commission's guidelines the political importance of ITS is high as it cuts across policy fields (e.g. sustainable development, competitiveness and economic growth), it raises concerns related to proportionality (amongst others mandatory versus voluntary), it could become very controversial and it affects fundamental rights.[108] The level of political importance is especially high in relation to privacy concerns, which the Commission recognises itself as the main obstacle in the way of the successful uptake of ITS.

The specific objectives of the ITS impact assessment include such abstract goals as 'to increase interoperability by standardisation of basic components', 'setting up of an efficient concertation/cooperation mechanism between all ITS stakeholders in order to provide a clear vision on how ITS should be deployed on a Europe-wide scale' and 'solving privacy and liability issues related to the provision and sharing of data'.[109] Since the specific objectives are not linked to solving any specific problems, it is virtually impossible to assess different policy options in terms of effectiveness and efficiency, because the fulfilment of the objective itself will not lead to solving the social problems. The same criticism can be directed at the assessment of whether a negative impact is necessary to realise the stated objective. If the specific objectives would have been to reduce the number of deaths or emissions, the necessity of the proposed solution could be tested. This is why the Commission's impact assessment guidelines instruct the staff to make the objectives SMART, so the objectives can be linked to the identification of policy options and compare them.[110] Without establishing how the different policy options contribute to solving the problem it is impossible to pursue one of the most important aims of the assessment with respect to fundamental rights: the assessment whether there are less infringing alternatives.[111] The inventory of different policy options here would have forced an early evaluation of alternatives to system-design in relation to the privacy concerns. The Commission systematically omits to address the design of ITS.

In the Recommendation's Impact Assessment, the 'specific objectives' do address more concrete aims, like the improvement of the operation of emergency services and the reduction

[106] SEC(2009) 92 (n 72) 4.
[107] ibid 13.
[108] ibid 14. Four out of five can also be found in these guidelines.
[109] SEC (2008) 3083 (n 25) 38.
[110] SEC(2009) 92 (n 72) 28.
[111] Commission, 'Operational Guidance on Taking Account of Fundamental Rights in Commission Impact Assessments'(Commission Staff Working Paper) SEC(2011) 567 final 18.

of secondary accidents.[112] These are, however, not linked to the design of the system. With respect to the added value services the impact assessment only provides that 'these should be covered by the appropriate contract between the user and the service provider'.[113] Taking privacy into account in the design of the system through which these added value services are provided should have been addressed in the impact assessment of Regulation 2015/758/EU.

3.2.1 Identifying the impact of the eCall system

No party was in a better position to assess the *likelihood* and the *magnitude* of the impact of the eCall-system within the ITS framework than the European Commission. It has been the constant driving force behind the policy and legal developments and was the binding factor working hard to align the interests of the stakeholders, with the exception of citizens, using soft force backed up by the threat of legislative intervention. The recommendation of the eCall Driving Group in 2006 introduced four large constituencies, including such industries as automotive and mobile telecommunications, as well as 'the public emergency authorities and associated or cooperating service organisations'; and 'the public social security organizations, private insurance companies and Automobile Clubs'.[114]

These parties and their respective agendas could have informed the Commission in assessing the *likelihood* and *magnitude* of the various impacts. This is particularly the case since the exploitation by industry and public authorities has been a key selling point of the Commission all along in order to gain cross-sectoral support for a mandatory deployment of eCall and ITS. The relation between the data that can be collected through eCall, the information that can be inferred from it and the relevance of this data and information for these third parties, plus other public authorities and commercial parties, denominates the likelihood that this information will actually be used. The magnitude of this impact can be established by using the ECtHR criteria: the nature of the interference and the interests to be protected from the interference.[115]

The installation of eCall opens up a spectrum of potential surveillance measures. The compulsory introduction of eCall lowers the threshold for the state, as well as other parties powerful enough to exploit this option, to engage in surveillance practices regarding travelling movements by car and potentially eavesdropping on conversations in the car.[116]

---

[112] SEC(2011) 1019 (n 94) 14.

[113] ibid 13.

[114] eCall Driving Group (n 69) 2.

[115] Ursula Kilkelly, *The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention of Human Rights* (Human rights handbook, No 1, Council of Europe 2003) 32.

[116] Compare the calculations made by two American scholars on the reduction of costs by the introduction of GPS: Kevin S Bankston and Ashkan Soltani, 'Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v Jones' (2013) 123 The Yale Law Journal 335. It should be noted that they treat the case where a tracking device is installed by the designated public authority. With the adoption of Regulation 2015/758/EU the installation of a tracking device became the standard. Stefan Eisses, Tom van de Ven and Alexandre Fievée,

There is a wide range of (risks to) interferences with the right to privacy introduced by the eCall system, which for the sake of readability are redubbed 'challenges'. These challenges are outlined below.

Unchecked connection to the network

Some of the challenges introduced were already addressed in 2006 by the Article 29 Working Party. Then the idea for the eCall architecture was practically the same. One of the demands of the Working Party was that eCall should not be permanently connected to the mobile communication networks in order to prevent continuous monitoring of people.[117] If eCall was continuously connected to these networks this would result in a permanent processing of personal data. Through triangulation this data could be used to create a detailed map of the motorist's travelling movements. The importance of this feature of the design was known, thus, at least eight and a half years before the Regulation was adopted. This feature is left unaddressed in the Regulation.

Parliamentary history shows there has been some confusion as to the exact status of the eCall modem. When MP Judith Sargentini asked Commissioner Kroes about this matter, she was told that the first thing eCall would do when a car was started was to register with a public mobile wireless communications network.[118] As such, eCall could constitute an interference with the right to private life and the protection of personal data.[119] This was also confirmed in another Commission document which provides that in case of insufficient coverage 'the device will normally register in whatever network is available'.[120] In response to follow-up

---

'ITS Action Plan: ITS & Personal Data Protection' (Final Report, European Commission DG Mobility and Transport 2012) 6.

[117] Article 29 Data Protection Working Party, 'Working document on data protection and privacy implications in eCall initiative'(Adopted on 26th September 2006 1609/06/EN WP 125, The Article 29 Working Party 2006) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf> accessed 4 June 2018, 3.

[118] 'In its reply of 21 August 2013 to my Question E-008690/2013, the Commission stated that when a vehicle which is equipped with eCall technology is started, the in-vehicle system will automatically 'register' in the telecommunication network with the best coverage reachable, but 'communication' will take place only after an eCall has been triggered.' See European Parliament, 'Answer given by Ms Kroes on behalf of the Commission' (Parliamentary questions E-008690/2013, European Parliament 2013) <http://bit.ly/1Na51gc> accessed 5 June 2015.

[119] Notice that a car is different from a telephone which needs to connect to a network in order to perform its function. The same does not hold true for a car. Also note that 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* App no 35623/05 (ECtHR, 2 September 2010) , para 52), this view has been criticized. For criticism see Paul De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 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.

[120] SEC(2009) 92 (n 72) 25.

questions of EP Sargentini, about the parties involved in the registration of the system and transmitted data, Commissioner Kroes made a U-turn and stated that eCall in its normal operational status is not registered to any telecommunications network and that it only 'scans' the radio spectrum for available networks, without communicating with the mobile network operators.[121] This statement was echoed in the informal communication from the Commission with the questionable title: 'eCall – Do you have any concerns for your privacy? You shouldn't….'.[122] This was a major shift in the explanation of the functioning of the system, in which it moves from a standard interference with the right to privacy and the right to the protection of personal data to no interference at all. 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.[123] When Simon Hania, privacy officer of TomTom, informally asked the Commission staff involved in eCall whether these implications were fully taken into account, their answer was 'no'.[124]

The microphone

Another privacy risk created by eCall is the installation of the microphone. Just like the microphone on a mobile phone it is possible to turn this on from a distance.[125] eCall works with a sim-card and these can be hacked fairly simply.[126] Apart from criminals, parties that engage in industrial and political espionage or in tactical operations against dissident groups, could have an interest in exploiting these vulnerabilities.[127] In the US, there is at least one

[121] European Parliament, 'Written questions with answer: Written questions by Members of the European Parliament and their answers given by a European Union institution' (Notices from European Union institutions, bodies, offices and agencies OJ 2014 C 179/252, The Publications office of the European Union 2014) 251-252. See also, C-ITS Platform, 'Final Report' (Report, European Commission 2016) 74: "The eCall unit is not registered in the mobile networks (to avoid tracking) until the eCall is activated, automatically or manually. It remains registered for some time to enable call back from the emergency call centre and then goes back to "dormant mode" and cannot be reached from the network side."

[122] See European Commission, 'eCall: Do you have any concerns for your privacy? You shouldn't' (Digital Single Market factsheet/infographic, 4 June 2014) <https://ec.europa.eu/digital-single-market/en/news/ecall-%E2%80%93-do-you-have-any-concerns-your-privacy-you-shouldnt> accessed 3 March 2015.

[123] 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. 'Tell-all telephone' (Zeit Online, 31 August 2009) < https://www.zeit.de/datenschutz/malte-spitz-data-retention> accessed 7 June 2018.

[124] Tijmen HA Wisman, 'eCall and the Quest for Effective Protection of the Right to Privacy' (2016) 1 EDPL 59, 61.

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

[126] Security expert Peter Rietveld agrees to this. He pointed out in a private communication that 'building an attack-proof system2system authentication system over an untrusted network (such as mobile) has until today never been successful. Chances that an attacker may actually breach such as system must not be underestimated.' He sees a much bigger problem in the reverse: criminals can use the system as a solution to start (preferably expensive) cars without the ignition key.

[127] A most revealing story of a private surveillance company was about 'Hacking Team'. Among its primary targets were Privacy International and Human Rights Watch. See Alex Hern, 'Hacking Team hack casts

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.[128] Bart Jacobs, professor of computer security, warned in 2013 that this system allows for intelligence agencies to know the exact location of all cars as well as the capability to listen in.[129] In the Netherlands, a bill has been proposed which allows public authorities to hack automated works, a category which covers eCall, and turn on a microphone.[130] If this vulnerability proves exploitable, the mandatory deployment of eCall is equal to the obligation to install a tapping-device in every new car from 2018 onwards.[131] Again, the impact assessment remains silent on this issue.

Remote shut down of the car

The fourth challenge already received attention in the Netherlands in 2013 from security expert Peter Rietveld. His concern was the weak security of the chip used in eCall. The chip accepts incoming traffic in order for the PSAP to make a call to the car and to receive updates. Rietveld pointed out that this feature could be abused by malicious parties to get access to the motor management system. This vulnerability might also be attractive for the police to exploit. The European Networks of Law Enforcement Technology Services (ENLETS) is an informal network of heads of departments responsible for implementing new technologies in police departments instigated under the Council of the EU.[132] ENLETS searches for opportunities provided by emerging technologies related to EU security research and industrial policy. It established a programme through which Member States will share best practices on inter alia 'Front Line Policing, Vehicle Stopping'.[133] It states that cars on the run are dangerous for citizens and that there are insufficient means available for a proportionate response, therefore they will work 'on a technological solution that can be a

---

spotlight on murky world of state surveillance' (The Guardian, 11 July 2015) <https://www.theguardian.com/technology/2015/jul/11/hacking-team-hack-state-surveillance-human-rights> accessed 2 August 2015.

[128] Jonathan L Zittrain, *The Future of the Internet and how to stop it* (Yale University Press) 2008, 109. 'Mobile phones can be reprogrammed at a distance, allowing their microphones to be secretly turned on even when the phone is powered down.'

[129] See Boris van Zonneveld, 'Nieuwe chip maakt auto doelwit' (Technisch Weekblad, 29 June 2013) <https://www.technischweekblad.nl/nieuws/nieuwe-chip-maakt-auto-doelwit/item4237> accessed 29 February 2016.

[130] Kamerstukken II 2015-2016, 34 372, no 2 & 3, 12 'Computercrime III' (legislative proposal, 2013) <https://www.rijksoverheid.nl/documenten/kamerstukken/2013/05/02/wetsvoorstel-aanpak-computercriminaliteit> accessed 28 August 2015.

[131] Boris van Zonneveld, 'Nieuwe chip maakt auto doelwit'(Technisch Weekblad, 29 Juni 2013) <https://www.technischweekblad.nl/nieuws/nieuwe-chip-maakt-auto-doelwit/item4237> accessed 10 December 2015.

[132] Council of the European Union, 'European Network of Internal Security Technology Departments' (Doc 14669/08, 2008).

[133] Council of the European Union, 'ENLETS Work programme 2014-2020: European Network of Law Enforcement Technology Services' (Doc 17365/13, The Publications Office of the European Union 2013) 5.

"build in standard" for all cars that enter the European market'.[134] The current design of eCall provides a platform for ENLETS to realise this obscure plan.[135] The interference with the right to private life consists in the potential for control that the police would gain over vehicles of citizens.

Added value services: constant tracking and other risks

eCall introduces another way to constantly track a vehicle.[136] In practice, this can be done by using the GSM modem to communicate the location data acquired through the satellite in real-time. Added value services can actually use satellite and GSM-technologies from the 112 system to facilitate their own operation.[137] This was noted also by the EP in its note on Data Protection Aspects of eCall, in which it held that there was a clear conflict between the prohibition of the permanent tracking of the 112 eCall and the possibility of using the in-vehicle platform to offer added value services 'which require permanent contact with the in-vehicle device and downloading data on the vehicle location'.[138] According to the EP, 'accepting the possibility of permanent tracking for purposes connected with providing added value services raises the question as to the effectiveness of the prohibition of permanent tracking with regard to the eCall system's normal functioning mode.'[139] This demonstrates that the commercial function of the eCall system has a severe impact on the effective protection of the right to privacy. The ability of the 112 system to facilitate added value services implies it is designed to serve more purposes than providing the emergency service (see section 2.2) and this design carries implications for how the system can be (ab)used against citizens. Other authors also noticed the risk that eCall could be used to calculate the average speed and prosecute motorists for traffic offences, or render void insurance coverage in case of an accident.[140]

---

[134] ibid 8.

[135] Eric Töpfer, 'A new player in SecurityResearch: the European Network of Law Enforcement Services (ENLETS)' (2010) 21/2 Statewatch < http://www.statewatch.org/subscriber/protected/sw21n2.pdf> accessed on 7 June 2018.

[136] In a presentation of NXP the options for the software to offer applications for road pricing and stolen vehicle tracking affirms that outside of the normal operational status constant tracking is possible. 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> accessed 6 July 2015.

[137] Source: an employee of ERTICO-ITS Europe, 'a platform founded in 1991 as a platform for the cooperation of all relevant stakeholders in the deployments of ITS systems in Europe', see Ertico, 'The ERTICO Partnership – Vision & Mission' <http://ertico.com/vision-and-mission/> accessed 17 September 2015.

[138] Xawery Konarski, Damian Karwala and Hans Schulte-Nölke, 'Data Protection Aspects of eCall' (Document requested by the European Parliament's Committee on the Internal Market and Consumer Protection IP/A/IMCO/NT/2013-12, European Union, 2014) 20.

[139] ibid.

[140] Christophe Geuens and Jos Dumortier, 'Mandatory implementation for in-vehicle eCall: Privacy compatible'(2010) 26 Computer Law & Security Review 385, 386.

Processing of personal data for added value services

The processing of personal data for added value services also introduces other risks. Another action plan by the European Commission warns on ITS applications which collect vast amounts of location data. It asks for 'special attention from a data protection point of view, as the potential privacy infringement resulting from unauthorised access to, or misuse of such data is considerable'.[141] This is related to the priority actions of the Commission to provide EU-wide real-time traffic information services.[142] The technical components which enable the 112 system to function provide the basis for telematics services such as pay-as-you-drive insurance, road pricing (toll) and fleet management.[143] If the processing of detailed data necessary to provide these services takes place on a central level it creates the risk of potential privacy interferences. The magnitude and likelihood that these risks will materialise is high, since there are many ways in which this data offers different stakeholders opportunities to capitalise on it. Furthermore, there is a considerable chance that this data will have a monetary value. As a result this can make the freedom to refuse the processing of this data dependent on whether the data subject can afford her or his privacy.

The threat areas identified by the Commission in its action plan include unauthorised access to personal data, re-use of personal data beyond the legally defined purpose (although it should be noticed that re-use for a legally defined purpose also represents an impact on privacy) and excessive processing (processing more than is necessary for the purpose).[144] This is only one part of the problem. The recent developments elaborated upon in the next section reveal that there are plans to use the eCall-system to constantly collect data from the car, amongst others about the location.[145] The privacy problem precedes the problem of access and excessive processing of personal data: 'the fact that it has been possible to *record* the circumstances of a person's private life in the form of data'.[146] This is inextricably linked to the mandatory installation of the eCall system in its current form.[147]

C-ITS

The impact assessment of Directive 2010/40/EU established that the definition of an 'open functional platform' for ITS services would 'support the development of cooperative systems building on standardised data exchange between vehicles and 'communication portals along

[141] 'ITS Action Plan: ITS & Personal Data Protection' (n 116) 6.
[142] Article 3(b) Directive 2010/40/EU.
[143] COM (2009) 434 (n 34) 7; Cognizant, 'The New Auto Insurance Ecosystem: Telematics, Mobility and the Connected Car' (Cognizant Reports, Cognizant 2012) 5.
[144] 'ITS Action Plan: ITS & Personal Data Protection' (n 116) 53.
[145] Mike McCarthy and others, 'Access to In-vehicle Data and Resources'(DG-MOVE Final report, European Union 2017).
[146] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* EU:C:2014:238, [2014], Opinion of Villalón, paras 61, 63 and 65.
[147] ibid. Italics added by author.

the roadside'.[148] Regulation 2015/758/EU established the ambition for the Commission to take a legislative initiative based on requirements for the open-access platform.[149] Although such an initiative has not yet been taken, the Commission has already started the groundwork. In 2016, it adopted a 'European Strategy on Cooperative Intelligent Transport Systems (C-ITS)' which associates the interest to save lives with the commercial interests of industry, similar to the approach taken in its communication from 2003. On the one hand, according to the Commission, the objective 'is to allow for a wide-scale commercial deployment of C-ITS as of 2019', on the other it states that '(M)ost importantly, digital technologies help reduce human error, by far the greatest source of accidents in transport'.[150]

Directive 2010/40/EU established linking the vehicle to the transport infrastructure as a priority area for the development and use of specifications and standards, and thus provided the legal bases for the Commission's and ESOs' work on C-ITS. Regulation 2015/758/EU established the ground for the Commission's further work on the open-access platform, but did so in the context of the mandatory deployment of eCall, thus setting up a legal link between eCall and C-ITS. In the final report from the C-ITS platform in 2016, the technical link between the two was described as follows:

> 'eCall introduces an in-vehicle system that provides an advanced vehicle telematics function which may share the same basic hardware and software components that can also be used for other telematics system functions.'[151]

C-ITS builds on hardware and software components of eCall, but it is not fully intertwined with it. The C-ITS Working Group 6 of the C-ITS Platform on 'Access to in-vehicle resources and data', discussed a number of ways to gain access to in-vehicle data. One of the ways to realise access to in-vehicle data is through a 'data server platform'.[152] Accordingly, data will be sent from the car to the server using the GSM modem. Stored on the server it can be used on the basis of consent or contract by the motorist to allow access to it by third party services providers. The data can also be accessed on the basis of legal obligations. In terms of privacy and data protection this implies that the motorists loses control over the collection of data recorded by their car and only retain some control over how the data is *used* in horizontal relations, excluding vertical ones (police, public authorities, intelligence agencies etc.).

In a 2017 European Commission report there is a curious paragraph on how this data server platform relates to data protection, which states that 'it is only the actual use of personal data by service providers that would require the consent and notification of the data subject'.[153]

---

[148] SEC (2008) 3083 (n 25) 46.

[149] Recital 16 Regulation (EU) 2015/758.

[150] European Commission, 'An EU strategy on cooperative, connected and automated mobility' (Fact Sheet MEMO/16/3933, European Union 2016).

[151] C-ITS Platform, 'Final Report' (Report, European Commission 2016) 74.

[152] There is still discussion between the car manufacturers an independent operators and service providers about who should manage and control the platform.

[153] 'Access to In-vehicle Data and Resources' (n 145) 32.

This report discusses a number of 'technical solutions for the access to in-vehicle data', such as the data server platform, and none of these solutions are 'in principle incompatible' with the obligation following from the GDPR.[154] The claim that consent, a processing ground for personal data, is only required for the actual use of personal data, is false. Recital 15 of Regulation 2015/758/EU provides some space for this error as it states that the added value services 'should always remain optional for consumers', however, this only addresses the delivery of the service, not the initial collection of data intended by car manufacturers. The contention that the collection of data can take place without a processing ground is at odds with the very letter of European data protection law . The ACEA website demonstrates that industry has embraced this misconception of data protection law.[155]

3.2.2 Addressing the impact of the eCall system

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 at least try to explore the full spectrum of these negative impacts (intended and unintended) and to assess for each specific impact whether it could be avoided.[156] For the impact that could not be avoided the next step would be to develop safeguards mitigating these negative impacts and to adopt them in the legislative proposal, contributing to a design of eCall which would be the least infringing alternative.[157] The remaining interference should have been clearly established in the legislative acts, ideally making it technically impossible or at least hard for third parties to abuse the system for their own purposes. These together should have formed the concrete elements of system design.

In retrospect, the legislator should have adopted demands on essential elements of design in the eCall Regulation and the ITS Directive to delineate the area in which the Commission, and in its turn the ESOs, could exercise their discretion. If the Commission had developed demands mitigating the negative impacts on the right to privacy in the impact assessment, it could have promoted their adoption in the Regulation. This shows the relationship between a properly executed impact assessment and the adoption of essential elements of design in the legislation. Ideally, this should rule out the possibility for purpose and function-creep.[158] This comes down to setting demands for a privacy-friendly design, or Privacy Enhancing Technologies (PETs) in the legislative acts. In order to adequately address privacy in the design of the system, the specific demands for the system and what privacy interferences they

[154] ibid 125.

[155] Car data facts, (fact-based overview on everything related to the sharing of vehicle-generated data with third parties) <http://cardatafacts.eu/> accessed 7 June 2018.

[156] Commission, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'(Communication from the Commission) COM (2010) 573 final 3.

