Faculty of Law
University of Helsinki
Helsinki, Finland

PERSONAL DATA PROTECTION ON THE INTERNET OF THINGS
AN EU PERSPECTIVE

Jenna Lindqvist

ACADEMIC DISSERTATION

Doctoral dissertation to be presented for public examination, by due permission of the Faculty of Law at the University of Helsinki in Auditorium XII at the University's main building, on the 15th of December, 2018 at 10 o'clock.

Helsinki 2018

ISBN 978-951-51-4752-3 (painettu)
ISBN 978-951-51-4753-0 (PDF)

Unigrafia Oy
Helsinki 2018

Acknowledgements

I started writing my doctoral dissertation with great enthusiasm. I had found a topic that was quite novel and I planned on solving a lot of issues relating to personal data protection legislation in the EU. However, when I started writing, I noticed that the more I learned about the field of information law, the more confusing it became. Simple terms such as 'personal data' that were once completely clear to me, become dim and I felt that instead of moving forward, I had taken many steps back. After consulting some of my colleagues at the university, I understood that it was a necessary part of the phd process. Now looking back at my years of research, I can see how they were right. When I started, also the term 'Internet of Things' was not very commonly accepted. It was seen more as a buzzword, and a technology of the future, which could only be studied in theory. Now, at the end of my PhD project, IoT is a word that everybody understands and most of the people I know own at least one smart device.

I would like to take this opportunity to thank the people and organisations, that contributed to my dissertation in one way or another. I would like to start by extending my huge appreciation to my supervisor, Professor Päivi Korpisaari, who inspired me to write a doctoral dissertation. Without her encouragement, I would never have applied for a position as a doctoral candidate in the first place. Päivi has supported me, given me valuable advice and acted as a huge inspiration throughout the process. Together we have attended and organised numerous seminars, and as time went by, we became good friends. Thank you so much Päivi, not only for your help with my writing, but for always staying positive, and spreading good mood and a can-do attitude, which has given me so much joy and confidence.

I would like to thank Docent Olli Pitkänen for agreeing to act as my opponent. A big thank you also to Professor Rauno Karhu and Doctor Paul Bernal, who acted as preliminary examiners of my dissertation. I received good feedback and constructive criticism from them, which helped me finalise the research and pushed me over the finishing line.

Furthermore, this dissertation would not have been possible without financial support. I'd like to thank Emil Aaltosen säätiö and Business Finland (earlier called Innovaatiorahoituskeskus Tekes) for your generous funding, which has allowed me to focus on my research full-time. During the past years, I have worked in three research groups: Henkilötietojen suoja digitalisoituvassa yhteiskunnassa, The MyGeoTrust project, and Information Security of Location Estimation and Navigation Applications (INSURE). The latter two were multi-disciplinary, giving me an insight into the technological side of my research topic. I do believe that to be able to fully understand legislation legislating technology, you also have to understand the technology itself. Thank you to all members of the teams, and a special thank you to Robert Guinness and Professor Heidi Kuusniemi, who initiated and managed the projects, giving me the opportunity to blend in with engineers as a counterbalance to all the legal minds.

This project would not have been possible without the help and support from my family. I am for ever thankful for all your unselfish love and kindness. Lastly I would like to thank you my wonderful husband Niklas for supporting me throughout this process. I finished the dissertation on maternity leave. I was writing the finishing touches to my last article at the moment we left for the hospital to give birth. Niklas had to literally drag me away from the computer. Thank you my love for taking the responsibility for our daughter and our household and for allowing me to finalise my dissertation. I would also like to thank our daughter Amelie for being the easiest, happiest baby in the world, letting us sleep

and giving me energy to work on my research, despite of all the strain of life with a little baby. Thank you for being there!

Abstract

The Internet of Things ('IoT') has become an important part of major cities' infrastructure, where the quality of life is improved by, for example, connected healthcare, transport, and parking. The IoT is also present in homes where the technology is used for home-automation, such as automated heating, -lighting, or -appliances. People also use smart devices to monitor their health and daily activities. Along with the increasing use of smart technology, personal data are often collected and recorded, and they can, for example, be used to derive the location of a person's home or workplace, to monitor habits and lifestyle, or to target advertisement based on the data subject's interests.

As the traditional Internet has developed into the IoT, personal data protection law has also expanded from being a niche field of law, into a legal area that is applicable in almost all sectors, services, and technologies. Globalisation and the vast technological development, and elaborated collection of data, has raised questions about whether the current EU data protection legislation can cope with the new challenges that the IoT poses.[1] Some of the issues identified by the European Commission ('Commission') include: a need to more clearly define how the data protection principles apply to new technologies; the need for harmonisation between EU Member States' data protection legislation; a need for additional regulation of data processors; and the need of better ensuring enforcement of

[1] European Commission Communication, 'A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final, 2-4.

data protection rules.[2] As a result, the Commission undertook to propose a new EU data protection legislation, to replace the Data Protection Directive ('DPD'), and to better cope with modern data protection issues, the legislation which we now know as the General Data Protection Regulation ('GDPR'), and which became applicable in 2018.

This article-based doctoral dissertation sets out some of the key elements of the EU data protection reform package that has been processed for the past six years, and highlights some of the main changes in comparison to the situation governed by the outdated DPD. The main method is legal dogmatic with elements of both 'legal-political' and 'problem-centred' methods. The context of the research is the IoT and personal data challenges brought by it to data subjects, mainly by private stakeholders. As will be identified in this dissertation, the IoT poses challenges to personal data protection mainly because the amount of personal data that is collected has increased substantially, and because information is gathered from so many different, scattered sources. In addition, the form of automatic communication between smart devices makes it difficult to apply fundamental transparency and fairness principles. This dissertation investigates the complexity of the legal state in EU surrounding personal data protection in the context of the IoT. The articles forming the dissertation outline changes both in law, and the world at large, point out legal unclarities, and contribute to the academic discussion about the possible effects of the GDPR. In a nutshell, this study aims to answer the question: *Is the GDPR fit to deal with new technologies such as the IoT?*

[2] ibid.

Content

List of publications

This doctoral dissertation consists of a summarizing report and the following original publications listed in the chronological order of publication:

I. Article I: Jenna Mäkinen, 'Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things' (2015) Information & Communications Technology Law 24/3, 262-277.

II. Article II: Jenna Lindqvist, 'The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges' In Tobias Bräutigam & Samuli Miettinen (eds.) *Data Protection, Privacy and European Regulation in the Internet Age* (Forum Iuris, Helsinki 2016) 84-109.

III. Article III: Jenna Lindqvist, 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' 26 (2018) International Journal of Law and Information Technology 45–63.

IV. Article IV: Jenna Lindqvist, 'Automated vehicles and personal location data in a smart world – an EU perspective' (under peer review).

Abbreviations

AG Advocate General

Board European Data Protection Board

CASAGRAS Coordination and support action for global RFID-related activities and standardisation

Charter Charter of Fundamental Rights of the European Union

CJEU Court of Justice of the European Union

Convention UN Convention On The Rights Of The Child

Convention 108 Convention for the protection of individuals with regard to the automatic processing of personal data

Council the Council of Europe

COPPA US Children Online Data Protection Act of 1998

Data Retention Directive Directive 2002/58/EC (OJ L 105 13 April 2006)

DPA the Data Protection Authority

DPD 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 OJ L 281 , 23/11/1995 p. 31-50.

ECHR European Convention on Human Rights

ECtHR European Court of Human Rights

EU European Union

FGI Finnish Geospatial Research Institute

GDPR General Data Protection Regulation

GDPR 2012 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data

and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final.