[157] In doing so the Commission would comply with the sub-test of necessity which follows from the proportionality test in Article 52(1) of the Charter.

[158] Wisman (n 11).

seek to address should be provided in the legislative act, ensuring a clear instruction which cannot be circumvented through creative interpretation.

Without intending to be exhaustive, these elements will be illustrated by two examples. First, it could have been provided in the Regulation that eCall could only connect with wireless communication networks after an accident and not before. Currently, the Regulation remains silent on this important feature, leaving it to the Commission and possibly ESOs to decide on this precarious matter. The only vital information for emergency services is the location of the accident and the number of people involved.[159] Even the unique number of the car, the Vehicle Identification Number (hereinafter VIN), is not necessary to include in the MSD. What the VIN could do is to serve as a client number. The unique address of the car is a practical feature to provide services to its owner, making it possible to track individual vehicles. In other words, the relevant industry has a big interest in this feature which has an adverse effect on the right to privacy. To establish a voice/audio-connection a unique point of contact is necessary, which does not have to be linked to a person. Moreover, the microphone is not necessary, even though it could be of added value.

Second, since there is no real necessity for the microphone, there should be the possibility to remove the microphone or deploy a technical solution which guarantees it cannot be turned on. Although the microphone might assist the car passengers in communicating to the emergency services and reporting their status, 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 disconnected from power through a physical feature of the design, which would only be terminated in the case of a crash or when triggered manually. This feature of the design also should have been regulated in the Regulation. In conclusion, the design of eCall prioritises corporate interests over respecting citizens' fundamental rights. This is logical within the ITS-framework and furthermore an unsurprising outcome of the process that led up to the adoption of the Regulation, yet it is in stark conflict with the Commission's declared stance on fundamental rights.[160]

Addressing the impact of added value services

Convoluting the solution of privacy and liability issues 'related to the provision and sharing of data, and to the deployment of novel safety-enhancing applications and value-adding services'[161] does not help in specifying the problem. In order to address privacy issues adequately these have to be stated accurately prior to relevant solutions being sought. As established in the previous section the Commission mentions 'aspects of security and privacy of data (exchange of data being the core of ITS)', but does not address key questions on how ITS-systems can be designed in a way which effectively protects the right to privacy, namely

[159] Cars nowadays are equipped with sensors in chairs.
[160] See Chapter 4, section 3.1 and 3.2.
[161] SEC (2008) 3083 (n 25) 38.

through motorists control over the data sharing extent and possibly the form of data exchange, e.g. aggregated versus detailed data.[162]

The requirement of necessity plays an important role when data processing happens against the will of the data subject. The thoroughness with which this test should be executed would have to be, in line with the Commission's ambitions, sought in the case law of the ECtHR and CJEU. This would have instructed the Commission officials that there are no such legislative precedents entailing such a grave and sweeping interference with the right to privacy of such a huge amount of people, other than perhaps the legislation on the smart meter. Keeping in mind that this measure would affect everyone using a car and therefore would constitute an interference with the right to privacy on a near-continental scale, the relevant officials could have placed this interference in the light of the effects on society.

In its data protection action plan, the Commission establishes a list of privacy-improving approaches which can have a significant positive effect on the impact of these technologies on the right to privacy.[163] eCall can be used for a number of GNSS related services,[164] which can all be provided over a privacy-friendly 'smart client' solution, in which eCall could play a crucial role by providing the hardware for this solution. One of the most efficient approaches is to install a so-called smart or 'thick client' that allows motorists to use these services without processing detailed information centrally, outside the platform in the car. A thick client allows to only upload the aggregated results to the central server, shielding the detailed data from the outside world.[165] This is also referred to as *distributed* processing.[166] This report by the European Commission, DG Mobility and Transport, was published in October 2012. These highly relevant findings have not resurfaced in the impact assessment accompanying Regulation 2015/758/EU, let alone in the 2013 explanatory memorandum of the proposal. The report even draws an analogy with the smart meter and grid. The EDPS also pressed for added value services to comply with even stricter safeguards with the explicit aim of avoiding function creep.[167] It held the added value services to be more privacy-intrusive, requiring data protection safeguards to be taken into account at the design stage.[168]

Considering the mandatory installation of this in-vehicle platform and the Commission's observations that privacy concerns are the biggest obstacle to a successful uptake of ITS, eCall's design should have been governed strictly by the norms following from data protection and privacy law. The system should have been designed in a way that the interference with fundamental rights is avoided or minimised in line with the right to privacy, data protection law (data minimisation), as well as with the Commission's approach to fundamental rights impact assessments. It is possible that the 'economies of scale' could

[162] ibid 50.
[163] 'ITS Action Plan: ITS & Personal Data Protection' (n 116) 50-110.
[164] GNSS refers to Global Navigation Satellite Systems.
[165] 'ITS Action Plan: ITS & Personal Data Protection' (n 116) 4-5.
[166] ibid.
[167] (EDPS) 29 October 2013 (n 60) 5.
[168] ibid 6.

have locked steps with the ambition of realising 'a fundamental rights culture', if the Commission had actually taken up the challenge of identifying and addressing eCall's and ITS' impact. This could have led to the eCall system processing data in a form that respects motorists' privacy, instead of confronting them with an ICT-variant of a stick-up: 'your car or your private life!'.

4. Privacy and data protection in eCall legislation

Privacy and data protection are addressed in the eCall legislation to a certain extent. The aim of this section is to make an inventory of the provisions and establish if these address the challenges identified in the previous section.

4.1 Privacy and data protection in the ITS Directive and eCall Regulation

In the initial proposal of Directive 2010/40, the Commission addressed privacy and data protection only in a general recital, providing that the processing of personal data in the context of ITS systems needs to comply with Directive 95/46/EC and Directive 2002/58/EC (data protection directives).[169] The EDPS issued an opinion on the proposal emphasising the importance of, inter alia, data minimisation, purpose limitation and anonymisation.[170] The Council added to the general recital on data protection that the processing needed to comply with purpose limitation and data minimisation.[171] The Council, also, added a recital introducing the principle of anonymisation, stating this should be encouraged in order to enhance individuals' privacy.[172] This recital also introduced an obligation for the Commission to consult the EDPS and request an opinion of the Article 29 Working Party whenever privacy and data protection issues arise in the field of ITS. These additions were adopted in the final version of the Directive.[173] The explicit reference to purpose limitation and data minimisation is a step forward, however, it does not guarantee the adequate interpretation and application of these principles to ITS in practice.

Article 10 instructs Member States to ensure the processing is carried out in accordance with Directive 95/46/EC and Directive 2002/58/EC with a focus on protecting data from unlawful access, alteration or loss, i.e. data security. It is also unclear why anonymisation would be merely encouraged. It follows from data protection law that data, where possible, is anonymised. What remained unaffected was the power of the Commission to adopt

[169] This point was also made in the opinion of the EDPS, which noted that it was too broad and general to adequately address the concerns raised by ITS deployment. (OJ 2010 C 47/02) (n 49) para 14.
[170] ibid paras 11-12.
[171] Council, 'Position (EU) No 11/2010 of the Council at first reading with a view to the adoption of a directive of the European Parliament and of the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport'(Adopted by the Council on 10 May 2010 OJ 2010 C 203 E/01) Recital 12.
[172] ibid Recital 13.
[173] Recital 12 Directive 2010/40/EU.

specifications with respect to the deployment of ITS systems, although the final Directive did provide that this power should be exercised through the adoption of delegated acts.[174] In line with the proposal the specifications were to be adopted by ESOs after a request by the Commission, having consulted the EIC. Notably, no substantial demands on the processing of personal data were adopted in the final act and therefore the power of the Commission with respect to technical decisions was not limited.[175]

The eCall Regulation only addresses the design of the 112 system to the extent that it provides for emergency services. Article 6 on rules on privacy and data protection only addresses the 112-based eCall in-vehicle system, which implies it only covers the system to the extent it is used in emergency situations.[176] Article 6(11) which requires that the 112 system will not exchange data with a TPS system or an added value service, is the exception to this rule. In addition, the Regulation contains several recitals and provisions dedicated to data protection legislation (Article 8 of the Charter, Directive 95/46/EC and Directive 2002/58/EC (data protection directives)), addressing a variety of issues.

General obligations are imposed on manufacturers to implement all necessary measures in order to comply with Article 7 and 8 Charter.[177] This is the only reference to the right to privacy in the Regulation. There is an obligation that any processing of personal data by the 112-service has to comply with the data protection directives. This is intended to guarantee eCall is not traceable in its 'normal operational status related to 112 eCall', nor subjected to any constant tracking.[178] This does leave space for constant tracking through the added value services, i.e. outside the normal operational status related to 112 with the consent of the driver of the car. In addition to an obligation for manufacturers to ensure non-traceability,[179] manufacturers need to ensure that the data stored on the internal memory of the 112-system is automatically and continuously removed[180] and that it should not be available outside the 112-system before eCall is triggered.[181] The personal data should only be used in case of a severe accident and be retained for no longer than necessary to handle the emergency situation.[182] The last four paragraphs were added after the initial proposal by the Council at first reading and can be viewed as the application of some of the substantive data protection

[174] Article 7 Directive 2010/40/EU.

[175] This is despite the EDPS indicating that this should be done. This will be further elaborated on in section 5.1.

[176] Article 3(1) Regulation 2015/758/EU: '"112-based eCall in-vehicle system" means an emergency system, comprising in-vehicle equipment and the means to trigger, manage and enact the eCall transmission, that is activated either automatically via in-vehicle sensors or manually, which carries, by means of public mobile wireless communications networks, a minimum set of data and establishes a 112-based audio channel between the occupants of the vehicle and an eCall PSAP'.

[177] Recital 22 Regulation 2015/758/EU.

[178] Article 6(1) and Recital 21 Regulation 2015/758/EU.

[179] Article 6(4) Regulation 2015/758/EU.

[180] Article 6(5) Regulation 2015/758/EU. Except for the last three locations as these are necessary to determine the current location and the direction the vehicle was driving in.

[181] Article 6(6) Regulation 2015/758/EU.

[182] Article 6 (2) and Article 6(3) Regulation 2015/758/EU. These can be seen as expressions of the purpose limitation and data retention principle respectively.

principles, albeit only in relation to the 112 eCall system. Also, there is a list of information that manufacturers are obliged to provide in the owner's manual.[183] This is the implementation of the duty to provide information to the data subject.

Vehicle manufacturers have the duty to integrate technical forms of data protection and have to adhere to the principle of 'privacy by design',[184] when they comply with technical requirements (recital 23). The Regulation does not elaborate on what these instructions entail, or how the manufacturers should comply with these highly abstract demands. Both of these demands seem out of place, since the vehicle manufacturers do not decide on the requirements for the design.[185] These technical requirements fall under the competence of the Commission, which is empowered to adopt delegated acts to establish them.[186] In effect, the instruction to adhere to 'privacy by design' (PbD) is addressed to a party that does not, or at least not fundamentally, decide on the design. Article 6(7) provides that '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'. What the 'appropriate level of privacy protection' is, as well as whose duty it is to embed this technology, remains unclear.

In the last paragraphs of Article 6 the quasi-legislative instructions are established. Paragraph 12 instructs the Commission to adopt delegated acts to establish the detailed technical requirements and test procedures for the rules laid down in paragraph 2, 3 and 11.[187] Paragraph 13 instructs the Commission to make practical arrangements for paragraph 4, 5, 6 and a template for the user information in paragraph 9 through implementing acts.[188]

The legislator has clearly made an effort to address the right to privacy and the protection of personal data in the Regulation, nevertheless, the foreseeable challenges established in section 6.3.2 are not addressed.

4.2 Added value services

Added value services can be activated during the course of regular driving. Its foreseeable impact on the privacy of motorists is therefore significantly larger than that of the 112 eCall

[183] Article 6(9) Regulation 2015/758/EU.
[184] It is not specified what definition of privacy by design is followed.
[185] This is done by European Standardisation Organisations (ESOs).
[186] Recital 27 and Article 5(8) Regulation 2015/758/EU.
[187] Commission Delegated Regulation (EU) 2017/79 of 12 September 2016 establishing detailed technical requirements and test procedures for the EC type-approval of motor vehicles with respect to their 112-based eCall in-vehicles systems, of 112-based in-vehicle separate technical units and components and supplementing and amending Regulation (EU) 2015/758 of the European Parliament and of the Council with regard to the exemptions and applicable standards [2017] OJ L 12/44.
[188] Commission Implementing Regulation (EU) 2017/78 of 15 July 2016 establishing administrative provisions for the EC type-approval of motor vehicles with respect to their 112-based eCall in-vehicle systems and uniform conditions for the implementation of Regulation (EU) 2015/758 of the European Parliament and of the Council with regard to the privacy and data protection of users of such systems [2017] OJ L 12/26.

system, which is only activated in exceptional circumstances. The Regulation, however, does not provide any requirements for the operation of the added value services and essentially leaves the processing of personal data to the market. The open norms in data protection law and the incentives for economic actors to collect personal data are a combination which makes it highly likely that more data will be collected than is actually necessary for these services to be provided.

Article 6(9)(i) provides that a different processing regime applies to the processing for added value services and that the manufacturers have to provide:

> 'any necessary additional information regarding traceability, tracking and processing of personal data in relation to the provision of a TPS eCall and/or other added value services, which shall be subject to explicit consent by the owner and in compliance with Directive 95/46/EC. Particular account shall be taken of the fact that differences may exist between the data processing carried out through the 112-based eCall in-vehicle system and the TPS eCall in-vehicle systems or other added value services.'

In other words, the Regulation implicitly affirms that constant tracking through eCall is possible when the added value services are activated and that processing for these services does not have to be in line with the rules provided by the Regulation. The odd situation motorists find themselves in is that the EU legislature has decided to use statutory force to equip their cars with an in-vehicle platform because it can save lives, but the same legislator does not address the use of the same technologies by third parties. This is disconcerting, keeping in mind that eCall is a corporate effort facilitated in the context of a road safety initiative by the EU, national governments and industry joined together to force this technology upon the 'reluctant consumers'.[189] When motorists make the choice whether or not to use this system, this choice should not be between giving up privacy and using these services, or maintaining privacy and missing out on eCall's benefits. The developments described in section 3.2 (subsection C-ITS) raise the question whether the collection of data is dependent on the activation of the added value services.

5. What is left unsettled: the Commission, ESOs and essential elements of design

The eCall legislation confers delegating and implementing powers to the Commission to set rules with respect to technical requirements for ITS and the eCall system. The ITS Directive confers power to the Commission to adopt delegated acts on the priority actions in which, as discussed in section 2.2, data transmitted by cars (and possibly eCall) could play a vital role. The ITS Directive confers power to the Commission to request ESOs to adopt standards to provide for interoperability, compatibility and continuity for the deployment and operational use of ITS, after consulting the European ITS Committee (EIC), under Directive 98/34/EC

[189] COM (2008) 886 (n 28) 2, 47.

(the former standardisation Directive).[190] The power of the Commission to request ESOs to adopt standards on ITS in general is, therefore, restrained by the constitutional limits of the implementing acts. The eCall Regulation empowers the Commission to adopt delegated acts establishing detailed technical requirements, which in turn are based on an open list of standards.[191] The power of the Commission to request ESOs to adopt standards on the 112 eCall is, hence, restrained by the constitutional limits of the delegated act as set in Article 290 TFEU.

5.1 Instructing the Commission

Article 7 of the ITS Directive authorises the Commission to adopt delegated acts as regards specifications necessary to ensure compatibility, interoperability and continuity for the deployment and operational use of ITS for the priority actions, which includes 'the harmonised provision for an interoperable EU-wide eCall'. The Directive also provides that these specifications will 'where appropriate, be based on any standards referred to in Article 8'.[192] In these delegated regulations the Commission in turn prescribes the use of certain standards, for instance, it instructs Member States with respect to the provision of real-time traffic information services to 'rely on existing technical solutions and standards, provided by the European and international standardisation organisations, such as DATEX II (CEN/TS 16157 and subsequently upgraded versions) and ISO standards'.[193]

The ITS Directive does not establish any rules concerning privacy or data protection for the Commission whilst adopting delegated acts, nor for the issuing of requests to ESOs. The Directive does establish rules on privacy, security and re-use of information, however, these are addressed to the Member States which are not involved in developing eCall's design. Moreover, the rules reflect the data protection light approach which is only concerned with the further processing of data, but not the initial collection. The design is the decisive factor for the amount and nature of the personal data processed and the exploitability of other features of the system which can affect the right to privacy. As a result, it can be suggested that the Commission received a carte blanche from the legislator to issue requests to ESOs on ITS which can have a big impact on cars, transport infrastructure and back-end-systems. This provides the Commission with virtually unfettered power to decide on the materialisation of ubiquitous computing in road transport in EU Member States. This conferral of non-defined power to the Commission is in conflict with the specificity principle. Moreover, as a legal basis to develop ITS-applications and services which will interfere with the right to private life it does not meet the requirement of foreseeability. The absence of instruction with respect to privacy and data protection makes it impossible to determine the scope of and manner in

[190] Article 8 Directive 2010/40/EU.
[191] Article 5(8) Regulation 2015/758/EU.
[192] Article 6 (6) Directive 2010/40/EU.
[193] Recital 11 of Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services [2015] OJ L 157/21.

which the power of the Commission will be exercised. In more formal wording the definition of the power conferred is not 'sufficiently precise, in that it must indicate clearly the limits of the power and must enable the Commission's use of the power to be reviewed by reference to objective criteria fixed by the EU legislature'.[194] The lack of boundaries means that motorists are simply left to the mercy of the Commission. It is hard to imagine how any of the institutions involved might have missed ITS' potential to change the right to privacy and the freedom of movement radically for practically every motorist in the EU. It is surprising that this legislative process, which entails the datafication of the highway and practically all the activity taking place on it, did not raise any questions on the fundamental architectural choices involved.

In the eCall Regulation the Commission is authorised to adopt delegated acts under Article 8 'establishing the detailed technical requirements and test for the EC type-approval vehicles in respect of their 112-based eCall in-vehicle systems and the EC type-approval of 112-based eCall in-vehicle systems, components and separate technical units.'[195] The Regulation also provides that these detailed technical requirements should be based on the relevant standards that relate to eCall and provides five of these ITS standards. These standards include four related to eSafety: pan-European eCall operating requirements; eCall high level application requirements (HLAP); eCall end to end conformance testing. eCall minimum set of data (MSD). The fifth is on eCall operating requirements for third party support. The final standard in Article 5(8)(f) is an open category – 'any additional European standards relating to the eCall system'.

This is quite an exhaustive list of system functionalities, which consist of design features relevant to the impact on the right to privacy. For example, the way the 112 system starts scanning or registering with the public mobile wireless communication networks is defined in the standard on Pan-European eCall operating requirements (EN 16072).[196] So whether the starting of a car equipped with eCall automatically starts the processing of personal data is decided in a standard, rather than an accessible transparent law. Under this provision, the Commission is also granted the power to adopt delegated acts with respect to additional European standards relating to the eCall system.

After comments of the EDPS on the initial proposal of the eCall Regulation which left full discretion to the Commission to further develop privacy requirements, a number of specifications were adopted in the final Regulation. These are mostly addressed to the car manufacturers which do not, or only to a minimal extent, influence the design of eCall. Moreover, these specifications formulated in the eCall Regulation only address the 112 service. This means that the Commission can act practically unrestrained with respect to the development of standards for the added value services, which is the part of eCall that will have the greatest impact on privacy, because it concerns everyday services. In both the ITS

[194] Case C-696/15 *P République Tchèque v Commission* ECLI:EU:C:2017:595, para 49.

[195] Article 5(8) Regulation (EU) 2015/758/EU.

[196] This was written in an e-mail from a senior manager of ERTICO ITS Europe (Europe's Intelligent Transportation System organization that promotes research and defines standards).

Directive and the eCall Regulation, the specificity principle and the requirement of foreseeability are not respected in relation to added value services.

By adopting the standards in the Regulation the technical requirements that follow from them become binding. This shifts their nature from private to public law.[197] Not only is the discretion to decide on essential features of design wrongfully delegated to the Commission, the Regulation assigns statutory power to these documents in which final decisions on eCall's design are drafted in complex technical language which is almost incomprehensible to laymen. What exactly is provided in these standards that could pose a risk to the right to privacy is unknown. The rule of law is further undermined by the fact that these documents and their implications are unavailable to citizens, unless they are willing to pay a substantial fee and get a technical consultant to explain in an accessible manner their practical implications.[198] In sum, these standards fail in several cardinal issues associated with governance – legitimacy, accountability and transparency – and run counter to basic requirements under the rule of law.

5.2 Essential elements of eCall's design

The discretion given to the Commission and ESOs to take decisions on design features interfering with fundamental rights sits uneasily with the underlying rationale of delegated acts. The latter may only supplement or amend *non-essential elements* of the legislative act.[199] Details concerning the functioning of eCall, negatively affecting the right to privacy, cannot be regarded as non-essential elements. There is a wide array of vulnerabilities within eCall's design and features that allow constant tracking, which can be exploited for the purpose of surveillance, serve the interests of public authorities (for instance, tax services and social services) and businesses, while going against the interests of citizens.[200] It is irreconcilable with the rationale of Article 290(1) TFEU to delegate discretionary power to the Commission to decide on features of the design which impact the right to privacy, i.e. the *essential elements of design*. It conflicts with the requirements in Article 290(1) TFEU which codifies the non-delegation doctrine.

[197] See also Robin A Hoenkamp, Adrienne JC de Moor- van Vugt and George B Huitema, 'Law and standards: Safeguarding societal interests in smart grids' in Ronald Leenes and Eleni Kosta (eds), *Bridging distances in technology and regulation* (Wolf Legal Publishers 2013) 117.

[198] See European Standards, 'CSN EN 16072 Intelligent transport systems - ESafety - Pan-European eCall operating requirements' (European Standards 2015) <http://www.en-standard.eu/csn-en-16072-intelligent-transport-systems-esafety-pan-european-ecall-operating-requirements-1/> accessed 17 December 2015.

[199] Article 290(1) TFEU.

[200] Of course, citizens also have an interest in catching criminals, but then again, criminals (as well as foreign intelligence agencies) also can exploit the vulnerabilities of eCall. The platitude 'if you did nothing wrong you have nothing to hide', was already untenable, but Snowden's revelations again exposed how surveillance capabilities are used against people and organisations that exercise their democratic freedoms, like Unicef, Amnesty International, Human Rights Watch and others, yet are subjected to surveillance measures for no clear reason.

The decision of the legislator with respect to essential elements in the legislative act must have its basis in objective factors amenable to judicial review.[201] In its opinion on Directive 2010/40/EU, the EDPS commented on this aspect:

> 'In a democratic society, decisions on essential principles and modalities that impact fundamental rights should be taken within a full legislative procedure, which includes the appropriate checks and balances. In this case, this means that decisions that have a major impact on the privacy and data protection of individuals, such as purposes and modalities of mandatory data processing activities and the definition of modalities for the deployment of ITS in new areas should be decided by European Parliament and Council and not through comitology procedure.'[202]

The EDPS proposed its involvement, together with the Article 29 Working Party, in the work of the Committees.[203] It also held that the design of ITS applications and systems takes place at several stages, in which privacy and data protection should be taken into account; in particular, the Commission and the ITS Committee 'will bear specific initial responsibility in the definition, through the comitology procedure, of measures, standardisation initiatives, procedures and best practices that should promote "privacy by design".'[204] By adopting essential elements in the ITS Directive the legislator could have set strict rules for the Commission to abide by, leaving it limited or no margin of discretion on design-issues affecting fundamental rights.

It should be repeated here that the EDPS insisted on stricter safeguards for the added value services with the explicit aim of avoiding function creep.[205] The EDPS acknowledged that these services would be more privacy-intrusive, and addressed the matter of PbD, requiring data protection safeguards to be taken into account at the design stage.[206] It noted, furthermore, that the potential of eCall for car manufacturers to offer added value services was not addressed in the proposal, which allows the system 'to develop in an unregulated manner, thus creating a legal loophole'.[207] The EDPS, furthermore, emphasised the importance of giving clear and unambiguous consent prior to the use of personal data for added value services.[208] The voluntary activation was held particularly important 'since the provision of facultative added value services by car manufacturers is based on a system that the clients have by default in their cars'.[209] This observation is also relevant for other third parties utilising the system. The EDPS notices that the prohibition on constant tracking only applies to the '112 eCall services and private eCall services', and recommends that the

[201] Case C-355/10 *Parliament v Council* ECLI:EU:C:2012:516.
[202] (OJ 2010 C 47/02) (n 49) para 24.
[203] ibid, para 25. EDPS also addresses private eCall services. These are provided through a private eCall system which functions in parallel to the 112 eCall and is outside the scope of this research.
[204] ibid, para 29.
[205] (EDPS) 29 October 2013 (n 60) 5.
[206] ibid 6.
[207] ibid 6.
[208] This can also be criticised, because the supervisor does not address the collection.
[209] (EDPS) 29 October 2013 (n 60) 7.

proposal should clarify it also apply to added value services.[210] Given this observation it is quite remarkable that the obligation for the car manufacturers in the final version only applies to the '112-based eCall in-vehicle system'.[211] EDPS also observes that third party service providers have to comply with the data minimisation principle.[212]

Parallel to this, the Commission developed food for thought on essential elements in its data protection action plan on ITS, in which numerous ITS services in various countries were assessed providing useful lessons and recommendations for privacy-friendly services.[213] For an important part, these concerned a number of GNSS-related services which could be provided through the eCall system (as already established in section 3.2). If GNSS-related services are provided through a smart or thick client solution, they share only aggregate and not detailed data. This is a privacy-friendly alternative in comparison to a system that would share detailed data. A thick client implies that there is additional hardware. This is a matter of design which requires a choice with respect to the architecture of the system. Bearing in mind the implications of this choice for fundamental rights, it is safe to say that it touches on the essential elements of the eCall Regulation (see section 6.3.2 and 6.4.2). The fact that this was consolidated in a public report from the Commission, supported by opinions of the EDPS, yet absent in the legislation, is a strong indication that the EU institutions failed to live up to their constitutional duties. The lack of attention on the design of the system in the impact assessments and the explanatory memoranda, as well as the fact that privacy concerns were raised by the Article 29 Working Party and recognised in the impact assessment of the ITS Directive in 2008, justifies an assessment of the Commission's approach as wilfully negligent. Once again, a contrast can be seen between the Commission's rhetoric and practice.

The EU legislator has a positive obligation to see to a society in which the right to privacy is respected. If it mandates ICT-systems in citizens' cars under the banner of saving lives, it should ensure that this technology does that in a way that minimises the interference necessary to attain this goal. If the same system mandated under EU law is also used to make a profit through the provision of private services, the duty to design this system in a way which ensures the effective protection of the right to privacy becomes particularly urgent. The fact that the obligation to install this system will affect practically all motorists in the Union gives extra weight to the duty of the legislature to make architectural choices on the design of the system which respect the lesser restrictive means-requirement.

[210] ibid 10.
[211] Article 6(4) Regulation 2015/758/EU.
[212] (EDPS) 29 October 2013 (n 60) 10.
[213] 'ITS Action Plan: ITS & Personal Data Protection' (n 116) 50-110.

5.3 Instructing the ESOs

The Commission plays an important part in the interpretation and application of the right to privacy and data protection in its role as a principal in relation to the ESOs developing European standards. It does so when it assesses the standards, but the most obvious place to start is in the mandate it issues. Here, it can establish the concrete requirements in order to guarantee that the ESOs will respect the right to privacy and data protection legislation. Similar to the smart meter, the ESOs drafted standards after accepting a mandate from the Commission, but in this case the standards have been adopted in the eCall Regulation making the installation of the system compulsory. Four out of five standards referred to in Article 5(8) Regulation 2015/758/EU are 'EN', which stands for 'European Norms'. This means that they have been approved by the Commission following their development upon its request. The document underlying this request is Mandate M/453, issued by the then DG Enterprise and Industry, which aims to support the interoperability of C-ITS systems.[214] eCall is not mentioned in this mandate. It was issued in 2009, long before the obligation to install eCall in cars certified for the EU market became a reality. The mandate does mention that 'ESOs should identify the risks for the privacy of the users of these functionalities and the measures to be taken to eliminate these risks'.[215] Thereby the Commission shifts the task they should have performed in the impact assessment to the ESOs and confers discretion to them in conflict with the non-delegation doctrine. The Commission does not adhere to the approach it advocates with respect to the formulation of safeguards resulting from impact assessments: general safeguards do not suffice, they need to be concrete.[216]

The position of the Commission to set forth these requirements in a mandate is strong with respect to the 112 services, yet in relation to the added value services it is extremely weak due to the absence of requirements in the eCall Regulation. It is unclear why the adoption of the eCall Regulation, obliging the installation of eCall and referring to standards, thus making these technical documents binding, did not lead to a new mandate. The shift to a mandatory regime requires a higher level of involvement from the EU institutions. The fact that the ESOs still base their work on a mandate that was issued before the eCall Regulation was proposed and even before the Lisbon Treaty was signed, and therefore before the Charter became legally binding, raises yet more questions concerning the Commission's dedication to fundamental rights in this policy field.

The Commission could have drawn lessons from its own body of communications that positioned privacy and data protection in ITS as one of the most important policy concerns, from the opinions of EDPS and from its own action plan on personal data which held that technical measures could be taken on the level of components and interfaces in order to

[214] European Commission, 'Standardisation Mandate addressed to CEN, CENELEC and ETSI in the field of Information and Communication Technologies to support the interoperability of Co-operative systems for Intelligent Transport in the European Community'(DG ENTR/D4 M/453 EN , European Union 2009).
[215] ibid.
[216] SEC (2011) 567 (n 111) 18.

secure a privacy-by-design approach.[217] The authors of the action plan struck a careful though sceptical note when they observed that 'optimum provisions for data protection are not always on the top of the minds of all (industry) experts involved in elaborating standards'.[218]

Meanwhile, CEN and ETSI reports show that the Technical Committee especially established for ITS is attended by governmental organisations, industrial stakeholders, telecommunication network operators, mobile industry, as well as communication companies.[219] On the website of the ACEA, which already anticipates the sharing of car data on data server platforms (based on the untenable application of data protection law as not covering the collection of data), the interested parties are indicated. These concern breakdown services, insurance companies, operators of parking garages, financial and fleet service providers, road infrastructure operators, entertainment and travel service providers, social networks and search engine providers.[220] A great number of stakeholders await to profit from the Commission's incompetence. On the receiving end are the motorists who will have to pay for this scheme. In its report on C-ITS, the Commission acknowledged that most costs would probably fall on the shoulders of (reluctant) consumers, while many benefits are to the wider society, whereby the consumers would need certain encouragement to invest in 'safety and health benefits' offered by the C-ITS services.[221] In the EU of tomorrow, motorists are not only forced to surf in the Internet of Things, they are presented the bill for their equipment.

6. Conclusion

For almost fifteen years the Commission has been working steadily towards the uptake of ITS. In the first half of this period, it relied on the proverbial carrot only, but later it increasingly relied on the stick. The struggle with a 'non-obvious business case' had to be brought to a success, despite the 'reluctant consumers' blocking the road to it. This culminated in Regulation 2015/758 obliging every car certified for the EU market to be equipped with the eCall system from the 31st of March 2018. Despite the Commission's claim that it would benefit motorists, the carrot it waved in front of the car manufacturers consisted of motorists' personal data. The mandatory installation of this system is justified under the banner of saving lives, a reduction in the severity of injuries and a decrease in the congestion caused by the accident.[222] Aside from the doubts about the correctness of this

[217] 'ITS Action Plan: ITS & Personal Data Protection' (n 116) 42.
[218] ibid 42.
[219] CEN and ETSI, 'Final joint CEN/ETSI-Progress Report to the European Commission on Mandate M/453' (CEN and ETSI 2013) 14.
[220] See Car data facts, 'Why share car data?' <http://cardatafacts.eu/> accessed 2 February 2018.
[221] European Commission, 'Study on the Deployment of C-ITS in Europe: Final Report' (Framework Contract on Impact Assessment and Evaluation Studies in the Field of Transport MOVE/A3/119-2013-Lot № 5 "Horizontal", DG MOVE 2016).
[222] The estimation is the prevention of 2 500 (6.4% of 39 000) traffic deaths per year, mitigate the consequences of severe accidents in 5850 cases (15% of 39 000), see European Commission, 'Emergency calls: Commission

number, it implies that 8 350 lives per year are directly affected by this measure. This measure affects the privacy of the motorists driving approximately 291 000 000 vehicles on the road.[223] A percentage of 0,002869% of EU's motorists is arguably helped with this measure, whilst it unnecessarily affects the privacy of 100% of them.

The Commission has not addressed the way eCall should function outside of emergencies, whilst it was involved in drafting reports establishing how privacy could be maintained whilst serving other purposes.[224] These omissions demonstrate the Commission's failure to undertake an adequate impact assessment addressing the effective protection of the right to privacy. Moreover, the analysis of various impact assessments bares the fact that the right to privacy is not addressed at all. The Commission limits itself to data security, addressing 'data integrity, confidentiality and availability', ignoring obvious considerations of such substantial requirements as the necessity of the collection.[225] The impact assessments indicate that most challenges to privacy raised by the introduction of eCall have not even been noticed by the Commission. This is surprising since the Commission has not made it a secret that eCall was never considered as a stand-alone application.[226] The impact assessments, however, are perfectly in line with the Commission's *data protection light* approach.

The most interesting aspect of the legal framework resulting from the Commission's approach to privacy, is revealed in its omissions. The eCall system receives a great deal of attention to the extent it serves emergency purposes, but the other functions it will fulfil, within and beyond this legal framework, remain basically unaddressed. This silence is remarkable, given the importance of eCall as a vital enabler to serve a range of government and industry interests, as well as a key enabler for C-ITS. With the ever continuing sophistication of technology, its potential for surveillance will only increase. Despite the fact that the Regulation addresses the right to privacy and the protection of personal data with respect to the emergency eCall, the vast potential for surveillance offered by the system is left uncurbed.

In this respect, one of the main weaknesses identified above is the lack of any specific instructions to the Commission with respect to the design of the mandatory in-vehicle system. The legislator could have made a distinction between the two systems, allowing only the mandatory installation of the emergency system. Alternatively, it could have addressed both the emergency as well as the commercial functions served by the system. It chose neither of the above options. Instead it gave the Commission a carte blanche. The result is that private property becomes equipped with 'public' technology which exposes citizens to the risk of (arbitrary) interference by third parties. One of the few things left to do for citizens,

---

welcomes growing Member State endorsement for eCall in-car system' (IP/ 10/488 Press Release, Brussels, 4 May 2010) <http://europa.eu/rapid/press-release_IP-10-488_en.htm> accessed 7 August 2015.

[223] See ACEA, 'Vehicles in Use' <http://www.acea.be/statistics/tag/category/vehicles-in-use> accessed 9 April 2018.

[224] 'ITS Action Plan: ITS & Personal Data Protection' (n 116).

[225] COM (2008) 886 (n 28) 2, 12.

[226] COM (2008) 887 (n 48). See also COM (2005) 431 (n 19) 2.

involuntarily confronted by the illegitimate outcome of this corporate collaboration, is to hire a specialist technician in order to deactivate the in-vehicle eCall system.[227] In the black market of the criminal world a range of products are offered capable of disturbing signals. Civil disobedience, hence, could also lead to people equipping themselves with these type of devices to protect their privacy.

The architectural choices of eCall appear to have been inspired by corporate motivations which should have no place in legislation that makes these systems mandatory in the public interest. The power of the legislature has been abused as a crowbar to open up a traditionally secluded private sphere in order to install a device which enables mediation between consumer and companies, and creates greater potential for the state to control its citizens. The Regulation thus leaves the impression of an unholy union of state and commercial interests, materialising in the compulsory installation of ICT-systems in the car, trumping the hard-won fundamental principle of freedom from arbitrary interference.

[227] This option is actually mentioned in the 'Data Protection Aspects of eCall' (n 138) 10. The authors of this note notices that there is no prohibition to do such a thing in the proposal of the regulation, but does consider this apt in the face of the obligatory character.

Chapter VII
Conclusion

The right to privacy and data protection legislation

As revealed in the two case studies of this thesis, it is the data protection legislation that the Commission relies on in its policy and rule-making activities on mandatory IoT systems. As established in Chapter 3, data protection legislation can offer guidance in establishing certain safeguards and principles such as data minimisation and purpose limitation which have the potential to prohibit the legislator from equipping these systems with unnecessary surveillance features — what is coined as the prohibitive potential. Data protection law is limited in scope and only offers this potential with regard to features involving the processing of personal data. It is inadequate to address other features of IoT systems, such as actuators and sensors that can be remotely turned on or off. More pressing, however, is the point that data protection law is commonly relied on in transparent relationships which are usually entered into voluntarily.

The transparency requirement follows from a number of data protection rules, such as the duty of the controller to inform the data subject about the processing and the subjective rights (access rights) for the data subject. The mandatory installation of IoT systems in the private sphere of citizens is controversial and politically sensitive as it can take place voluntarily, involuntarily or even unknowingly. Moreover, these systems serve a broad plethora of interests, most of which are at odds with the interests of citizens in informational privacy. The current information society, in which these systems function, is characterised by the opacity of data processing operations. This was, once again, demonstrated by the upheaval caused by the revelations about the collaboration between Facebook and Cambridge Analytica.

Another problem with data protection law is that it leaves the interpretation and application of principles with prohibitive potential to the data controller. Furthermore, data protection law does not apply to ESOs, which are the parties developing the technical rules for IoT systems. A final objection to the excessive reliance on data protection law is that its application is not likely to question the necessity of the initial recording and collection of data by IoT systems. Data protection law, in isolation from the right to privacy, is ill-suited in mediating the conflict-ridden relationship between the legislature and the Commission on the one hand – and in the slipstream of the latter also industry – and the interests of citizens in the effective protection of the right to respect for their private life and home on the other.

The fluidity of the concept of privacy is reflected in the creativity it allows the courts in interpreting and applying it to technological challenges raised by the developments in the information society. Although far from perfect, the right to privacy has been a steady and

reliable source for judicial innovations directed at the protection of citizens against the power of the state or industry. Taking the conflicting interests involved in the architectural choices regarding IoT systems as a starting point, the right to privacy is well-suited to engage in the required mediation of these interests. Moreover, the scope of the right covers all features of IoT systems, those that concern the processing of personal data, but also sensors and actuators that can be controlled remotely.

The analysis of the case law of the ECtHR and the CJEU suggest a number of factors which contribute to the assessment of the severity of the interference, as well as to the impact assessment of the Commission. Three factors are distinguished in this thesis of which the first two concern the processing of personal data only. These are the context of the processing, the nature of the data and the potential future violations. Both the ECtHR and the CJEU have demonstrated to be susceptible to the extent to which a measure facilitates further interferences in the future. This factor can be coined the potential future violations, in which the potential future use of data and systems can be assessed. There lies a duty with the legislature to assess the impact of IoT systems beyond their initial purpose and functioning and critically evaluate what can be, instead of limiting itself to what is. Some of the surveillance features of IoT systems are self-evident, such as the communication of detailed usage of electricity data by smart meters. Others are more complicated to discover as the features seem innocuous at first sight, only to reveal their surveillance and control potential upon closer scrutiny. One example of this is the microphone of eCall which is intended to facilitate communication between the motorist and a PSAP, but which can be used to eavesdrop on conversations in the car. One control feature which requires a high level of understanding of technology is the possibility to use the eCall system to shut down cars at a distance.

The two other factors apply primarily to the processing of personal data and concern the context of the processing and the nature of the data. The context can be helpful in analysing and establishing the relevant factors which determine the severity of the interference caused by the installation of IoT systems. First of all, it is in the nature of the IoT vision that the obligation to install these devices will affect virtually all citizens within the EU. Second, their installation does not take place on the basis of consent. It is a system which penetrates into the private sphere of citizens on the basis of statutory force. Any subsequent surveillance feature these devices are equipped with will be a feature that affects the lives of all citizens. An uncurbed surveillance potential could subject aspects of citizens' private lives to permanent recording and collection of data and basically amount to an obligation to live online, with all the ramifications one can think of. In the Commission's communications on data in the future economy, this data will be used for a multitude of purposes. If the IoT systems discussed in this thesis are used for these purposes it implies that, except for some applications in business relationships, the data is used without consent of the citizens. IoT systems have the potential to animate private spheres and properties and to turn them against inhabitants and users, consequently eroding not just their right to privacy, but their very freedom, or in Brandeis words, their 'personal security'.

A number of requirements follow from the right to privacy. In view of the near-continental implications for the right to privacy related to the architectural choices at hand, the EU legislature enjoys a narrow margin of appreciation when it comes to design features which interfere with the right to private life and the home. The requirement of necessity embedded in the proportionality test – used to establish the lesser restrictive means to attain a goal – should be taken into account already in the first elaborations on system design. This test allows to 'smoke out unacceptable motives' guiding the system's design.[1] It follows from this test that IoT systems should not enable centralised storage of data when the officially stated goal of the installation can be pursued through decentralised storage. By restricting the functions of IoT systems to what is necessary their surveillance and control potential can be adequately addressed. This element of the proportionality test also links to the doctrine of positive obligations where the EU legislature should 'minimise, as far as possible, the interference with these rights, by trying to find alternative solutions and by generally seeking to achieve their aims in the least onerous way as regards human rights'.[2] The reliance on the power of the EU legislature to force the installation of IoT systems in the private sphere, places the burden of responsibility for the avoidance, or alternatively minimisation, of interference(s) following from this, firmly with the EU institutions.[3]

If the interference, or the risk of interference, cannot be avoided in the design, proportionality in the strict sense has to be tested by balancing the interests at stake against the right to privacy. The functions which create (risk of) interferences should have a clear and foreseeable basis in the legislative act introducing the system. Adequate safeguards should be adopted to address, amongst others, risks of abuse. If the exploitation of these functions facilitates mass surveillance practices it is unlikely that the right to privacy will be outbalanced by the interests of other parties. Drawing up extensive laws which would allow these practices does not change this conclusion, as was demonstrated in the judgments of the CJEU on data retention.[4] An IoT data retention regime exposes citizens' lives to arbitrary interferences by public authorities, businesses and malevolent parties. The perspective of the mandatory installation of surveillance equipment, which records and communicates detailed data to a central server where it is mined for a multitude of purposes, compromises the essence of the right to privacy. Even if these purposes are meticulously set out in data protection legislation, it would not change the conclusion that this would affect everybody on an unconditional basis. The rationale of human rights generally and Article 8(2) ECHR particularly takes freedom as the rule and interference as the exception. This requirement follows from the texts of the ECHR and the case law of both courts.[5] The right to privacy is

[1] Eva Brems and Laurens Lavrysen, '"Don't Use a Sledgehammer to Crack a Nut": Less Restrictive Means in the Case Law of the European Court of Human Rights' [2015] 15/1 HRLRev 139, 143.

[2] Hatton and Others v The United Kingdom Application no. 36022/97 (ECtHR 2 October 2001) para 86.

[3] This is also consistent with other case law from the ECtHR. See López Ostra v Spain App no 16798/90 (ECtHR, 9 December 1994) para 55.

[4] Joined cases C-203/15 and C-698/15 Tele2 Sverige EU:C:2016:970.

[5] Article 8(2) ECHR explicitly mentions the exceptional character of the interference. 'There shall be no interference (…) except such as is (…).This requirement was also confirmed by the CJEU in Tele2 Sverige,

the rule, the interference should be the exception. The mandatory installation of IoT systems recording and retaining data indiscriminately turns the interference into the rule.

Both the right to privacy and data protection legislation work with the notion of necessity and offer requirements which can be used address the surveillance potential of IoT systems. Moreover, they can complement each other as is demonstrated in the case law of both the CJEU as well as the ECtHR. Data protection legislation, however, does not address the control potential of these systems. Together these rights, taken seriously, could inform an IoT policy in which architectural choices are taken by the legislature with their protection as a priority.