ICCPR International Covenant on Civil and Political Rights

IoT Internet of things

LIBE Committee on Civil Liberties, Justice and Home Affairs

MAC media access control

OECD Organisation for Economic Co-operation and Development

OJ Official Journal

Parliament the European Parliament

TFEU Treaty on the Functioning of the European Union

WP29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. Introduction

1.1. Background to the topic

The Internet has moved from just computer screens to other objects and invisible sensors, forming a system that connects so-called 'smart things' to the Internet. This system is called 'the Internet of Things'[3] ('IoT') and it bridges the gap between the physical- and the online worlds. The IoT brings with it enormous potential for both individuals and businesses. It can, for example, help us save energy and it can bring with it large lifestyle improvements for individuals in sectors such as home-automation, health, and transport. At the same time, the IoT poses significant privacy, security, and data protection challenges and it has demanded a closer look into how the European Union ('EU') legal framework is applied in the IoT context.

Technologies have been seen as 'privacy-destroying' and some scholars feel that technologies are pushing us into an era of 'zero informational privacy'.[4] Smart devices create a world of so-called 'multiveillance', which means 'surveillance not just by the state but by companies, marketers, and those in our social networks'.[5] The classical privacy cases relate to so-called 'public disclosure of private facts' and 'intrusion upon an individual's seclusion, solitude, or private affairs'. However in a digitalised world, so-called computerised personal data has become an important part of the privacy discussion.[6]

[3] For more detailed definition of the IoT, see Section 2.1. of the summarising report.

[4] A. Michael Froomkin, 'The death of privacy?' (2000) 52 Stanford Law Review 1461, 1465.

[5] Neil Richards, *Intellectual privacy rethinking civil liberties in the digital age* (Oxford University Press 2015) 6.

[6] Raymond Wacks, *Law, Mortality and the Public Domain* (Hong Kong University Press 2000) 241.

IoT poses challenges to personal data protection and privacy mainly because the amount of personal data that is collected has increased substantially and because information is gathered from so many different, scattered sources. In addition, the form of automatic communication between smart devices makes it difficult to apply fundamental transparency and fairness principles. Furthermore, in practice, the need for innovation often overrides the need for privacy regulation and some feel that data protection legislation stiffens innovation altogether. Some of the main risks include intrusive use of smart devices by controllers and processors, unauthorised access to personal data, unlawful surveillance and hacking, and data losses.[7] Also manipulation and loss of equality have been identified as two major issues that new technologies cause personal data protection. Legal scholars are worried about how new technologies control people's desires and that in the end, the technologies may cause a 'normalisation' of the population, as well as discrimination, such as price discrimination.[8]

As the traditional Internet has developed into the IoT, personal data protection law has also expanded from being a niche field of law, into a legal area that is applicable in almost all sectors, services, and technologies.[9] As a result, the EU legal data protection framework has undergone a reform during the past years. After lengthy negotiations lasting almost six years, the EU Parliament has approved a final version of a new General Data

[7] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (WP 223, 16 September 2014) 3.

[8] Lawrence Lessig, *CODE* (Version 2.0 Basic Books, New York 2006) 220.

[9] Christopher Kuner, 'Data Protection Law and International jurisdiction on the Internet (Part1)'(2010) 18 International Journal of Law and Information Technology 176, 176.

Protection Regulation in April 2016.[10] The Regulation became directly applicable in all EU member states on 25 May 2018.[11]

1.2. Objectives and scope of the study

1.2.1. Research questions

This dissertation investigates the complexity of the current legal state in the EU surrounding personal data protection in the context of new technologies, namely the IoT. The articles forming the dissertation map out changes both in law and the world at large, point out unclarities, and contribute to the academic discussion about the possible effects of the GDPR. This dissertation further presents an analysis of the societal significance of the field of information- and communication law, as well as monitors the development of core information law issues, especially relating to personal data protection in a new technological environment. This dissertation focuses on real-life issues with the aim of exemplifying and illustrating the recent developments within EU information law; and in that way adding to the academic *de lege ferenda* discussion surrounding the IoT and the law, which is both very topical and challenging at the same time.

Most of this study would apply as-is to EU data protection in general (eg, issues relating to social media or GPS technology). However, even though the law is technology neutral in theory,[12] there can be differences in *interpretation* depending on which

[10] 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 95/46/EC (General Data Protection Regulation) OJ L 119/1 4.5.2016, p. 1–88 ('GDPR').