The conflicting roles of the Commission

One of the problems of the Commission's role in the IoT policy and rule-making process lies in its performance of two, at times irreconcilable, roles. On the one hand, the Commission is a policy entrepreneur which brings together public and private parties in the policy fields pertaining to the mandatory systems, in order to align their respective interests and contribute to the establishment and the functioning of the digital single market. In this process, the Commission is sensitive to the wishes of the more powerful parties, because it is dependent upon them for the success of the policy it formulates. Such dependency puts it in a difficult position with regard to its second role, that of the guardian of fundamental rights. There, the Commission must see to the effective protection of fundamental rights in its communications, legislative proposals and quasi-legislative activities. In this role, taking fundamental rights seriously is likely to lead to conflicts with its policy partners.

In the pre-legislative phase the Commission's ambivalence helps to explain why it focuses in its communications on data protection law, whilst meaningful considerations on the right to privacy are absent.[6] Data protection legislation is elaborated on, but the prohibitive potential of data protection legislation is not discussed. The contours that become visible in these documents is one in which data security and procedural rules on the use of data are prominent, which results in what one might view as the Commission's *data protection-light* approach. One returning phenomenon in these documents is the use of data on a mass scale for multitude of purposes, including those conflicting with the interests of citizens, implicitly rejecting the principle of purpose limitation. This amounts to a radical departure from the original conception of data protection, discarding the legal fundament without which the processing of personal data cannot be justified.

The stakeholders the Commission is involved with in its role as executive governing IoT-policy are typically either economic operators or public authorities that have an interest in the recording and dissemination of data by (mandatory) IoT systems and, thus, a loose

---

where it held that a legal basis which allows restrictions on the scope of a fundamental right should be interpreted strictly and cannot allow the exception to become the rule. Tele2 Sverige and Watson (n 4) para 89.

[6] See Chapter 4, section 2.

interpretation of privacy and data protection legislation. A strict interpretation and application implies that the personal data processed is limited to the strict minimum necessary to attain the stated policy goal. This would be energy efficiency in the case of smart meters and road safety in the case of eCall. Such limitation of the personal data processed implies the reduction of commercial stakeholders' incentive to participate and cooperate in the implementation of this policy. For the Commission the loose interpretation and application of privacy and data protection law is conducive towards realising concrete policy goals; it is even likely to contribute to building closer ties with its policy partners. This helps to explain the contradiction between the Commission's rhetoric on its supposed quest for the most effective protection of fundamental rights, and the data protection-light approach that it takes in its policy and rule-making activities regarding smart meters and eCall.

In the legislative phase, the Commission interprets and applies the right to privacy and data protection at various points, the most important of which is the impact assessment. One of the aims of this assessment is to establish the impact on fundamental rights, already in the early stages of the development of a proposal. The next step is to address this impact accordingly, in line with the case law of the CJEU and ECtHR, ultimately leading to a proposal which respects the Charter of Fundamental Rights. The impact assessment in theory provides the fundamental rights groundwork for a legislative proposal. The Commission produced a rich body of communications, reports and guidelines in which it has taken an ambitious approach to the protection of fundamental rights, where in its own words the EU should fulfil an exemplary role by making the Charter rights 'as effective as possible'.[7]

Even though such a systematic and pragmatic approach should be welcomed, a number of pitfalls have been identified. First, in the impact assessment the legislative act will be taken as a starting point to assess the IoT system. This allows the Commission officials to sidestep difficult questions that might be raised if the assessment included unforeseen scenarios in which these systems can be used. Potential privacy violations which consist of the secondary use of IoT systems should be part of the impact assessment. Second, the execution of this impact assessment takes place after the Commission has mapped out the policy and established its main features. Moreover, the extent to which the impact assessment will recognise design choices for IoT systems as a matter of fundamental rights is dependent upon the Commission employees' conception of fundamental rights, which in turn is likely to be affected by the data protection-light rhetoric, which appears to be ever-present in the Commission's communications. This raises the question whether the impact assessment allows for genuine proofing of fundamental rights, or is it destined to be a mere box-ticking activity.

There is another pitfall which is linked with the quasi-legislative phase. The focus of the impact assessment is on the main legislative act, while the sting can be in the delegated or implementing acts. Here, the ESOs at the request of the Commission develop technical rules the system should abide by. The probability that these rules will amount to violations of the

[7] Commission, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'(Communication from the Commission) COM (2010) 573 final 3.

right to privacy increases if the Commission does not set boundaries in its request. There are two constitutional limits for the legislature. There is the non-delegation doctrine which instructs the Commission when it adopts 'non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act' and that 'the essential elements of the area shall be reserved for the legislative act'.[8] This imposes a duty on the Commission to refrain from adopting delegated acts which contain essential elements. What qualifies as essential is not merely subjective and, according to the CJEU, it also depends upon 'objective factors amenable to judicial review'.[9] The CJEU established two such factors consisting in political choices for the legislature and when decisions concern fundamental rights.[10] These factors link the competence of the Commission in the quasi-legislative phase back to the ultimate aim of the impact assessment: to guarantee that the legislative proposal respects the Charter. In order to pursue the most effective protection of the rights enshrined in the Charter the Commission should propose rules in the legislative act setting the limits for its own work in the quasi-legislative phase. These rules can also contribute to the EU legislature acting in line with the second constitutional limit, the specificity principle, which provides that the 'objectives, content, scope and duration of the delegated power shall be explicitly defined in the legislative acts'. The legislature has a duty — stemming from the specificity principle and the non-delegation doctrine — to take the essential elements of the act into account whilst defining the details of the power conferred on the Commission. The definition of the conferred powers needs to take into account the interferences as well as risk of interferences with the right to privacy posed by the installation of the IoT system. It should also ensure that the requirements following from the Charter are respected. This is also in line with the foreseeability requirement. The legislature has the duty to set the *essential elements of design*. These contain the type and content of safeguards addressing the elements of IoT system design which can negatively impact fundamental rights and which concern opposing interests between industry and citizens. This duty for the legislature can be seen as the hinge between the role of the Commission in the impact assessment and the role of the Commission in the quasi-legislative phase. Ideally, the impact assessment would prepare the ground for the legislature and assist it in establishing the essential elements of IoT system design in the legislative act, adequately addressing the surveillance and control potential of the system and ensuring the effective protection of the right to privacy. If the impact assessment does not establish any impact on fundamental rights, it is unlikely that the EU legislature will identify a problem in provisions on implementing and delegated powers in the legislative proposal. This gives rise to the same criticism raised above with respect to the impact assessment: the work of the Commission builds on its misconception of data protection.

If these elements are not set in the legislative act and this silence is perpetuated in the mandate the Commission issues to ESOs, this mandate will not set limits with respect to

[8] This duty also applies to the implementing acts. See Chapter 4, section 4.1.

[9] C-355/10 Parliament v Council EU:C:2012:516, paras 67, 68.

[10] Ibid para 77. Maarten den Heijer and Eljalill Tauschinsky, 'Where Human Rights Meet Administrative Law: Essential Elements and Limits to Delegation' (2013) 9 European Constitutional Law Review 513, 519.

fundamental rights which have to be respected whilst drafting the standards. This mandate is in fact a contract and the Commission failing to address respect for fundamental rights in this capacity means its bargaining away Europe's hard-won human rights heritage. This would mean private parties enjoy discretion on essential elements of the legislative act, involving architectural decisions on the surveillance and control potential of the system. Thereby, it should be kept in mind that the constituency of ESOs consists of representatives of a profit-driven industry with an interest in personal data as an economic asset. It is, however, unlikely for the Commission to adopt requirements in the mandate if these are absent in the main legislative act. Even if the Commission adopted them, the ESOs could refuse to accept the mandate.[11] The legal status of a mandate is a contract, which is more accurately defined as a 'request' in the Standardisation Regulation, and ESOs are free to refuse this. The formal discretion of the Commission to determine the requirements and policy objectives, thus, finds its limits in its dependency on the ESOs in fulfilling their task.[12] ESOs have a monopoly position and can simply veto requirements viewed as too strict and which do not follow from the legislative act. Setting out the requirements in the legislative act provides the Commission with a clear framework for its mandate and a strong position within the negotiation process with the ESOs.

Officially the Commission oversees the development of the standard, however, commentators criticise the Commission for lacking expertise, resources and willingness to attend the meetings of the ESOs as observers.[13] There is a gap between the expertise of the Commission compared to that of the ESOs, which is even wider in relation to the EP and the Council. Problems born out of this expertise asymmetry in this principal-agent relationship are agency shirking and slippage.[14] Agency shirking refers to the behaviour of the agent, in this case the ESOs and their lack of effort to meet requirements which do not serve their interests. Agency slippage refers to the principal, in this case the Commission and its inability to effectively see to the ESOs meeting the requirements. The Commission's dependence on the ESOs and its lack of expertise, resources and willingness undermine its ambition to guard the effective protection of fundamental rights in the case of smart meters and eCall.

[11] Article 10(3) of Council Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council [2012] OJ L 316/12.

[12] Christian Frankel and Erik Højberg, 'The constitution of a transnational policy field: negotiating the EU internal market for products' (2007) 14 Journal of European Public Policy 108, 109.

[13] Harm Schepel, The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets (1st edition, Hart Publishing 2005) 243.

[14] Michelle Egan, 'Regulatory strategies, delegation and European market integration' (1998) 5 Journal of European Public Policy 485, 489.

The case study of the smart meter and the eCall system

The case studies into the mandatory IoT systems followed a somewhat divergent approach due to the particularities of both cases.

The policy and rule-making process regarding the functionalities of the smart meter consisted of negotiations between the Commission and Member State representatives responsible for energy. There are no traces of any deliberations on fundamental rights, or data protection law, in the document in which the privacy infringing functions of smart meters were established.[15] Directive 2012/27 does not provide any privacy infringing functions, and inferring these functions from the Directive requires adequate knowledge of the policy field and extensive further analysis. The technical description of the functions, in any case, cannot satisfy the standards of foreseeability which follow from ECtHR case law. This, in turn, also reveals that the EU legislature's approach on the smart meter legislation violates the specificity principle.

The silence on privacy infringing functions in the energy directives can be explained by the Commission not conceiving them as such. This is also evidenced in the explanatory memoranda of Directive 2006/32/EC, Directive 2009/72/EC and Directive 2012/27/EU, which share a common characteristic: not a single word is dedicated to either fundamental rights or data protection legislation. The groundwork for this awkward silence was laid in the impact assessments executed prior to the proposal of Directive 2009/72/EC and Directive 2012/27/EU: neither of them addressed the right to privacy or data protection law. The awkwardness of this silence increased by the fact that both the Article 29 WP and the EG2 have highlighted the importance of architectural choices of smart meter design, in particular the choice between centralised and decentralised storage of detailed data, where both recommended decentralised storage.[16] The Commission has ignored these recommendations and has not justified its choice for centralised storage, despite the apparent conflict with its proclaimed fundamental rights ambitions. The preference for centralised storage is at odds with the availability of lesser restrictive means, which is a requirement unequivocally following from both the right to privacy and data protection legislation separate and in conjunction. The Commission's choice goes against the imperative of the fundamental rights framework. Moreover, the recognition that these architectural choices concern the essential elements of the area reserved for the legislature would force it to defer this choice back to the Council and EP.

The need to make fundamental choices has also been ignored by the Commission in the mandate it offered to the ESOs indicating only that data protection deliverables should take into account applicable legal requirements concerning the confidentiality of personal data

[15] EU Commission Information Society and Media Directorate-General and Energy Directorate-General, 'A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the Smart Meter' (Full Report, The Publications Office of the European Union 2011).
[16] See Chapter 5.

protected under Directive 95/46/EC and Directive 2002/58/EC'. [17] The focus on confidentiality as a form of data security confirms the Commission's neglect of principles with prohibitive potential, the application of which could lead to the minimising of collection and storage on the meter, thus, facilitating informational control of meter holders, i.e. the citizens. By remaining silent on these issues, the Commission effectively leaves space to ESOs to take decisions with fundamental implications for power relations between households on the one side and government and industry on the other. The Commission's silence is understandable if the smart meter architecture is viewed through the prism of data protection-light. If one, however, looks at it through the lens of ECtHR and CJEU case law it becomes clear that the design choices for the smart meter can be considered an historical error with implications for the entire EU. The intrusive potential which follows from the monitoring and controlling features of the smart meter strikes at the heart of personal freedom and permanently breaches the right to respect for the home that is fundamental to people's personal security and well-being.

If the European roads are transformed into an internet of things, than the eCall system is what the Commission aims to tag cars with in order to make motorists surf in this new technological paradigm. In four consecutive communications the Commission, hinted at the mandatory introduction of eCall in various forms: the possibilities to adopt legislation mandating 'advanced safety systems';[18] 'in case the eCall roll-out fails [the Commission is] to (…) consider further measures';[19] if the automotive industry failed to accept a 'voluntary agreement of introducing an eCall in-vehicle device [the Commission will] propose further measures'[20] and 'setting up a regulatory framework for deploying eCall'.[21] This sheds new light on the Commission's carrot and stick tactics, in which it demonstrated its willingness to beat the mule into eating the carrot. Despite its own findings that industry struggled 'with a non-obvious business case and reluctant consumers' and the public sector was 'not (or not sufficiently) aware of the potential of ITS to help achieve policy objectives', [22] the

[17] Commission, 'Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability' (Enterprise and Industry Directorate-General , Consultation date: 21 January 2009) M/441 EN.

[18] Commission, 'Information and Communications Technologies for Safe and Intelligent Vehicles' (Communication from the Commission to the Council and the European Parliament) COM (2003) 542 final 13.

[19] Commission, 'The 2nd eSafety Communication: Bringing eCall to Citizens' (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions) COM (2005) 431 final 10.

[20] Commission, 'Bringing eCall back on track – Action Plan (3rd eSafety Communication)' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2006) 723 final 8-9.

[21] Commission, 'eCall: Time for Deployment' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2009) 434 final 3.

[22] Commission, 'Impact Assessment accompanying the Communication from the Commission Action plan for the deployment of Intelligent Transport Systems in Europe and the Proposal for a Directive of the European Parliament and of the Council lying down the Framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes' (Commission Staff Working Document) SEC (2008) 3083, 47.

Commission displayed great tenacity in realising the adoption of eCall, either voluntary or compulsory. The interests of the stakeholders involved and the variety of purposes pursued by the installation of eCall raise the question what the implications of these envisioned applications are for the design of the mandatory system. The majority of these applications do not fall under the purpose of safety used to justify the mandatory installation, yet they do influence the design of the system that is forced into the cars of all citizens.

This lack of clarity surrounding the purposes served by the installation of eCall and the system's relation to ITS, is perpetuated in the ITS Directive and the eCall Regulation. The ITS Directive introduced 'the harmonised provision for an interoperable EU-wide eCall' as a priority action, without a definition of the system.[23] The five delegated regulations which were adopted on the basis of this Directive and included matters such as the 'EU-wide real-time traffic information services' do raise questions if, and if so, how these relate to the functioning of eCall. The eCall Regulation introduces seven distinct terms for eCall-services and six distinct terms for eCall-systems, without any of these recurring in the definitions. The result is that this regulation is as puzzling to read as a pirates' treasure map and that the implications are hard to grasp for a layman. The eCall Regulation does define the '112-based eCall in-vehicle system' as an 'emergency system, comprising in-vehicle equipment and the means to trigger, manage and enact the eCall transmission' and the 'eCall' as an in-vehicle emergency call to 112'. The obligation to install eCall is linked to its emergency-related function as opposed to the added value services that build on it.[24] Added value services and the open-access platform are introduced in Recital 15, yet there are no further provisions elaborating on how they relate to the 112 system. Definitions of added value services and the 'open-access platform' are not provided. The text of the Regulation also remains silent on definitions for added value services and 'future in-vehicle applications and services'. A legal vacuum is, thus, created with respect to these services and the functioning of the mandatory in-vehicle system. Such silence is staggering in the face of the potential extreme consequences outside emergency situations. The use of eCall in emergency situations, in the hypothetical scenario that all cars are already equipped with it, directly concerns only 0,002869% of EU motorists, in contrast to the system's potential for secondary use which can affect all motorists.[25] This silence cloaks the fact that secondary use of a system which is forced into private property under the banner of saving lives, for a plethora of interests which do not necessarily align with the owner of the vehicle, is politically controversial, legally questionable and morally loose.

The impact assessments accompanying the ITS Directive, the eCall Recommendation and the eCall Regulation demonstrate how the Commission continues its quest for the effective protection of the right to privacy by viewing it through the prism of data protection-light. The one paragraph on fundamental rights that is fumbled in the impact assessment of the ITS Directive, states that attention will be paid to individual privacy. No strands of thought from

[23] Article 3(d) Directive 2010/40/EU.
[24] Article 3(1)(2) Regulation 2015/758/EU.
[25] See Chapter 6.

the case law of the CJEU and ECtHR are to be found, however, which explains that the initial recording and collection of data are not recognised as an interference and subsequently not tested against the requirements which follow from Article 52 Charter. Privacy and data protection are commonly addressed in terms of 'data security, privacy and liability', and elaborations on these categories are devoid of any substantive reasoning. The impact assessments are silent on architectural choices with implications for fundamental rights. Before any useful assessment of the necessity of eCall or its design can take place, the problem the system is supposed to solve should first be established. Even this task, which is the first concern in the execution of the impact assessment, is not performed properly by the Commission. The Commission frames the problem as the slow and fragmented uptake of ITS, whilst ITS is an umbrella term for almost everything involving ICT and cars.[26] This does not qualify as a well-described problem. An accurate description of the problem is essential within the fundamental rights impact assessment in order to establish if and to what extent an interference with fundamental rights is justified, as a precondition for setting objectives and considering different policy options, as well as for outlining safeguards mitigating the impact on fundamental rights. Testing proportionality requires the assessment of the relation between the ends and the means. If the Commission wishes to be faithful to its own fundamental rights policy declaration, at the very least it should clearly identify the ends for which it proposes certain measures. It is unfortunate that there is no acknowledgement by the Commission of the great potential for fundamental rights violations. The lack of attention to the design of the system in the impact assessments and the explanatory memoranda, given the privacy concerns raised by the Article 29 Working Party and recognised in the impact assessment of the ITS Directive in 2008, qualifies the Commission's approach as wilfully negligent. Once again, a contrast can be seen between the Commission's rhetoric and practice.

The (risks of) interferences with the right to private life raised by the eCall system can be divided into two categories. There is the exploitability of its communication technologies, sensors and actuators, which allow for targeted interferences, such as eavesdropping and remotely shutting down the car.[27] The biggest (risks of) interferences, however, follow from the ambition to use the 112 system to provide added value services. The Commission identified privacy threats following from these services, such as unauthorised access to personal data, re-use of personal data beyond the legally defined purpose and excessive processing.[28] Re-use for a legally defined purpose, nonetheless, might just as well pose a threat to motorists' privacy. More troublesome is the envisioned use described in the latest Commission report and announced on the ACEA website.[29] The claims made in this report suggest that data protection law only applies to the use of data and not to the initial collection. Although demonstrably wrong, this application of data protection law is not out of tune with the interpretation and application of data protection legislation by the Commission, as

[26] SEC (2008) 3083 (n 22) 12.

[27] Council of the European Union, 'ENLETS Work programme 2014-2020: European Network of Law Enforcement Technology Services' (Doc 17365/13, The Publications Office of the European Union 2013) 5.

[28] Stefan Eisses, Tom van de Ven and Alexandre Fievée, 'ITS Action Plan: ITS & Personal Data Protection' (Final Report, European Commission DG Mobility and Transport 2012) 6.

[29] See <http://cardatafacts.eu/> accessed 7 June 2018.

analysed in this research. The failure to question the necessity of the initial recording and collection of data by the IoT systems is typical of the Commission's approach, even though this approach is usually not made explicit. This can be explained by the fact that this report carries a Commission stamp, but was prepared by TRL. This demonstrates in unearthing terms what the Commission meant when it indicated that automotive industry was interested in eCall as a 'platform to offer added value services to boost their business'.[30]

Both the ITS Directive and the eCall Regulation confer powers to the Commission, without instructions on privacy or data protection. The ITS Directive establishes 'Rules on privacy, security and re-use of information' for Member States. These rules, however, mainly concern the duty for Member States to protect data against unlawful access, alteration or loss, i.e. data security. The eCall Regulation only addresses car manufacturers, not the Commission. Moreover, the instructions contain referral to principles without specifying or applying them. In both the ITS Directive and the eCall Regulation, the specificity principle and the requirement of foreseeability are not respected in relation to added value services. The decisions taken by the Commission and the standards developed by ESOs have implications for the respect for the right to privacy and the protection of personal data and, as such, concern essential elements which are the preserve of the EU legislature. This point has also been stressed by the EDPS.[31] Despite recommendations of the EDPS and the DG Mobility and Transport on the potential for PETs to shield privacy of motorists, similar to the solutions proposed by Jacobs,[32] there is no trace of a follow-up on this issue by the Commission. The EDPS's warnings that the silence on added value services would result in the creation of a 'legal loophole' fell on deaf ears.

The link between the mandate and the relevant legislative requirements established in the Standardisation Regulation is absent. Mandate M/453 was issued in 2009, long before the drafting of the eCall Regulation, but just one and a half month following the Commission communication 'eCall: Time for Deployment'. eCall is not mentioned in this mandate. It was aimed at supporting the interoperability of C-ITS systems.[33] The standards were developed on the basis of this mandate and were subsequently adopted in the eCall Regulation. Thereby these documents attained statutory power,[34] yet these documents can only be accessed after paying a substantial fee. Furthermore, they are written in complex technical language almost incomprehensible to a layman. In short, the adoption of these standards significantly undermines the rule of law in the EU.

[30] COM (2009) 434 (n 21) 6.

[31] EDPS 2010, C 47/10, para 24.

[32] Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth and others (eds), *Data Protection in a Profiled World* (Springer 2010) 291.

[33] European Commission, 'Standardisation Mandate addressed to CEN, CENELEC and ETSI in the field of Information and Communication Technologies to support the interoperability of Co-operative systems for Intelligent Transport in the European Community'(DG ENTR/D4 M/453 EN , European Union 2009).

[34] This can be compared to smart grids: Robin A Hoenkamp, Adrienne JC de Moor- van Vugt and George B Huitema,'Law and standards: Safeguarding societal interests in smart grids' in Ronald Leenes and Eleni Kosta (ed), Bridging distances in technology and regulation (Wolf Legal Publishers 2013) 117.

Analysis of eCall policy exposes a public-private effort to transform private cars into beacons of personal data which are subsequently utilised for the good of government and commerce. Statutory force has been used as a crowbar to install a system which serves a corporate agenda, leaving the impression of an unholy union of governmental and commercial interests.

Concluding thoughts

Freedom and autonomy are two important values protected by the right to privacy. Data protection legislation is sometimes compared with environmental law, because it seeks to remedy the harmful external effects of the processing of personal data. Data was described in the Economist as 'the new oil' comparing data centres to drill platforms.[35] Data can be seen as a new raw material for the functioning of a variety of processes. The more personal this data is the more extensive is the 'pollution' that follows from it. Only the 'pollution' here consists in the negative external effects of data processing on the liberty and autonomy of the people concerned. The data centres depend on raw material to perform their operations on. The mandatory IoT systems can be seen as drill platforms which drill for data. The difference between a system that respects privacy and one that does not is a difference between a system harming freedom and autonomy and one that does not do so.

This difference in harm needs to be multiplied by the number of systems that are installed across the EU. Although impossible to express in numbers, it gives an idea of the implications at stake for the architectural choices at hand. These implications are not recognised in any of the documents produced by the Commission in the course of the policies and legislation assessed in this thesis. Invoking the right to privacy allows challenging the compulsory installation of invasive devices in ones' private environment. It also demands a critical evaluation of the necessity of the introduction of such technologies and a balancing of the rights and interests at stake. No such evaluation has been conducted. Moreover, the Commission has failed to state the exact problem it seeks to solve through the deployment of the relevant systems.

How did the Commission succeed in brushing of the responsibility it took upon with much bravado, even claiming that the post-Lisbon status of the Charter would result in a 'fundamental rights reflex' in its departments responsible for drawing up proposals and acts?[36] How can the Commission justify the fact it does not even recognise that the mandatory installation of smart meters and eCall is a fundamental rights issue? The answer lies in the data protection-light approach it takes to privacy concerns. With this approach the Commission neglects all rules which have a prohibitive potential and shifts the focus to the sharing of data according to a set of rules, rather than preventing the latter or putting the data subject in control. The Commission pays lip service to data protection and privacy, but it

[35] 'Data is giving rise to a new economy' (Economist, 6 May 2017) <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> accessed 7 June 2018.

[36] COM (2010) 573 (n 7).

stays silent on rules that would get in the way of the data processing schemes of the stakeholders involved in IoT policy. The data protection-light approach is the foundation on which the Commission constructs data protection issues in all phases of policy and rule-making and allows it to reduce human rights concerns to easy to digest technical issues for the major stakeholders involved. The Commission uses the language of data protection to justify data dispossession.

Decisions about system design take place outside the democratic arena without meaningful oversight in a homogeneous environment of technical experts serving the business community and overzealous public servants seeking to expand the governmental sphere of influence. These decisions are inspired by a mix of government and commercial considerations that benefit the few, while its potential drawbacks concern all citizens in EU Member States. The mandatory installation of invasive IoT systems is presented as the solution to a range of societal issues. This narrative follows the narrow interests of these few powerful well-organised groups and is founded on a monistic materialist view of society lacking a critical review of the IoT systems and their effects. The stakeholders they represent reap the benefits from the data drilled by IoT systems leaving citizens bereft of their privacy and freedom. This will increase the a-symmetry already present in the power relations in which they are deployed. IoT policy in which certain private aspects of everyday life are subjected to an intense surveillance regime mark the departure from the founding values of the EU.[37] Democracy means respect for a pluralist society and the imposition of this monistic view on society goes against the very nature of this distinctive feature of the European project. Pluralist society will not be respected by applying 'data protection principles in the private sphere'.[38] IoT policy, unchallenged by the right to privacy, will transform the environment of every citizen in the EU into a modern-day panopticon. 'Every object the individual uses…will create a detailed digital record', which will subsequently be used in big data projects to increase the productivity of 'public security efforts'.[39] The citizens of the EU are sleepwalking into a society Mark Weiser warned about: one that will 'make totalitarianism up to now seem like sheerest anarchy'.[40]

If architecture is politics, then the politics of the Commission in policy and rule-making is one of orchestrated silence on the fundamental architectural decisions at stake. In this silence decisions on IoT systems are shaped unrestricted by fundamental rights. The Commission's approach leads to the default recording, collection and retention of data which is generated in the course of the use of electricity or driving a car, as well as the introduction of a range of

[37] Alan F Westin, Privacy and Freedom (New York, Atheneum 1970) 23. He noted attacking the right to privacy is something which is characteristic for both fascism and communism.

[38] Council of the European Union, 'The Stockholm Programme – An open and secure Europe serving and protecting the citizens' (2009) Brussels <https://ec.europa.eu/anti-trafficking/eu-policy/stockholm-programme-open-and-secure-europe-serving-and-protecting-citizens-0_en > accessed 7 June 2018 18.

[39] Future Group, 'Public Security and Technology in Europe: Moving Forward' (Concept paper on the European strategy to transform Public security organisations in a Connected World, Portugal 2007) <http://bit.ly/PqvWIJ> accessed 17 August 2012 8.

[40] Mark Weiser, The Computer for the 21st Century (Scientific American 1991) 25.

vulnerable sensors which can be exploited and turned against citizens. A standard data dispossession regime on these aspects of citizens' lives is the exact opposite of what one would understand as the effective protection of the right to privacy. The collection of data does not serve the right to privacy, especially not if this collection is followed by central storage on servers outside the control of the data subject. The Commission received from internal as well as external sources, time and again, information on how to design both the smart meter and eCall in ways that would respect the right to privacy. It has wilfully ignored this input, leading to a legal vacuum in which architectural choices follow the logic of data dispossession-by-design.

The Commission, of all parties involved, is best placed to turn this development around. It must secure full respect for the right to privacy in pursuance to IoT policy in all its facets if it sincerely desires to stop contributing to the furnishing of its Member States with a technological infrastructure which can be turned into a national or transnational surveillance tool. The Commission plays an important role throughout the policy and rule-making process in which it has the power and duty to guard the fundamental right to privacy. The involuntary systematic recording and collection of data falls under the scope of the right to private life as confirmed in the case law of the ECtHR and the CJEU. The recording and collection of data also falls under data protection legislation as attested to in the GDPR. The rules stemming from Article 7, 8 and 52 of the Charter, as well as the GDPR impose a duty on the legislature to consider the architectural choices at stake. Remaining silent on the architecture of IoT systems and providing merely vague instructions do not meet the specificity principle or the requirement of foreseeability. The architectural choices of the legislature should be guided by the proportionality principle. The relationship between the architectural choices and the surveillance and control potential which can be exploited against citizens, make the application of the necessity test of particular importance: in the context of mandatory IoT systems it allows to 'smoke out unacceptable motives'.[41] A correct application of the proportionality principle, in which the societal implications of the forced installation of IoT systems are taken into consideration, demands that the pursued design avoids or minimises the (risks to) interference with the right to privacy. These choices should ideally result in architectural safeguards which secure the respect for the right to private life and the home and prevent third parties from arbitrarily interfering with citizens' lives. These architectural safeguards can be considered essential elements of design and should have been established by the Commission in the impact assessments prior to the legislative proposal on smart meters and eCall. These essential elements should be adopted in the proposal, and it should be clear for the Council and the EP what is at stake before the relevant legislation is passed. The legislature might then decide against the mandatory nature of the installation.

The architecture of IoT systems should concern all relevant EU institutions if democracy and fundamental rights are not mere slogans in the EU. Deploying surveillance devices on a massive scale which provide public access to private data is typical for totalitarian regimes to

[41] Brems and Lavrysen (n 1) 147.

which the ECHR was a reaction in the first place.[42] This is not to say that the parties which support an all-pervasive vision of the IoT have any political aspirations as such. Totalitarian regimes, nevertheless, share traits with corporations in their attempt to impose a certain vision against people's will, to the extent that they seek to control the feelings, desires and opinions of their respective citizens and customers.[43] The Commission's rhetoric on the importance of privacy and trust for the uptake of the IoT deserves severe criticism given the silent imposition of these systems. The obligation to take on IoT in one's private sphere bears striking similarity with the features going against the essence of democratic justice as conceived by Shapiro: 'it is unnecessary, it is not usually entered into voluntarily, it is hard or impossible to escape, it is both a-symmetrical and non-self-liquidating, and it has effects that permeate through the social world.'[44] The phenomenon he described was slavery.

Ultimately, the answer to be given to the question how the Commission interprets and applies the right to privacy in the policy and rule-making process concerning IoT systems is fairly short. It does not.

[42] Alan F Westin, Privacy and Freedom (New York, Atheneum 1970) 23.
[43] John Dewey, Freedom and culture (London, George Allen and Unwin Ltd 1940) 10.
[44] Ian Shapiro, Democratic Justice (Yale University Press, 1999) 46.

Samenvatting

In 2009 lanceerde de Europese Commissie het actieplan voor het Internet van Dingen (hierna het 'IvD'). Om de bijdrage van netwerktechnologieën aan de maatschappij te optimaliseren moeten we van een netwerk van computers naar een netwerk van 'onderling gekoppelde objecten', aldus de Commissie. Dit zou de levenskwaliteit van burgers, werkgelegenheid, de creatie van bedrijfsmogelijkheden, groei van de industrie en het concurrerend vermogen van Europa ten goede komen. Het centrale idee achter deze visie is het uitrusten van objecten met ICT waardoor deze vanuit een unieke digitale identiteit autonoom gegevens kunnen communiceren middels netwerktechnologie en eventueel vanaf een afstand kunnen worden aan- of uitgeschakeld. De Commissie is inmiddels gestopt met het beleid rond het IvD in het algemeen, maar is op verschillende beleidsterreinen nog steeds actief. Deze beleidsterreinen betreffen onder andere transport en energie. De Commissie voert beleid en heeft succesvol wetgeving voorgesteld die de verplichting opleggen tot slimme meters in de woning en het eCall-systeem in de auto. Deze ontwikkeling is politiek omstreden, omdat het uitrusten van deze objecten met IvD-systemen gevolgen kan hebben voor de vrijheid waarmee mensen van deze objecten gebruik kunnen maken. Slimme meters kunnen een gedetailleerd beeld geven van iemands privéleven en het eCall-systeem is in staat om het gaan en staan van een burger in zijn of haar auto nauwkeurig in kaart te brengen. Bovendien kunnen deze systemen van een afstand worden aan-of uitgeschakeld. Bij een slimme meter kan de toevoer van stroom op afstand worden uitgezet, een eCall-systeem introduceert een kwetsbaarheid waardoor een auto op afstand kan worden uitgeschakeld.

Het realiseren van deze visie van de Europese Commissie heeft ingrijpende gevolgen voor het recht op privacy en de vrijheid van burgers. Het herverdeelt de macht in het voordeel van bedrijfsleven en overheden ten koste van grondrechten. De Commissie heeft erkend dat privacy een belangrijk onderwerp is dat moet worden geadresseerd, maar in zijn communicaties wordt privacy onder de noemer 'obstakels' geschaard. In de verschillende documenten die de Commissie rond het IvD naar buiten heeft gebracht komt naar voren dat het de zorgen rond privacy beoogt te adresseren met het gegevensbeschermingsrecht. De achterliggende aanname lijkt te zijn dat het gegevensbeschermingsrecht dezelfde reikwijdte en beperkingsvoorwaarden heeft als het recht op privacy. De Commissie heeft echter in zijn communicaties rond 'fundamental rights impact assessments' aangegeven dat het de bescherming van grondrechten belangrijk vindt en dat er voor de interpretatie en toepassing van deze rechten aansluiting moet worden gezocht bij de rechtspraak van het Europese Hof voor de Rechten van de Mens (hierna 'EHRM') en het Hof van Justitie van de Europese Unie (hierna 'HvJEU'). Naar aanleiding van bovenstaande staat in dit proefschrift de volgende onderzoeksvraag centraal:

Hoe wordt het recht op privacy door de Commissie geïnterpreteerd en toegepast binnen het beleid en regulering van verplichte IvD-systemen?

Het recht op privacy en gegevensbeschermingswetgeving

In dit proefschrift is aangetoond dat de Commissie exclusief gebruik maakt van gegevensbeschermingsrecht in het beleid en reguleren rond verplichte Internet van Dingen-systemen (hierna 'IvD-systemen'). Het recht op privacy, zoals vastgelegd in diverse bronnen van EU recht, wordt buiten beschouwing gelaten. In hoofdstuk 3 is aangetoond dat het gegevensbeschermingsrecht beginselen kent die uitkomst kunnen bieden bij het vaststellen van waarborgen en beperkingen aan deze systemen. Toetsing aan principes zoals doelbinding en dataminimalisering stellen de EU wetgever in staat om te voorkomen dat IvD-systemen worden uitgerust met onnodige surveillance functies. Gegevensbeschermingsrecht ziet echter niet op functies die derde partijen in staat stellen om van een afstand een systeem uit te schakelen, of het aanzetten van een sensor voor een ander doel dan waarvoor deze is geïnstalleerd. Het gegevensbeschermingsrecht ziet typisch op transparante relaties die normaalgesproken vrijwillig worden aangegaan. Daarom is het de vraag hoe geschikt dit recht is om te worden toegepast op ICT-systemen die gedwongen in de privé-omgeving van burgers worden geïnstalleerd.

Een ander problematisch aspect van het gegevensbeschermingsrecht is dat het voorziet in open normen die normaliter worden geïnterpreteerd en toegepast door de (verwerkings)verantwoordelijke, kortom de partij die een belang heeft bij het verwerken van persoonsgegevens. Bovendien is het gegevensbeschermingsrecht niet van toepassing op Europese standaardiseringsorganisaties (hierna 'ESOs'), terwijl dit de partijen zijn die de technische voorschriften opstellen waaraan de IvD-systemen dienen te voldoen. Een laatste bezwaar is dat het onwaarschijnlijk is dat de toepassing van het gegevensbeschermingsrecht leidt tot de toetsing van de noodzakelijkheid van de initiële opname en verzameling van gegevens. Dit geldt te meer nu de Commissie het gegevensbeschermingsrecht in zijn communicaties veelal positioneert als een recht op gegevensbeveiliging.

De kneedbaarheid van het concept privacy kan worden teruggevonden in de creativiteit waarmee het EHRM en het HvjEU het recht hierop toepassen op technologische fenomenen. Het recht op privacy is steevast een betrouwbare bron geweest voor rechters om burgers te beschermen tegen de macht van de overheid en het bedrijfsleven. Daarom biedt dit recht een goed uitgangspunt om te bemiddelen tussen de conflicterende belangen die inherent zijn aan het ontwerp van IvD-systemen. De functies die zien op de verwerkingen van persoonsgegevens, de sensoren en de schakelaars, vallen allemaal onder de reikwijdte van het recht op privacy.

Een analyse van de jurisprudentie toont drie factoren die relevant zijn bij het bepalen van de ernst van de inmenging met het recht op privacy die wordt veroorzaakt door de verplichte installatie van deze systemen. Er moet worden gekeken naar de context van de gegevensverwerking, de aard van de gegevens en de mogelijke toekomstige inbreuken die deze systemen faciliteren. Uit de verscheidene communicaties van de Commissie blijkt dat ze beogen dat IvD-systemen zowel het bedrijfsleven als de overheid zullen dienen en de installatie van deze systemen dient dan ook te worden beoordeeld tegen de achtergrond van deze agenda. Deze systemen hebben het vermogen om de omgeving van burgers uit te rusten

met zintuigen, maar de waarnemingen kunnen tegen de burger worden gebruikt. Om dit panoptisch potentieel van IvD-systemen in de kiem te smoren dienen de vereisten die het EVRM en het Handvest van de Grondrechten van de Europese Unie (hierna 'EU Handvest') stellen aan inmengingen met dit recht strikt te worden getoetst. Beoogde functies die een inmenging vormen op het recht op privacy en gegevensbeschermingsrecht moeten in de wetgeving worden vastgesteld, zodat deze een wettelijke basis krijgen. Het vereiste van voorzienbaarheid vereist dat deze inmenging voldoende precies wordt omschreven. De grootschalige inmengingen en mogelijke toekomstige inbreuken op het recht op privacy die worden veroorzaakt door de installatie van deze systemen geven de EU wetgever slechts een beperkte beoordelingsvrijheid. De noodzakelijkheid van iedere individuele functie van een systeem die het recht op privacy beperkt dient daarom strikt getoetst te worden, waardoor er nadrukkelijk aandacht dient te zijn voor de subsidiariteit van een functie. De subsidiariteitstoets stelt de EU wetgever in staat om overbodige functies of een onnodig inbreuk makende uitvoering van functies te adresseren en om te komen tot een ontwerp dat het recht op privacy respecteert. De subsidiariteitstoets is daarom geschikt om de burger te beschermen tegen het gevaar van *purpose- en function creep*, kortom het inzetten van IvD-systemen tegen burgers voor andere doeleinden dan waarvoor ze oorspronkelijk zijn geïnstalleerd.

Dit deel van de rechtspraak van het EHRM en HvJEU raakt ook aan de communicaties van de Europese Commissie omtrent hun impact assessments, een instrument dat ze inzetten voorafgaand aan het opstellen van een wetgevingsvoorstel om de impact op grondrechten vast te stellen. De Commissie stelt in deze communicaties dat de inzet is om de bescherming van de rechten in het Handvest zo effectief mogelijk te maken. Indien een negatieve impact wordt vastgesteld moet de Commissie kijken of dit wel nodig is. Indien deze impact niet kan worden voorkomen is de vraag of en hoe deze kan worden verlicht door middel van concrete waarborgen. Indien een functie een inmenging of mogelijk toekomstige inbreuk mogelijk maakt moet proportionaliteit in de strikte zin worden getoetst, dit betekent dat er een belangenafweging moet worden gemaakt, waarbij het gegeven dat de privacy van alle burgers in EU lidstaten aan de orde is extra gewicht in de schaal legt.

Conflicterende rollen van de Europese Commissie

Eén van de belangrijkste problemen bij het beleid en het reguleren van het IvD ligt in het feit dat de Commissie twee, bij tijd en wijle, onverenigbare rollen heeft. Aan de ene kant is de Commissie de beleidsmaker die een coördinerende, uitvoerende en beheersende taak heeft binnen het beleid rond IvD-systemen. Aan de andere kant wordt de Commissie geacht op te treden als bewaker van de EU-grondrechten die zijn vastgelegd in het EU Handvest. Artikel 7 van het EU Handvest betreft het recht op privacy en dit correspondeert met artikel 8 EVRM. Als beleidsmaker ten aanzien van IvD-systemen onderhoudt de Commissie nauwe contacten met de partijen die een belang hebben bij een milde, of beter nog, afwezige handhaving van grondrechten. Daarbij dient te worden opgemerkt dat de Commissie in een afhankelijke positie kan verkeren ten aanzien van deze partijen die het probeert te betrekken in zijn beleid.

IvD-systemen kunnen worden uitgerust met functies die enerzijds inmengen met het recht op privacy, maar anderzijds warm worden verwelkomd door bedrijfsleven en overheden.

In de pre-wetgevende fase positioneert de Commissie het gegevensbeschermingsrecht als geschikt instrument om zorgen omtrent privacy mee aan te pakken. Het doet dit evenwel op een wijze waarop het beschermende potentieel van dit recht nagenoeg compleet wordt uitgehold, door de substantieve gegevensbeschermingsprincipes buiten beschouwing te laten. Een terugkerend fenomeen in deze communicaties is dat de Commissie beoogt de gegevens die op massale schaal verwerkt kunnen worden te laten gebruiken voor een groot aantal doelen, inclusief doelen die conflicteren met het privacybelang van burgers, hetgeen lijkt op een impliciete afwijzing van het doelbindingsbeginsel. Daarom staan de verwerkingen van persoonsgegevens die de Commissie in haar toekomstvisie voor ogen heeft haaks op deze hoeksteen van het gegevensbeschermingsrecht. Bij het uitvoeren van de impact analyse op de grondrechten, bij zowel slimme meters als eCall, wordt deze lijn doorgezet en worden principes als doelbinding en dataminimalisering niet besproken. De vereisten die voortvloeien uit het recht op privacy worden in deze analyses, in weerwil van de uitgesproken ambities van de Commissie in zijn eerdere communicaties, buiten beschouwing gelaten. De impact assessment is juist een geschikt instrument om vast te stellen welke functies bijzondere aandacht verdienen, waarbij ontwerpbeslissingen kunnen raken aan het recht op privacy, alvorens deze functies en de waarborgen waarmee ze worden omkleedt op te nemen in het wetsvoorstel, of te besluiten om de systemen hier niet mee uit te rusten.

De impact assessment zou een brug kunnen slaan tussen het werk van de Commissie voorafgaand aan de wetgeving, de wetgevingsprocedure zelf en de fase waarin de Commissie verantwoordelijk is voor uitvoerings- en gedelegeerde handelingen (quasi-wetgevende fase). In deze laatste fase onderhandelt de Commissie met ESOs over de ontwikkeling van standaarden waarin technische regels zijn opgenomen die zien op de werking van de IvD-systemen. In deze quasi-wetgevende fase zijn de betrokken instellingen gebonden aan artikel 290 en 291 VWEU en het EU Handvest. In artikel 290 VWEU wordt bepaald dat binnen een wetgevingshandeling de bevoegdheid aan de Commissie kan worden overgedragen om gedelegeerde handelingen vast te stellen van bepaalde *niet-essentiële onderdelen* van de wetgevingshandeling. Het onderscheid tussen essentiële en niet-essentiële onderdelen moet volgens het HvJEU onder andere worden vastgesteld op basis van de politieke gevoeligheid van een onderdeel en of dit onderdeel raakt aan EU-grondrechten. In artikel 291 VWEU wordt de wijze van toekenning van uitvoeringsbevoegdheden aan de Commissie geregeld. Beslissingen ten aanzien van IvD-systemen die een (mogelijke) inmenging met het recht op privacy veroorzaken moeten worden genomen door de wetgever. Wanneer de impact assessment overeenkomstig de ambities van de Commissie zou worden uitgevoerd, kan hierin een inventarisatie worden gemaakt van de fundamentele ontwerpkeuzes die zijn voorbehouden aan de EU wetgever.

Het vaststellen en opstellen van deze onderdelen is daarom ook van belang voor het verdere wetgevingsproces. Het kan dienen als aanknopingspunt voor het Europees Parlement en de Raad om het debat te voeren over het systeemontwerp en binnen welke grenzen de Commissie mag onderhandelen met ESOs om standaarden te laten ontwikkelen. Zo kan er

worden voorkomen dat er in standaarden regels worden vastgelegd die leiden tot inmengingen met het recht op privacy, zonder dat deze bij wet zijn voorzien en zonder dat de Commissie een duidelijke instructie van de wetgever heeft ontvangen waarin deze inmenging nauwkeurig wordt begrensd en omkleed met waarborgen. Als hierover niets wordt geregeld in de basisregeling waarin die de installatie van IvD-systemen verplicht, dan gaat de Commissie de onderhandelingen met de ESOs in zonder een duidelijke instructie over de ontwerponderdelen die raken aan grondrechten. Mocht de Commissie in het verzoek dat het richt aan de ESOs hierover stil blijven, dan is het dus uiteindelijk aan deze organisaties of het uiteindelijke ontwerp van het IvD-systeem zal raken aan de fundamentele rechten. Een dergelijk verzoek van de Commissie aan ESOs, dat ten grondslag ligt aan de ontwikkeling van standaarden door de ESOs, kan door hen geweigerd worden (bijvoorbeeld als er te strenge eisen in zijn opgenomen ten aanzien van gegevensverwerking). Een dergelijke weigering is met het oog op de belangen die worden vertegenwoordigd in ESOs, deze bestaand hoofdzakelijk uit het bedrijfsleven, geenszins denkbeeldig. De Commissie kan in dat geval makkelijker besluiten tegemoet te komen aan de eisen van zijn autonome onderhandelingspartner als de wetgevingshandeling waarin de uitvoeringsbevoegdheid van de Commissie is vastgelegd geen eisen stelt aan het verzoek dat ze aan de ESOs moet doen.

De twee case studies die zijn gedaan in dit boek, in hoofdstuk vijf en zes, tonen aan dat de Commissie in haar impact assessments stil blijft over grondrechten en deze stilte continueert in de verzoeken die worden gedaan aan ESOs. Het verzoek aan de ESOs betreffende de slimme meter stelt slechts dat er *rekening moet worden gehouden* (‘take account of’) met gegevensbeschermingswetgeving. Het verzoek op basis waarvan de standaarden voor het eCall-systeem zijn ontwikkeld noemt het identificeren en adresseren van privacyrisico’s, maar noemt het eCall-systeem niet. Het interpreteren en toepassen van privacy- en gegevensbeschermingswetgeving op specifieke onderdelen van het ontwerp van de verplichte IvD-systemen blijft uit.

Vrijheid, autonomie en architectuur

Vrijheid en autonomie zijn twee belangrijke waarden die het recht op privacy beoogt te beschermen. Gegevensbeschermingsrecht wordt soms vergeleken met milieurecht, omdat het beoogt schadelijke gevolgen van de verwerking van persoonsgegevens te beperken. Het verwerken van persoonsgegevens is in de media wel eens vergeleken met het boren naar olie. Gegevens zijn de grondstof voor tal van processen die een hele industrie dienen. Hoe persoonlijker gegevens zijn en hoe indringender het beeld is dat ze blootgeven van de burgers op wie ze betrekking hebben, hoe schadelijker de gevolgen van verwerkingen zijn voor de vrijheid en autonomie van deze burgers. Beslissingen ten aanzien van het ontwerp van IvD-systemen zijn bepalend voor de vraag of deze systemen schadelijke effecten hebben op onze vrijheid en autonomie. Dit schadelijke effect moet worden vermenigvuldigd met het aantal systemen dat in de EU wordt uitgerold. Dit geeft een idee van de gevolgen van slecht ontworpen systemen. Het recht op privacy geeft de mogelijkheid om de verplichte installatie van deze systemen, de noodzakelijkheid van de functies waarmee zij zijn uitgerust en de

belangenafweging die aan de uitrol ten grondslag ligt, te toetsen. De Commissie heeft gefaald in de uitvoering van deze taak. Nota bene, de Commissie is er niet eens in geslaagd om de exacte problemen vast te stellen die het heeft beoogd op te lossen met de verplichte uitrol van deze systemen.

De inertie van de Commissie staat in scherp contrast met zijn ambities om te komen tot een zo effectief mogelijke bescherming van de rechten in het EU Handvest en zelfs een cultuur te kweken waarin medewerkers die schrijven aan wetsvoorstellen een 'fundamental rights reflex' krijgen. Hoe rechtvaardigt de Commissie het uitblijven van deze reflex bij het opstellen van voorstellen die beogen de privé-omgeving van de burger uit te rusten met ICT, zodat deze kan worden onderworpen aan een publiek-privaat surveillance regime? Dit doet de Commissie door de zorgen omtrent privacy te adresseren met een interpretatie en toepassing van het gegevensbeschermingsrecht waarin het alle substantieve beginselen buiten beschouwing laat, ofwel '*data protection light*'. In deze aanpak worden beginselen zoals doelbinding en dataminimalisering genegeerd en ligt de nadruk op het delen van gegevens waarbij de eisen van vertrouwelijkheid, integriteit en beveiliging centraal staan. Dit zijn eisen die voorwaarden stellen aan de verwerking van gegevens, maar niet geschikt zijn om de noodzakelijkheid van de initiële opname en verzameling van gegevens te toetsen. De Commissie bewijst lippendienst aan het gegevensbeschermingsrecht en zo nu en dan aan het recht op privacy, maar wanneer het aankomt op een toepassing van het recht in overeenstemming met de rechtspraak van het EHRM en het HvJEU blijft het muisstil. De Commissie vertrouwt consequent in alle fases van beleid en regulering in deze benadering van gegevensbescherming-light, waardoor ernstige inbreuken op het recht op privacy worden verpakt in technische termen die een neutrale indruk maken. Dit maskeert het feit dat deze systemen de privé-omgeving van de burger in vergaande mate incorporeert in de immer uitdijende surveillance-staat. De Commissie gebruikt de taal van gegevensbescherming teneinde de gegevens van burgers te onteigenen.

Indien architectuur politiek is, kenmerkt de Europese Commissie zijn beleid en regulering rond verplichte IvD-systemen een gecoördineerde stilte ten aanzien van fundamentele ontwerpbeslissingen. Deze stilte maakt het mogelijk dat deze beslissingen worden genomen door ESOs en dit zal normaliter niet leiden tot beslissingen die de effectieve bescherming van het recht op privacy dienen. De Commissie heeft zowel intern als extern signalen ontvangen over hoe de slimme meter en eCall konden worden ontworpen op een wijze die de privacy van burgers daadwerkelijk zou beschermen, maar hier is niets mee gedaan. Dit heeft geleidt tot een vacuüm in de wetgeving rond het ontwerp van deze systemen. De uiteindelijke beslissingen omtrent gegevensontwerp van IvD-systemen worden buiten de democratische arena genomen. De partijen die hierover beslissingen nemen, vertegenwoordigen niet de burgers van de EU, maar deelbelangen die aanwezig zijn in overheden en bedrijfsleven en die veelal worden vertegenwoordigd door technische experts. De voordelen die uit deze beslissingen worden verwacht dienen de belangen van een relatief kleine groep, terwijl alle burgers in EU lidstaten de negatieve gevolgen zullen ondergaan. Het zal de a-symmetrie in bestaande machtsrelaties alleen maar verder vergroten. Deze praktijk is in strijd met de waarden waar de EU op berust: menselijke waardigheid, vrijheid, democratie, de rechtstaat

en eerbiediging van mensenrechten. Als de Commissie zijn beleid doorzet transformeert de privéomgeving van de burger langzaamaan in een hedendaags digitaal panopticum. Het uiteindelijke ontwerp van deze systemen volgt een logica die zou kunnen worden geduid met *gegevens-onteigening door ontwerp*.

De Commissie is in de beste positie om het huidige beleid grondig te herzien. Het kan door impact assessments de ontwerpbeslissingen in kaart brengen die belangrijk zijn en die aan de basis behoren te liggen van beleid en wetgeving. De architectuur van IvD-systemen gaat alle relevante EU instellingen aan, tenminste als democratie en grondrechten niet slechts zijn bestemd om te functioneren als slogans. De opstelling van surveillance-systemen op een massale schaal waardoor publieke toegang kan worden verschaft tot gegevens over de privésfeer is kenmerkend voor een totalitaire samenleving, de dreiging waarvan onder andere leidde tot het opstellen van het EVRM. Hiermee wordt niet beweerd dat de partijen die deze opdringerige visie ondersteunen dergelijke aspiraties hebben. Totalitaire regimes delen echter wel eigenschappen met deze partijen in het feit dat ze proberen een bepaalde visie op te leggen waarin gedrag, gevoel en verlangen tot in vergaande mate worden gecontroleerd. Wat gebeurt er immers met de burgers die geen boodschap hebben aan deze visie en er graag buiten willen leven? Ongehoorzame burgers, of 'onwillige consumenten' (de Commissie spreekt van 'reluctant consumers') krijgen niet de keuze om buiten het IvD te leven. Iedereen wordt geacht mee te lopen in de parade die de Commissie organiseert tussen de industrieën van transport, energie, mobiele diensten, telecommunicatie en publieke autoriteiten. De burger wordt geacht mee te betalen aan de introductie van zijn eigen digitale dwangbuis. De verplichting om de privésfeer voor deze corporatieve visie open te stellen toont een treffende gelijkenis met de karaktertrekken die Ian Shapiro vaststelt die tegen de essentie van democratische rechtvaardigheid ingaan (zie noot 44 onder 'Conclusion'): 'it is unnecessary, it is not usually entered into voluntarily, it is hard or impossible to escape, it is both a-symmetrical and non-self-liquidating, and it has effects that permeate through the social world.' Het fenomeen dat hij omschreef was slavernij.

Uiteindelijk is het antwoord op de vraag hoe de Commissie het recht op privacy interpreteert en toepast binnen het beleid en regulering van verplichte IvD-systemen tamelijk kort. Niet.

BIBLIOGRAPHY

Primary Legislation

Treaty on European Union (TEU) [2012] OJ C 326.

Treaty on the Functioning of the European Union (TFEU) [2012] OJ C 326.

Treaty of Amsterdam [1997] OJ C 340/01.

Charter of Fundamental Rights of the European Union [2010] OJ C 83/02.

Explanations Relating to the Charter of Fundamental Rights [2010] OJ C 303/02.

Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 1950.

Universal Declaration of Human Rights, adopted by the General Assembly of the United Nations on 10 December 1948.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No 108, Strasbourg, 28 January 1981.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119.

Regulation (EU) 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 [2015] OJ L 123/77.

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council [2012] OJ L 316/12.

Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers [2011] OJ L 55/13.

Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information [2013] OJ L 175/1.

Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC [2012] OJ L 315/1.

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

Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC [2009] OJ L 211/55.

Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive) [2007] OJ L 263/1.

Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC [2006] OJ L 114/64.

Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments [2004] OJ L 135/1.

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 (Directive on privacy and electronic communications) [2002] OJ L201/37.

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 [1995] OJ L281/31.

Council Decision 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall Service [2014] OJ L 164/6.

Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services [2015] OJ L 157/21.

Commission Delegated Regulation (EU) 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an interoperable EU-wide eCall [2013] OJ L 91/1.

Commission Delegated Regulation (EU) 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an interoperable EU-wide eCall [2013] OJ L 91/1.

Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services [2015] OJ L 157/21.

Wet structuur uitvoeringsorganisatie werk en inkomen, Staatsblad 2013, 405.

European Commission Documents

Commission Recommendation 2012/148/EU on preparations for the roll-out of smart metering systems [2012] OJ L 73/9.

Commission Recommendation 2011/750/EU on support for an EU-wide eCall service in electronic communication networks for the transmission of in-vehicle emergency calls based on 112 (‘eCalls’) [2011] OJ L 303/46.

Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification [2009] OJ L 122/47.

‘European Governance: A White Paper’ COM (2001) 428 final.

‘Information and Communications Technologies for Safe and Intelligent Vehicles’ (Communication from the Commission to the Council and the European Parliament) COM (2003) 542 final.

‘First report on the implementation of the Data Protection Directive (95/46/EC)’ (Report from the Commission) COM (2003) 265 final.

‘Compliance with the Charter of Fundamental Rights in Commission legislative proposals: Methodology for systematic and rigorous monitoring’(Communication from the Commission) COM (2005) 172 final.

‘The 2nd eSafety Communication: Bringing eCall to Citizens’ (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions) COM (2005) 431 final.

‘Bringing eCall back on track – Action Plan (3rd eSafety Communication)’ (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2006) 723 final.

‘On the Intelligent Car Initiative “Raising Awareness of ICT for Smarter, Safer and Cleaner Vehicles”’ (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions), COM (2006) 59 final.

‘Impact Assessment Accompanying the Legislative Package on the Internal Market for Electricity and Gas COM (2007) 528 final COM (2007) 529 final COM (2007) 530 final COM (2007) 531 final COM (2007) 532 final SEC (2007) 1180’ (Commission Staff Working Document) SEC (2007) 1179/2.

‘Promoting data protection by privacy-enhancing technologies (PETs)’ (Communication from the Commission to the European Parliament and the Council) COM (2007) 228 final.

‘Action Plan for the Deployment of Intelligent Transport Systems in Europe’ (Action plan) COM (2008) 886 final.

‘Communication on future networks and the internet’ (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2008) 594 final.

‘Impact Assessment accompanying the Communication from the Commission Action plan for the deployment of Intelligent Transport Systems in Europe and the Proposal for a Directive of the European Parliament and of the Council lying down the Framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes’ (Commission Staff Working Document) SEC (2008) 3083.

‘Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes’ COM (2008) 887 final.

‘An area of freedom, security and justice serving the citizen’ (Communication From the Commission to the European Parliament and the Council) COM (2009) 262 final.

‘eCall: Time for Deployment’ (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2009) 434 final.

‘Impact Assessment Guidelines’ SEC(2009) 92.

‘Implementation of Article 290 of the Treaty on the Functioning of the European Union’ (Communication From the Commission to the European Parliament and the Council) COM (2009) 673 final.

‘Internet of Things – An action plan for Europe’ (Communication from the Commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions) COM (2009) 278 final.

‘Report on the practical operation of the methodology for a systematic and rigorous monitoring of compliance with the Charter of fundamental rights’ (Report from the Commission) COM (2009) 205 final.

‘Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability’ (Enterprise and Industry Directorate-General, Consultation date: 21 January 2009) M/441 EN.

‘A comprehensive approach on personal data protection in the European Union’ (Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions) COM (2010) 609 final.

‘Delivering an area of freedom, security and justice for Europe's citizens: Action Plan Implementing the Stockholm Programme’ (Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2010) 171 final.

‘Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union’(Communication from the Commission) COM (2010) 573 final.

‘Impact Assessment accompanying the document Commission Recommendation on Support for an EU-wide eCall service in electronic communication networks for the transmission of in-vehicle emergency calls based on 112 (‘eCalls’)’ (Commission Staff Working Paper) SEC (2011) 1019 final.

‘Impact Assessment accompanying the document Directive of the European Parliament and of the Council on energy efficiency and amending and subsequently repealing Directives 2004/8/EC and 2006/32/EC’ (Commission Staff Working Paper) SEC (2011) 779 final.

‘Operational Guidance on Taking Account of Fundamental Rights in Commission Impact Assessments’ (Commission Staff Working Paper) SEC(2011) 567 final.

‘Smart Grids: from innovation to deployment’ (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2011) 202 final.

‘Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century’ COM (2012) 9 final.

‘Implementing the Energy Efficiency Directive – Commission Guidance’ (Communication from the Commission to the European Parliament and the Council) COM (2013) 762 final.

‘Proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall in-vehicle system and amending Directive 2007/46/EC’ COM (2013) 316 final.

‘Benchmarking smart metering deployment in the EU-27 with a focus on electricity’(Report from the Commission) COM (2014) 356 final.

‘Towards a thriving data-driven economy’ (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2014) 442 final.

‘Building a European Data Economy’ (Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2017) 9 final.

‘On the free flow of data and emerging issues of the European data economy’, SWD (2017).

‘On the Mid-Term on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All’ (Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM (2017) 228 final.

Directorate-General for the Information Society and Media (European Commission), Vision and challenges for realising the Internet of things (The Publications Office of the European Union 2010).

Directorate-General for the Information Society and Media (European Commission), *European policy outlook RFID* (final version, The Publications Office of the European Union 2017).

eCall Driving Group, ‘Recommendations of the DG eCall for the introduction of the pan-European eCall’ (Version 2, eCall Driving Group 2006).

EU Commission Task Force for Smart Grids, Expert Group 1: Smart grid standards, 'Functionalities of smart grids and smart meters' (Final Deliverable, The Publications Office of the European Union 2010).

EU Commission Information Society and Media Directorate-General and Energy Directorate-General, 'A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the Smart Meter' (Full Report, The Publications Office of the European Union 2011).

EU Commission Task Force for Smart Grids Expert Group 2, 'Regulatory Recommendation for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, 'Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection' (Recommendation to the European Commission, The Publications Office of the European Union 2011).

EU Commission Task Force for Smart Grids Expert Group 2: Regulatory Recommendation for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems' (The Publications Office of the European Union 2014).

'Standardisation Mandate addressed to CEN, CENELEC and ETSI in the field of Information and Communication Technologies to support the interoperability of Co-operative systems for Intelligent Transport in the European Community'(DG ENTR/D4 M/453 EN , European Union 2009).

Proposal for a Directive of the European Parliament and of the Council on Energy Efficiency and Repealing Directives 2004/8/EC and 2006/32/EC, COM (2011) 370 final.

Proposal for a Directive of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, COM (2017) 495 final.

Case Law

Judgments of the Court of Justice of the EU

Case 9/56 *Meroni & Co, Industrie Metallurgiche SpA v High Authority of the European Coal and Steel Community* [1958] ECR 133.

Case 11/70 *Internationale Handelsgesellschaft* [1970] ECR I-1125.

Case 4/73 *Nold v Commission* [1974] ECR I-491.

Case 23/75 *Rey Soda v Cassa Conguaglio Zucchero* [1975] ECR I-1279.

Case 136/79 *National Panasonic* [1980] ECR I-02033.

Case 169/80 *Administration des Douanes v Gondrand Frères and Garancini* [1981] ECR I-1931.

Case C-22/88 *Vreugdenhil and Others v Minister van Landbouw en Visserij* [1989] ECR 02049.

Case C-331/88 *Fedesa* [1990] ECR I-4057.

Case C-240/90 *Germany v Commission* [1992] ECR 1-5383.

Case C-404/92 *P X v Commission* [1994] ECR I-04737.

Case C-376/98 *Germany* v *Parliament and Council (Tobacco Advertising I)* [2000] ECR I-8419.

Case C-491/01 *British American Tobacco (Investments) and Imperial Tobacco* [2002] ECR I-11453.

Joined cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-04989.

Case C-101/01 *Lindqvist* [2003] ECR I-12971.

Joined cases 453/03, C-11/04, C-12/04 and C-194/04, *ABNA and Others* [2005] ECR I-10423.

Case C-195/06 *Österreichischer Rundfunk (ORF)* [2007] ECR I-08817.

Case C-275/06 *Promusicae* [2008] ECR I-00271, Opinion of AG Kokott.

Case C-275/06 *Promusicae* [2008] ECR I-00271.

Case C-524/06 *Huber* [2008] ECR I-09705.

Case C-73/07 *Satakunnan Markkinapörsi and Satamedia* [2008] ECR I-09831.

Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063.

Joined cases C-468/10 and C-469/10 *Asnef* [2011] ECR I-12181.

Case C-70/10 *Scarlet Extended* [2011] ECR I-11959, Opinion of AG Cruz Villalón.

Case C-70/10 *Scarlet Extended* [2011] ECR I-11959.

Joined cases C-411/10 and C-493/10 *N S and Others* [2011] ECR I-13905.

Case C-355/10 *Parliament v Council* ECLI:EU:C:2012:516.

Case C-291/12 *Michael Schwarz v Stadt Bochum* ECLI:EU:2013:670.

Case C-473/12 *IPI* EU:C:2013:715.

Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* EU:C:2014:238.

Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* EU:C:2014:238, Opinion of AG Villalón.

Case C-427/12 *Commission v Parliament and Council* ECLI:EU:C:2014:170.

Case C-131/12 *Google Spain* EU:C:2014:317.

Joined cases C-446/12 to C-449/12 *Willems* EU:C:2015:238.

Case C-363/14 *Parliament v Council* ECLI:EU:C:2015:579.

Case C-201/14 *Smaranda Bara* ECLI:EU:C:2015:638.

Case C-362/14 *Schrems* EU:C:2015:627, Opinion of AG Bot.

Case C-362/14 *Schrems* EU:C:2015:650.

Case C-419/14 *WebMindLicenses* EU:C:2015:832.

Case C-73/16 *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy* ECLI:EU:C:2017:253, Opinion of AG Kokott.

Case C-582/14 *Breyer* ECLI:EU:C:2016:779.

Case C-613/14 *James Elliott Construction* ECLI:EU:C:2016:821.

Joined cases C-203/15 and C-698/15 *Tele2 Sverige* EU:C:2016:970, Opinion of AG Saugmansgaard.

Joined cases C-203/15 and C-698/15 *Tele2 Sverige* EU:C:2016:970.

Opinion 1/15, *Passenger Name Records (PNR)* ECLI:EU:C:2017:592.

Case C-696/15 *P République Tchèque v Commission* ECLI:EU:C:2017:595.

Judgements of the European Court of Human Rights

Handyside v The United Kingdom App no 5493/72 (ECtHR, 7 December 1976).

Tyrer v UK App no 5856/72 (ECtHR, 25 April 1978).

Sunday Times v The United Kingdom App no 6538/74 (ECtHR, 26 April 1979).

Airey v Ireland App no 6289/73 (ECtHR, 9 October 1979).

Klass and others v Federal Republic of Germany (1979-80) Series A No 28.

Dudgeon v The United Kingdom App no 7525/76 (ECtHR, 22 October 1981).

Malone v The United Kingdom App no 8691/79 (ECtHR, 2 August 1984).

X and Y v The Netherlands App no 8978/80 (ECtHR, 26 March 1985).

James and Others v The United Kingdom App no 8793/79 (ECtHR, 21 February 1986).

Gillow v The United Kingdom App no 9063/80 (ECtHR, 24 November 1986).

Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987).

Gaskin v The United Kingdom App no 10454/83 (ECtHR, 7 July 1989).

Tre Traktörer Aktiebolag v Sweden App no 10873/84 (ECtHR, 7 July 1989).

Soering v The United Kingdom App no 14038/88 (ECtHR, 7 July 1989) .

Powell and Rayner v The United Kingdom App no 9310/81 (ECtHR, 21 February 1990).

Huvig v France App no 11105/84 (ECHR, 24 April 1990).

Margareta and Roger Andersson v Sweden App no 12963/87 (ECtHR, 25 February 1992).

Niemietz v Germany App no 13710/88 (ECtHR, 16 December 1992).

Otto-Preminger-Institut v Austria App no 13470/8 (ECtHR, 20 September 1994).

López Ostra v Spain App no 16798/90 (ECtHR, 9 December 1994).

Vogt v Germany App no 17851/91 (ECtHR, 26 September 1995).

Z v Finland App no 22009/93 (ECtHR, 25 February 1997).

Pierre Herbecq and the Association 'Ligue des droits de l'homme' v Belgium App nos 32200/96 and 32201/96 (Commission Decision, 14 January 1998).

Amann v Switzerland App no 27798/95 (ECtHR, 16 February 2000).

Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000).

Bensaid v The United Kingdom App no 44599/98 (ECtHR, 6 February 2001).

PG and JH v The United Kingdom App no 44787/98 (ECtHR, 25 September 2001).

Pretty v The United Kingdom App no 2346/02 (ECtHR, 29 April 2002).

Christine Goodwin v The United Kingdom App no 28957/95 (ECtHR, 11 July 2002).

Peck v The United Kingdom App no 44647/98 (ECtHR, 28 January 2003) .

Roemen and Schmit v Luxembourg App no 51772/99 (ECtHR, 25 February 2003).

Van Kück v Germany App no 35968/97 (ECtHR, 12 September 2003).

Connors v The United Kingdom App no 66746/01 (ECtHR, 27 May 2004).

Moreno Gómez v Spain App no 4143/02 (ECtHR, 16 November 2004).

Mikulová v Slovakia App no 64001/00 (ECtHR, 6 December 2005).

Copland v The United Kingdom App no 62617/00 (ECHR, 3 April 2007).

Lars and Astrid Fägerskiöld v Sweden App no 37664/04 (ECtHR, 26 February 2008).

KU v Finland App no 2872/02 (ECtHR, 2 December 2008).

S and Marper v The United Kingdom App nos 30562 and 30566/04 (ECtHR, 4 December 2008).

Glor v Switzerland App no 13444/04 (ECtHR, 30 April 2009).

Gardel v France App no 16428/05 (ECtHR, 17 December 2009).

Uzun v Germany App no 35623/05 (ECtHR, 2 September 2010).

Kharin v Russia App no 37345/03 (ECtHR, 3 February 2011).

Lautsi v Italy App no 30814/06 (ECtHR, 18 March 2011).

Von Hannover v Germany (No 2), App nos 20660/08 and 60641/08 (ECtHR, 7 February 2012).

Nada v Switzerland App no 10593/08 (ECtHR, 12 September 2012).

Buckland v The United Kingdom App no 40060/08 (ECtHR, 18 September 2012).

MM v The United Kingdom App no 24029/07 (ECtHR, 13 November 2012).

MK v France App no 19522/09 (ECtHR, 18 April 2013).

Sabanchiyeva and Others v Russia App no 38450/05 (ECtHR, 6 June 2013).

Gobec v Slovenia App no 7233/04 (ECtHR, 3 October 2013).

LH v Latvia App no 52019/07 (ECtHR, 29 April 2014).

Gough v The United Kingdom App no 49327/11 (ECtHR, 28 October 2014).

Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015).

Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland App no 931/13 (ECtHR, 27 June 2017).

Bărbulescu v Romania App no 61496/08 (ECtHR, 5 September 2017).

Judgments of the US Supreme Court

Olmstead v United States 277 US 438 (1928) 474-475.

Other Documents

Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standards (85/C 136/01) [1985] OJ C 136/1.

Council of the European Union, 'ENLETS Work programme 2014-2020: European Network of Law Enforcement Technology Services' (Doc 17365/13, The Publications Office of the European Union 2013).

Council of the European Union, 'European Network of Internal Security Technology Departments' (Doc 14669/08, 2008).

Council of the European Union, 'The Stockholm Programme – An open and secure Europe serving and protecting the citizens' (2009) Brussels <https://ec.europa.eu/anti-trafficking/eu-policy/stockholm-programme-open-and-secure-europe-serving-and-protecting-citizens-0_en> accessed 7 June 2018.

Council of the European Union, 'Position (EU) No 11/2010 of the Council at first reading with a view to the adoption of a directive of the European Parliament and of the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport' [2010] OJ C 203 E/01.

General Secretariat of the Council, 'Conclusions 24/25 October 2013' (EUCO 169/13 CO EUR 13 CONCL 7, European Council Conclusions 2013)

European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the

European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes' [2010] OJ C 47/02.

—— 'Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes' (OJ 2010 C 47/6, The Publications office of the European Union 2010).

—— 'EDPS comments on the Commission Recommendation and the accompanying impact assessment on the implementation of the harmonised EU-wide in-vehicle emergency call ("eCall")*'* (European Data Protection Supervisor 2011).

—— 'Opinion of the European Data Protection Supervisor on the Commission Recommendation on preparations for the roll-out of smart metering Systems' (EDPS 2012).

——'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/EC' (EDPS 2013).

——'on the Commission Recommendation on preparations for the roll-out of smart metering systems' (8 June 2012) < https://edps.europa.eu/sites/edp/files/publication/12-06-08_smart_metering_en.pdf > accessed 7 June 2018.

European Parliament Committee on Industry, Research and Energy, 'Report on the proposal for a directive of the European Parliament and of the Council on energy efficiency and repealing Directives 2004/8/EC and 2006/32/EC (COM(2011)0370 – C7-0168/2011 – 2011/0172(COD))'(A7-0265/2012).

European Parliament, 'Answer given by Ms Kroes on behalf of the Commission' (Parliamentary questions E-008690/2013, European Parliament 2013) <http://bit.ly/1Na51gc> accessed 2 July 2018.

—— 'Written questions with answer: Written questions by Members of the European Parliament and their answers given by a European Union institution' (Notices from European Union institutions, bodies, offices and agencies OJ 2014 C 179/252, The Publications office of the European Union 2014).

European Standards, 'CSN EN 16072 Intelligent transport systems — ESafety — Pan-European eCall operating requirements' (European Standards 2015) <http://www.en-standard.eu/csn-en-16072-intelligent-transport-systems-esafety-pan-european-ecall-operating-requirements-1/> accessed 2 July 2018.

Article 29 Data Protection Working Party, 'Working document on data protection and privacy implications in eCall initiative' (Adopted on 26th September 2006 1609/06/EN WP 125, The Article 29 Working Party 2006) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf> accessed 4 June 2018.

—— 'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (Adopted on 01 December 2009 02356/09/EN WP 168, The Article 29 Working Party 2009) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf> accessed 4 June 2018.

—— 'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (Adopted on 01 December 2009 02356/09/EN WP 168, The Article 29 Working Party 2009) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf> accessed 4 June 2018.

—— 'Opinion 12/2011 on smart metering' (Adopted on 4 April 2011 00671/11/EN WP 183, The Article 29 Working Party 2011) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf> accessed 4 June 2018.

—— 'Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force' (Adopted on 22 April 2013 00678/13/EN WP205, The Article 29 Working Party 2013) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf> accessed 5 June 2018.

—— 'Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force' (2064/13/EN WP209, The Article 29 Working Party 2013) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf> accessed 5 June 2018.

—— 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (Adopted on 16 September 2014 14/EN WP 223, The Article 29 Working Party 2014) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 4 June 2018.

CEN and ETSI, 'Final joint CEN/ETSI-Progress Report to the European Commission on Mandate M/453' (CEN and ETSI 2013).

CEN, CENELEC and ETSI, 'Functional Reference Architecture for Communications in Smart Metering Systems' (CEN/CLC/ETSI/TR 50572:2011).

CEN, CENELEC and ETSI/Smart Meters Coordination Group, 'Introduction and Guide to the work undertaken under the M/441 mandate' (A report by the CEN-CENELEC-ETSI Smart Meters Coordination Group).

CEN, CENELEC and ETSI/Smart Meters Coordination Group, 'Introduction and Guide to the work undertaken under the M/441 mandate' (SM-CG report at end 2012 – Final draft, Private circulation PEL/13_12_0105).

CEN, CENELEC and ETSI/Smart Meters Coordination Group, 'Task Force Privacy and Security of the Smart Meters Coordination Group, 'Privacy and Security approach – part I' (Version 1.02, CEN-CENELEC-ETSI 2013) <ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/Management/SmartMeters/SMCG_Security_and_Privacy_Report_PartI.pdf > accessed 5 June 2018.

CEN-CENELEC-ETSI Smart Grid Coordination Group, 'First Set of Standards' (CEN CENELEC 2012) <ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/First%20Set%20of%20Standards.pdf> 2 July 2008.

C-ITS Platform, 'Final Report' (Report, European Commission 2016).

C-ITS Platform/Working Group 6, 'Access to in-vehicle resources and data' (Report, European Commission 2015).

Information and Privacy Commissioner of Ontario and The Future of Privacy Forum, 'SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation'(Information and Privacy Commissioner of Ontario 2009) <https://www.smartgrid.gov/files/SmartPrivacy_for_Smart_Grid_Embedding_Privacy_into_Design_El_200909.pdf> accessed 5 June 2018.

Internet of Things (Unit E4), 'The Internet of Things' (Policy, Digital Single Market, 2018) <http://ec.europa.eu/digital-agenda/en/internet-things> accessed 2 July 2018.

Parliamentary Assembly of the Council of Europe, Resolution No 428 (1970) containing a declaration on mass communication media and human rights (Part C Article 16, 23 January 1970) <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en.> accessed 7 June 2018.

Smart Mobility and Living (Unit H2) 'Smart Cities' (Policy, Digital Single Market, 2018) <http://ec.europa.eu/digital-agenda/en/smart-living> accessed 4 June 2018.

The European Council for an Energy Efficient Economy, 'Steering through the maze #5. Your eceee guide to following the approval process of the proposed Energy Efficiency Directive' (The European Council for an Energy Efficient Economy 2017).

The Stockholm Programme – An open and secure Europe serving and protecting the citizens (Notice from the Council of the European Union) [2010] OJ C 115/1.

Working Group IX on Simplification, 'Final report of Working Group IX on Simplification' (CONV 424/02 WG IX 13 The European Convention Brussels, 29 November 2002).

Secondary Sources

Akandji-Kombe J, *Positive Obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention of Human Rights* (Human Rights Handbooks, No 7, Council of Europe 2007).

Alexy R, 'Constitutional Rights, Balancing,and Rationality' (2003) 16 (2) Ratio Juris 131.

Anderson R and Fuloria S, 'Who controls the off switch?' (Published conference paper from the 1st IEEE International Conference on Smart Grid Communications, IEEE 2010).

Anderson R, 'Consultation response on Smart Meters' (Foundation for Information Policy Research 2010) <http://www.fipr.org/100110smartmeters.pdf> accessed 5 June 2018.

Arai Y, 'The Margin of Appreciation Doctrine in the Jurisprudence of Article 8 of the European Convention on Human Rights' (1998) 16(1) NQHR,41.

Arendt H, *The Origins of Totalitarianism* (Schocken Books 1951).

Ashton K, 'That "Internet of Things" Thing' (RFID Journal, 22 June 2009) <http://www.rfidjournal.com/articles/view?4986> accessed 7 June 2018.

Balkin JM, 'Interdisciplinarity as Colonization' (1996) 53 Washington and Lee Law Review 949.

Bankston KS and Soltani A, 'Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v Jones' (2013) 123 YaleLJ 335.

Bast J, 'Legal Instruments and Judicial Protection' in von Bogdandy A and Bast J (eds), *Principles of European Constitutional Law* (Second Revised Edition, Hart 2011).

Bentham J, 'Panopticon' in Bozovic M (ed), *The Panopticon Writings* (London, Verso, 1995).

Bergström CF, *Comitology: Delegation of Powers in the European Union and the Committee System* (Oxford Studies in European Law, Oxford University Press 2006).

Blok PH, *Het Recht op Privacy* (Boom Juridische uitgevers, 2002).

Bradley K St C, 'Legislating in the European Union' in Catherine Barnard and Steve Peers (eds), *European Union Law* (Oxford 2014).

Brems E and Lavrysen L, '"Don't Use a Sledgehammer to Crack a Nut": Less Restrictive Means in the Case Law of the European Court of Human Rights' (2015) 15 HRLRev 139.

Breyer P, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) 11(3) ELR 365.

Brown I, *The Challenges to European Data Protection Laws and Principles* (European Commission Directorate-General Justice, Freedom and Security 2010).

—— 'Britain's Smart Meter Programme: A Case Study in Privacy by Design' (2014) 28 International Review of Law, Computers & Technology 172.

Bygrave LA, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology 247.

——'Privacy-Enhancing Technologies: Caught between a Rock and a Hard Place' (2002) 9 Privacy Law & Policy Reporter 135.

—— and Schartum DW, *Consent, Proportionality and Collective Power,* 161 in Gutwirth S and others (eds), *Reinventing Data Protection?* (Springer 2009).

Çali B, 'Balancing Human Rights? Methodological Problems with Weights, Scales and Proportions' (2007) 29 (1) HumRtsQ 251.

Chamon M, 'How the Concept of Essential Elements of a Legislative Act Continues to Elude the Court: Parliament v. Council' (2013) 50 CMLRev 849.

—— 'Institutional Balance and Community Method in the Implementation of EU Legislation following the Lisbon Treaty' (2016) 53 CMLRev 1501.

Chomsky N, *Profit over People: Neoliberalism and Global Order* (1st edition, Seven Stories Press 1999).

Cini M, 'The European Commission: An Unelected Legislator?' (2002) 8 (4) The Journal of Legislative Studies 14.

Cotterrell R, 'Why Must Legal Ideas be Interpreted Sociologically?'(1998) 25 Journal of Law and Society 171.

Craig P, *EU Administrative Law* (Oxford University Press 2006).

——'Delegated Acts, Implementing Acts and the New Comitology Regulation' (2011) 36 European Law Review 673.

——'Comitology, Rulemaking, and the Lisbon Settlement' in Bergström CF and Ritleng D (eds), *Rulemaking by the European Commission: The New System for Delegation of Powers* (1st edition, Oxford Scholarship Online 2016).

—— and de Búrca G, *EU Law: Text, Cases and Materials*, (5th edition, Oxford University Press 2011).

Cuijpers C and Koops B, 'Het wetsvoorstel "slimmemeters": een privacytoets op basis van art. 8 EVRM' (Onderzoek in opdracht van de Consumentenbond, Universiteit van Tilburg TILT – Centrum voor Recht, Technologie en Samenleving 2008).

—— and Koops B,'Smart Metering and Privacy in Europe: Lessons from the Dutch Case' in Gutwirth S and others (eds), *European Data Protection: Coming of Age* (Springer Science + Business Media 2013).

De Castro L and Dutra, 'The Economics of the Smart Grid' (Published conference paper from the 49th Annual Allerton Conference on J Communication, Control, and Computing, IEEE 2012).

De Hert P, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Part of the Law, Governance and Technology Series vol 6, Springer 2012).

—— and Gutwirth S, 'Privacy, Data Protection and Law Enforcement. Opacity of the individual and transparency of power' in Eric Claes, Anthony Duff and Gutwirth S (eds), *Privacy and the criminal law* (Antwerpen/Oxford Intersentia 2006).

—— and Gutwirth S, 'Consent, Proportionality and Collective Power' in Gutwirth S and others (eds), *Reinventing Data Protection* (Springer 2009).

—— and Gutwirth S, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S and others (eds), *Reinventing Data Protection* (Springer 2009).

de Montjoye Y and others, 'Unique in the Crowd: The privacy bounds of human mobility' (2013) 3 Scientific Reports < https://www.nature.com/articles/srep01376 > accessed 29 June 2018.

DeMott DA, 'Organizational Incentives to Care about the Law' (1997) 60 (4) Law&ContempProbs 39.

den Heijer M and Tauschinsky E, 'Where Human Rights Meet Administrative Law: Essential Elements and Limits to Delegation' (2013) 9 EuConst 513.

Dewey J, 'Liberalism and Civil Liberties' in Boydston JA (ed), *The Later Works, 1925-1953* (Volume II 1935-1937) (Southern Illunois University Press 2008).

—— *Freedom and Culture* (London, George Allen and Unwin Ltd 1940).

Diggelmann O and Cleis MN, 'How the Right to Privacy Became a Human Right' [2014] HRLRev 441.

Egan M, 'Regulatory Strategies, Delegation and European Market Integration' (1998) 5 Journal of European Public Policy 485.

Eisses S, van de Ven T and Fievée A, 'ITS Action Plan: ITS & Personal Data Protection' (Final Report, European Commission DG Mobility and Transport 2012).

Eskens SJ, 'Ongerichte interceptie, of het verwerven van bulk-communicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden' (2015) 85 Computerrecht 125.

Ferretti F, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?' (2014) 51 CMLRev 843.

Foucault M, *Discipline and Punishment* (Translation copyright 1977 by Alan Sherdan, 2nd edition, Random House inc 1995).

Frankel C and Højberg E, 'The Constitution of a Transnational Policy Field: Negotiating the EU Internal Market for Products' (2007) 14 Journal of European Public Policy 108.

Fuster GG, 'Security and the Erasure of Privacy in the Data Protection Legal Landscape of the European Union' (Amsterdam Privacy Conference, October 2012).

——'Opening up Personal Data Protection: A Conceptual Controversy' (2013) 29 Computer Law & Security Review 531.

——'Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection' (2014) 2(2) Birkbeck Law Review 263.

——*The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

Gavison RE, 'Privacy and the Limits of Law' (1980) 89(3) YaleLJ 421.

Gellert R and Gutwirth S, *Beyond Accountability, the Return to Privacy* (Palgrave Macmillan 2012).

—— and Gutwirth S, 'The Legal Construction of Privacy and Data Protection' (2013) 29 Computer Law & Security Review 528.

Gerards J, *EVRM Algemene Beginselen* (SDU Uitgevers 2011).

Geuens C and Dumortier J, 'Mandatory Implementation for In-vehicle eCall: Privacy Compatible' (2010) 26 Computer Law & Security Review 385.

Goold BJ, '*Liberty and others v The United Kingdom*: A New Chance for Another Missed Opportunity' (2009) PublL 5.

Greenfield A, *Everyware: The Dawning Age of Ubiquitous Computing* (1st edition, Pearson Education 2006).

Greer S, *The exceptions to Article 8-11 of the European Convention on Human Rights* (Council of Europe Publishing, 1997).

—— '"Balancing" and the European Court of Human Rights: a Contribution to the Habermas-Alexy Debate' (2004) 63(2) CLJ 412.

Gutwirth S, *Privacyvrijheid! De vrijheid om zichzelf te zijn* (Rathenau 1998).

Haas PM, 'Introduction: epistemic communities and international policy coordination' (1992) 46 International Organization 1.

Habermas J, *Between Facts and Norms* (Cambridge 1996).

Harbo T, 'The Function of the Proportionality Principle in EU Law' (2010) 16(2) ELJ 158.

Hijmans H, *The European Union as Guardian of Internet Privacy* (Springer 2016).

Hildebrandt M, ‘Legal Protection by Design in the Smart Grid’ (Report commissioned by the Smart Energy Collective, Bepress 2013) <http://works.bepress.com/mireille_hildebrandt/42> accessed 5 June 2018.

Hoenkamp R, *Safeguarding EU Policy Aims and Requirements in Smart Grid Standardization* (2015, UvA-Dare) <http://hdl.handle.net/11245/2.158793 > accessed 7 June 2018.

——JC de Moor AJC- van Vugt and Huitema GB, ‘Law and Standards: Safeguarding Societal Interests in Smart Grids’ in Leenes R and Kosta E (ed), *Bridging Distances in Technology and Regulation* (Wolf Legal Publishers 2013).

Hoffman H, ‘Legislation, Delegation and Implementation under the Treaty of Lisbon: Typology Meets Reality’ (2009) 15 ELJ 482.

Homburg G and others, *ANPR: toepassingen en ontwikkelingen* (WODC 2016).

Howarth D, *Discourse* (Open University Press 2000).

Hughes K, ‘The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse’ in Roessler B and Mokrosinska D (eds), *Social Dimensions of Privacy* (Cambridge University Press 2015).

Hutchinson T and Duncan N, ‘Defining and Describing What We Do: Doctrinal Legal Research’ (2012) 17 Deakin Law Review 83.

Jacobs B, ‘Architecture Is Politics: Security and Privacy Issues in Transport and Beyond’ in Gutwirth S and others (eds), *Data Protection in a Profiled World* (Springer 2010).

——‘Keeping our surveillance society non-totalitarian’ [2009] 1(4) Amsterdam Law Forum <http://amsterdamlawforum.org/article/view/91> accessed 7 June 2018.

Jacqué JP, ‘Le Traité de Lisbonne: Une vue cavalière’ (2008) 44 Revue trimestrielle de droit européen 439.

Kilkelly U, *The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention of Human Rights* (Human rights handbook, No 1, Council of Europe 2003).

Knapp ED and Samani R, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure* (Elsevier 2013) ch 4.

Koenis F and van Steen J, ‘Schakelfunctie onder loep: Nadere verkenning van de maatschappelijke kosten en baten van de schakelmogelijkheid in de slimme meter’ (Rapport in opdracht van het Ministerie van Economische Zaken, KEMA Nederland BV 2013).

Konarski X, Karwala D and Schulte-Nölke H, ‘Data Protection Aspects of eCall’ (Document requested by the European Parliament's Committee on the Internal Market and Consumer Protection IP/A/IMCO/NT/2013-12, European Union, 2014).

Kortmann CAJM, *Constitutioneel Recht* (Kluwer 2001).

Kranenborg H, ‘Article 8’ in Peers S and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart 2014).

Kurasawe K, Danezis G and Kohlweiss M, 'Privacy-friendly Aggregation for the Smart-grid' (Microsoft Research, 2011) < https://www.microsoft.com/en-us/research/publication/privacy-friendly-aggregation-for-the-smart-grid/?from=http%3A%2F%2Fresearch.microsoft.com%2Fpubs%2F146092%2Fmain.pdf> accessed 5 June 2018.

Kyritsis D, 'Whatever Works: Proportionality as a Constitutional Doctrine' (2014) 34(2) OJLS 395.

Lazer D and Mayer-Schonberger V, Governance and Information Technology: From Electronic Government to Information Government (MIT Press 2007).

Leferink F, Keyer C and Melentjev A, 'Static Energy Meter Errors Caused by Conducted Electromagnetic Interference' (2016) 5 (4) IEEE Electromagnetic Compatibility Magazine 49.

Lessig L, *Code* (Version 2, Basic Books, 2006).

Lynskey O, 'Deconstructing Data Protection: the "Added-Value" of a Right to Data Protection in the EU Legal Order' (2014) 63(3) ICLQ 569.

McCarthy M and others, 'Access to In-vehicle Data and Resources' (DG-MOVE Final report, European Union 2017).

McKenna E, Richardson I and Thomson M, 'Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications' (2012) 41 Energy Policy 807.

Mihail S and Wisman THA, 'The Right to Privacy with Respect to the Processing of Personal Data in the Context of Controlling Tax Fraud' (2017) 3(2) EDPL 265.

Mowbray A, 'The Creativity of the European Court of Human Rights' (2005) 5 HRLRev 57.

Nugent N, *The Government and Politics of the European Union* (The European Union series, 6th edition, Palgrave Macmillan 2006).

Pallas F, 'Beyond Gut Level – Some Critical Remarks on the German Privacy Approach to Smart Metering' in Gutwirth S and others (eds) *European Data Protection: Coming of Age* (Springer 2013).

Peers S and Costa M, 'Accountability for Delegated and Implementing Acts after the Treaty of Lisbon' (2012) 18 ELJ 427.

Pirker B, *Proportionality Analysis and Models of Judicial Review* (Europa Law Publishing 2013).

Quinn EL, 'Privacy and the New Energy Infrastructure' (2008) Cees working paper no. 09-001 <http://dx.doi.org/10.2139/ssrn.1370731> accessed 5 June 2018.

Raab C, 'Effects of Surveillance on Civil Liberties and Fundamental Rights in Europe', in Wright D and Kreissl R (eds), *Surveillance in Europe* (Routledge 2015).

Rainey B, Wicks E, and Ovey C, *Jacobs, White & Ovey: The European Convention on Human Rights* (Oxford University Press 2010).

Regan PM, ‘Privacy and the Common Good: Revisited’ in Roessler B and Mokrosinska D (eds), *Social Dimensions of Privacy* (Cambridge University Press 2015).

Reich N, ‘How Proportionate is the Proportionality Principle’ (The Reach of Free Movement conference, Oslo, 18-19 May 2011).

Ritleng D, ‘The Reserved Domain of the Legislature’ in Bergström CF and Ritleng D (eds), *Rulemaking by the European Commission: The New System for Delegation of Powers* (1st edition, Oxford University Press 2016).

Rivers, J ‘Proportionality and Discretion in International and European Law’ in Tsagourias N (ed) *Transnational Constitutionalism* (Cambridge University Press 2014).

Robertson AH, *Collected edition of the 'travaux préparatoires' of the European Convention on Human Rights = Recueil des travaux préparatoires de la Convention Européenne des Droits de l'Homme* (Vol 1, Preparatory Commission of the Council of Europe Committee of Ministers, Consultative Assembly, 11 May-8 September 1949, The Hague, Nijhoff 1975).

Savirimuthu J, ‘Smart Meters and the Information Panopticon: Beyond the Rhetoric of Compliance’ (2013) 27 International Review of Law, Computers & Technology 161.

Schepel H, *The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets* (International Studies in the Theory of Private Law, 1st edition, Hart Publishing 2005).

Schermer BW, ‘The Limits of Privacy in Automated Profiling and Data Mining’ (2011) 27(1) Computer Law & Security Review 45.

Schütze R, ‘From Rome to Lisbon: “Executive Federalism” in the (New) European Union’ (2010) 47 CMLRev 1385.

——‘”Delegated” Legislation in the (new) European Union: A Constitutional Analysis’ (2011) 74 The ModLRev 661.

——*European Constitutional Law* (2nd edition, Cambridge University Press 2016).

Senden H, *Interpretation of Fundamental Rights in a Multilevel Legal System* (Intersentia 2011).

Shapiro I, *Democratic Justice* (Yale University Press, 1999).

Smits JM, *The Mind and Method of the Legal Academic* (Edward Elgar 2012).

Specht M and others, *Standardization in Smart Grids* (Springer-Verlag 2013) ch 11.

Strawbridge G, ‘The Single Market Effect: European Standardization in Theory and Practice’ (1990) 8 European Management Journal 174.

Surden H, ‘Structural Rights in Privacy’ (2007) 60 SMU Law Review 1605.

Tronsoco C and others, ‘PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance’ (2011) 8 IEEE Transactions on Dependable and Secure Computing.

Tsakyrakis S, ‘Proportionality: An Assault on Human Rights?’ (2009) 7(3) ICON 468.

van der Mei AP, 'Delegation of Rulemaking Powers to the European Commission post-Lisbon' (2016) 12 EuConst 538.

van Gestel R and Micklitz HW, 'Revitalizing Doctrinal Legal Research in Europe: What about Methodology?' (2011) LAW 2011/05 EUI Working Papers.

—— and Micklitz HW, 'European Integration through Standardization: How Judicial Review is Breaking down the Club House of Private Standardization Bodies' (2013) 50 CMLRev 145.

Vick DW, 'Interdisciplinarity and the Discipline of Law' (2004) 31 Journal of Law and Society 164.

Vickery G, 'Review on recent studies on PSI reuse and Related Market Developments' (final version) <https://ec.europa.eu/digital-single-market/en/news/review-recent-studies-psi-reuse-and-related-market-developments > accessed 5 June 2018.

Voermans WJM, 'Delegation Is a Matter of Confidence' (2011) 17(2) EPL 313.

——Hartmann J and Kaeding M, 'The Quest for Legitimacy in EU Secondary Legislation' (2014) 2 The Theory and Practice of Legislation 5.

Vringer K en Dassen T, 'De Slimme Meter, Uitgelezen Energie(K)?' (Achtergrondstudie, PBL Planbureau voor de Leefomgeving 2016).

Warren SD and LD Brandeis, 'The Right to Privacy' (1890) 4 Harv L Rev 193

Weiler JHH, 'Epilogue: "Comitology" as Revolution – Infranationalism, Constitutionalism and Democracy' in Joerges C and Vos E (eds), *EU Committees: Social Regulation, Law and Politics* (Hart 1999).

Weiser M, 'The Computer for the 21st Century' (1991) Scientific American.

Westin AF, 'Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part II, Balancing the Conflicting demands of Privacy, Disclosure and Surveillance' (1966) 66(7) Columbia Law Review 1205.

——*Privacy and Freedom* (New York, Atheneum 1970).

Wisman THA, 'Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things' (2013) 4(2) EJLT < http://ejlt.org/article/view/192/379> accessed 5 June 2018.

——'Giving Member States the Prints and Data Protection the Finger' (2015) 1 European Data Protection Law Review 245.

——'eCall and the Quest for Effective Protection of the Right to Privacy' (2016) 2 European Data Protection Law Review 59.

Wright D, 'Making Privacy Impact Assessment More Effective' (2013) 29 The Information Society 307.

Zittrain JL, *The Future of the Internet and How to Stop It* (Yale University Press) 2008.

Miscellaneous Sources

Big Brother Watch, 'Lifting the lid: The rising number of microchips in our bins and why it matters' (Report, Big Brother Watch 2009) <https://www.bigbrotherwatch.org.uk/liftingthelid.pdf.> accessed 5 June 2018.

Big Picture Media Corporation, 'The Corporation' (2003).

'60 años de investigaciones económicas han impulsado el desarrollo del país' (ElPais, 16 August 2015) <http://www.elpais.cr/2015/08/16/60-anos-de-investigaciones-economicas-han-impulsado-el-desarrollo-del-pais/83700/?fb_action_ids=604341192919588&fb_action_types=og.likes&fb_source=other_multiline&action_object_map> accessed 5 June 2018.

'Chronologic dossier "slimme" energie meters' (Wij vertrouwen slimme meters niet) <http://www.wijvertrouwenslimmemetersniet.nl/> accessed 2 July 2018.

'Data is giving rise to a new economy' (Economist, 6 May 2017) <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> accessed 7 June 2018.

'Europol chief warns on computer encryption' <http://www.bbc.com/news/technology-32087919> accessed 17 August 2016.

Car data facts, (fact-based overview on everything related to the sharing of vehicle-generated data with third parties) <http://cardatafacts.eu/> accessed 7 June 2018.

'Why share car data?' <http://cardatafacts.eu/> accessed 2 February 2018.

'Smart metering' (Online index, CEN and CENELEC) <http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartMeters/Pages/default.aspx> accessed 5 June 2018.

'Tell-all telephone' (Zeit Online, 31 August 2009) <https://www.zeit.de/datenschutz/malte-spitz-data-retention> accessed 29 June 2018.

ACEA, 'Vehicles in Use' <http://www.acea.be/statistics/tag/category/vehicles-in-use> accessed 9 April 2018.

Embassy The Hague, Ambassador's Parting Thoughts on Taking the Dutch, (22-08-2005) <http://213.251.145.96/cable/2005/08/GUARDIANUK-38987.html> accessed 7 June 2018.

ENISA, 'Smart Grid Security' (Annex II to the ENISA study Smart Grid Security: Recommendations for Europe and Member States, ENISA 2012).

Erb KP, ‘Out Of Ideas And In Debt, Spain Sets Sights On Taxing The Sun’ (Forbes, 19 August 2013).

Ernst & Young, ‘Cost-benefit analysis for the comprehensive use of smart metering’ (On behalf of the Federal Ministry of Economics and Technology, Ernst & Young GmbH 2013).

Ertico, ‘The ERTICO Partnership – Vision & Mission’ <http://ertico.com/vision-and-mission/> accessed 2 July 2018.

‘When your yogurt pots start talking to you: Europe prepares for the internet revolution’ (IP/09/952 Press Release, Brussels, 18 June 2009) <http://europa.eu/rapid/press-release_IP-09-952_en.htm> accessed 4 June 2018.

‘Emergency calls: Commission welcomes growing Member State endorsement for eCall in-car system’ (IP/ 10/488 Press Release, Brussels, 4 May 2010) <http://europa.eu/rapid/press-release_IP-10-488_en.htm> accessed 2 July 2018.

‘eCall: automated emergency call for road accidents mandatory in cars from 2015’ (IP/13/534 Press Release, Brussels, 13 June 2013) <http://europa.eu/rapid/press-release_IP-13-534_en.htm> accessed 2 July 2018.

‘Report on the Public Consultation on IoT Governance’ (16 January 2013).

‘eCall: Do you have any concerns for your privacy? You shouldn't’ (Digital Single Market factsheet/infographic, 4 June 2014) <https://ec.europa.eu/digital-single-market/en/news/ecall-%E2%80%93-do-you-have-any-concerns-your-privacy-you-shouldnt> accessed 2 July 2018.

‘Fundamental Rights: Importance of EU Charter grows as citizens stand to benefit’ (Press Release, Brussels, 14 April 2014) <http://europa.eu/rapid/press-release_IP-14-422_en.htm> accessed 2 July 2018.

‘An EU strategy on cooperative, connected and automated mobility’ (Fact Sheet MEMO/16/3933, European Union 2016).

‘Study on the Deployment of C-ITS in Europe: Final Report’ (Framework Contract on Impact Assessment and Evaluation Studies in the Field of Transport MOVE/A3/119-2013-Lot № 5 "Horizontal”, DG MOVE 2016).

Future Group, ‘First meeting of the Future Group’ (Warm-up session 20 and 21 May 2007, Eltville Germany) <http://bit.ly/VeLZf2> accessed 7 June 2018.

——‘Public Security and Technology in Europe: Moving Forward’ (Concept paper on the European strategy to transform Public security organisations in a Connected World, Portugal 2007) <http://bit.ly/PqvWIJ> accessed 2 July 2018.

——‘Freedom, Security, Privacy – European Home Affairs in an open world’ (June 2008) <www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf> accessed 7 June 2018.

Clapper JR, ‘Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community’ (2016) Congressional Testimonies 1.

Cognizant, ‘The New Auto Insurance Ecosystem: Telematics, Mobility and the Connected Car’ (Cognizant Reports, Cognizant 2012).

Cole D, ‘We Kill People Based on Metadata’ (NYR Dailey, 10 May 2014) <http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/> accessed 2 July 2018.

Criqui P and La Branche S, ‘Compteur électrique Linky: comprendre la polémique’ (The Conversation, 23 May 2016) <http://theconversation.com/compteur-electrique-linky-comprendre-la-polemique-59769> accessed 7 June 2018.

Hardesty L, ‘Privacy challenges Analysis: It’s surprisingly easy to identify individuals from credit-card metadata’ (MIT News, 29 January 2015) <http://news.mit.edu/2015/identify-from-credit-card-metadata-0129> accessed 2 July 2018.

Hern A, ‘Hacking Team hack casts spotlight on murky world of state surveillance’ (The Guardian, 11 July 2015) <https://www.theguardian.com/technology/2015/jul/11/hacking-team-hack-state-surveillance-human-rights> accessed 2 July 2018.

—— ‘“Am I at risk of being hacked?” What you need to know about the “Vault 7” documents’ (The Guardian, 8 March 2017) <https://www.theguardian.com/technology/2017/mar/08/wikileaks-vault-7-cia-documents-hacked-what-you-need-to-know> accessed 7 June 2018.

Hunn N, ‘Squirrels, Grid Security and a Stuffed Rudd’(Creative Connectivity, 2 May 2016) <http://www.nickhunn.com/squirrels-grid-security-and-a-stuffed-rudd/> accessed 5 June 2018;

—— ‘When Smart Meters get Hacked’ (Creative Connectivity, 8 June 2014) <http://www.nickhunn.com/when-smart-meters-get-hacked/> accessed 5 June 2018.

—— ‘What’s the difference between Sir Philip Green and the GB Smart Metering Program?’(Creative Connectivity, 28 November 2016) < http://www.nickhunn.com/whats-the-difference-between-sir-philip-green-and-the-gb-smart-metering-program/> accessed 5 June 2018.

Lhomme S, ‘Compteurs communicants: pourquoi il faut resister au diktat des politiques et industriels’(L’obs, 17 April 2016) <http://leplus.nouvelobs.com/contribution/1505932-

compteurs-communicants-pourquoi-il-faut-resister-au-diktat-des-politiques-et-industriels.html> accessed 7 June 2018.

McKinsey & Company, 'Monetizing car data: New service business opportunities to create new customer benefits' (Advanced Industries September Report, McKinsey & Company 2016).

Moerel L, 'Big Data Protection' (Lecture, 2014) <https://pure.uvt.nl/portal/files/2837675/oratie_Lokke_Moerel.pdf> accessed 7 June 2018.

Narciso D, 'Police seek utility data for homes of marijuana-growing suspects' (The Columbus dispatch, 28 February 2011) <http://www.dispatch.com/content/stories/local/2011/02/28/police-suspecting-home-pot-growing-get-power-use-data.html> accessed 18 June 2014.

Oettinger G, 'Speech of Commissioner Oettinger at the Press point EUSEW' (EUSEW, Brussels, 12 April 2011).

Peers S, 'Biometric data and data protection law: the CJEU loses the plot' (EU Law Analysis, 17 April 2015) <http://eulawanalysis.blogspot.se/2015/04/biometric-data-and-data-protection-law.html> accessed 2 July 2018.

Pell EH, 'Smart meters 'not needed' after all for European power grid' (Euractiv, 16 June 2016) <https://www.euractiv.com/section/energy/news/smart-meters-not-needed-after-all-for-european-power-grid/> accessed 2 July 2018.

Pillitteri VY and Brewer TL, 'Guidelines for Smart Grid Cybersecurity'(A Three-volume report, NIST Interagency/Internal Report (NISTIR) - 7628 Rev 1 2014), volume 2 <https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf> accessed 2 July 2018.

Poptcheva E, 'The European Commission's right to withdraw a legislative proposal' <https://epthinktank.eu/2015/04/23/the-european-commissions-right-to-withdraw-a-legislative-proposal/> accessed 4 June 2018.

Privacy international, 'National Data Retention Laws since the CJEU's Tele-2/Watson Judgment: A Concerning State of Play for the Right to Privacy in Europe' (Privacy International, 2017). <https://privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf> accessed 5 June 2018.

Python (Monty) Pictures, 'Monthy Python and the Holy Grail' (1975).

Punie Y, 'SWAMI Project: Safeguards in a World of AMbient Intelligence' (Starting date: February 2005 Duration: 18 months).

Quijones DQ, 'The Men Who're Stealing The Sun' (Wolf Street, 14 June 2015) <https://wolfstreet.com/2015/06/14/the-men-who-stole-the-sun-spain-solar-power-taxes-fines-to-protect-giants/> accessed 18 April 2016.

Radar, 'Slimme meter: van het meterkastje naar de muur' (20 March 2017) <https://radar.avrotros.nl/uitzendingen/gemist/20-03-2017/slimme-meter-van-het-meterkastje-naar-de-muur/> accessed 5 June 2018.

Reding V, 'RFID: Why we need a European policy' (EU RFID 2006 Conference: Heading for the Future, Brussels, 16 October 2006).

—— 'The importance of the EU Charter of Fundamental Rights for European legislative practice'(Lecture given at the German Institute for Human Rights, Berlin, 17 September 2010).

Rusbridger A, 'The Snowden Leaks and the Public' (NYR, 21 November 2013) <http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/> accessed 2 July 2018.

Schneier B, 'Will giving the internet eyes and ears mean the end of privacy?' (The Guardian, 16 May 2013) <http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google> accessed 7 June 2018.

Tommelein B, 'Overheid gaat fraude opsporen via onze energie- en waterfacturen', (MoneyTalk, 18 Februari 2016) <http://moneytalk.knack.be/geld-en-beurs/belastingen/overheid-gaat-fraude-opsporen-via-onze-energie-en-waterfacturen/article-normal-666995.html?utm_campaign=Echobox&utm_medium=social&utm_source=Facebook#link_time=1455789795> accessed 7 June 2018.

Töpfer E, 'A new player in SecurityResearch: the European Network of Law Enforcement Services (ENLETS)' (2010) 21/2 Statewatch <http://www.statewatch.org/subscriber/protected/sw21n2.pdf> accessed 28 June 2018.

van Zonneveld B, 'Nieuwe chip maakt auto doelwit' (Technisch Weekblad, 29 June 2013) <https://www.technischweekblad.nl/nieuws/nieuwe-chip-maakt-auto-doelwit/item4237> accessed 29 February 2016.

VPRO Tegenlicht, 'Bureau voor digitale sabotage' (Interview with Eleanor Saitta: excerpt starts from 12:50, Tegenlicht 2 March 2014) <https://www.vpro.nl/programmas/tegenlicht/kijk/afleveringen/2013-2014/bureau-voor-digitale-sabotage.html>, 2 July 2018.

Waugh R, 'The CIA wants to spy on you through your TV: Agency director says it will "transform" surveillance' (Mailonline, 16 March 2012)

<http://www.dailymail.co.uk/sciencetech/article-2115871/The-CIA-wants-spy-TV-Agency-director-says-net-connected-gadgets-transform-surveillance.html> accessed 7 June 2018.

Werkgroep Verkenning Kaderwet Gegevensuitwisseling, 'Kennis delen geeft kracht Naar een betere èn zorgvuldigere gegevensuitwisseling in samenwerkingsverbanden'(Rapport van de Werkgroep Verkenning kaderwet Gegevensuitwisseling, Den Haag, 5 December 2014) 24.

What-when-how, 'Fair information practices' <http://what-when-how.com/privacy/fair-information-practices/> accessed 7 June 2018.

Acknowledgements

I always like to compare research with travelling into unchartered territory and this research has been quite the journey in which I owe many thanks to all the helping hands.

First of all to my supervisors and co-supervisor. I owe the greatest gratitude to Arno Lodder for his trust and the full freedom he gave to me to develop my own ideas about this research, whilst encouraging me all the way. Thank you for remaining patient and allowing me to visit the land of eCall, while the time for exploring was officially over. I would like to thank Andrew Murray for joining this journey despite the fact the ship already left the harbour some years earlier. Your apt criticism and positive comments blew fresh wind in the sails. I also would like to express my gratitude to Tina van der Linden. Tina your positivity and kindness had already inspired me to study harder ever since we met in Utrecht when you let me finish your course despite the delay due to my concussion. You also offered me the prospect of publishing my thoughts early on, which was a lesson in itself that I still benefit from.

I would like to thank my colleagues at the Faculty of Law of the VU, especially of the departments of TLS and Legal Theory, for making this such a great place to work.

I would like to thank my friends for all the support they showed me throughout my PhD. Special mention goes to Reint, Maurits, Cata, Katya and Steef for their relentless support.

Thanks to my mother, my sisters, Harry and my brothers-in-law –for standing by my side in some of the less easy times. A special word of gratitude goes to my mother who has been a constant source of support, strength and laughter. I dedicate this book to her.

Finally, I would like to thank my wife Nara who helped to pilot this entire thing to a finish. Your love and support towards the end has been invaluable and it would have taken me at least another year drifting off the shore if it wasn't for you. I'm looking forward to the next journey with you by my side.