[11] Homepage of EU GDPR <https://www.eugdpr.org> accessed 21 December 2017.

[12] Accordning to GDPR, Rec. 15, 'the protection of natural persons should be technologically neutral and should not depend on the techniques used'.

technology is used to collect and process personal data.[13] Thus this provides grounds for a narrower focus on IoT technology. The research question of this study can be compressed as follows: *Is the GDPR fit to deal with new technologies such as the IoT?* I approach the main research question from the following different perspectives:

1. Article I provides a general introduction to the purposes and vision of the IoT and its impact on EU data protection legislation. The paper deals with provisions relating to joint controllership, sensitive personal data, and data quality principles with the aim of discussing the question of whether the IoT violates human identity and the right to privacy.
2. Article II describes and analyses the privacy protection mechanisms offered to children in the context of the IoT. The aim is to question whether the need for improved protection of children's personal data is going to be fulfilled by the GDPR. The main focus is placed on the articles of the GDPR that relate to data quality principles, security, and legitimacy of processing. Furthermore, the article 'aims to expose the need for clearer interpretation of children's data protection rights in an IoT context'.[14]

[13] To give an example, in determining whether a person is 'identifiable' in accordance with the GDPR, one of the the key questions is whether the means used by the data collector 'are reasonably likely to be used to identify the natural person'. In such cases, account should be taken of 'the available technology at the time of the processing and technological developments'. See GDPR, Rec. 26. Indirectly implying that the nature of data depends on the used technology.

[14] Jenna Lindqvist, 'The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges' In Tobias Bräutigam & Samuli Miettinen (eds.) *Data Protection, Privacy and European Regulation in the Internet Age* (Forum Iuris, Helsinki 2016) 84, 85.

3. Article III studies the expanded obligations of data processors and provides a better understanding of the intersection between personal data controllers and -processors. The focus lies on the contractual relationship between the parties and the changes to those relationships brought by new technology and the GDPR. Focus is placed on the distribution of responsibility between the contracting parties, with the main aim of investigating whether the GDPR is fit to deal with the IoT technologies in this context.
4. Article IV approaches the research question of the dissertation through an analysis regarding automated vehicles and personal location data collected or processed by them. The article answers questions such as 'what is meant by personal location data?' and 'what challenges do automated vehicles pose on EU data protection legislation?'. The core Articles of the GDPR that are analysed are related to lawful processing and data quality principles.
5. Lastly, overarching common factors are identified from the research results of the articles.

This overview provides the objectives of the published articles as a whole, the methodological and theoretical framework, a description of the foundations and core matter of the overarching themes of the articles, namely the technological environment, human rights aspects relating to privacy, and key factors about data protection law in the EU. The summarising report also places the research at hand into a field of law, namely that of information- and communications law. Furthermore, the overview produces a summary of the findings of the publications and an analysis of the meaning and importance of said findings.

1.2.2. Limiting the scope

Personal data issues concerns can be divided into two broad categories:

1. Government access to personal data; and
2. Private commercial use and processing of personal data.[15]

This study focuses on personal data processing and collection executed by private actors. Furthermore, the focus of the study is on EU law, namely the DPD and the GDPR, as the majority of national legislation within EU member states will soon be either outdated and/or renewed.

IoT technology is in the focus of the study, however it is a very broad concept, which reaches from manufacturing- and industry machinery to consumer applications. This dissertation concentrates on the latter, such as wearable technology, home automation, smart vehicles, and quantified-self devices. The reason for choosing this scope is that these devices are already in consumer use and have given reason to question how the EU data protection laws apply to them and to their users. As the aim is to draw parallels to real-life issues, these technologies are well suited as examples when illustrating the current state and analysing the adequacy of the GDPR now and in the future. Fully automated vehicles, which Article IV focuses on, are not in consumer use yet. Many vehicles in consumer use are however partly automated and therefore the technology also works well as a subject in the discussion.

In tandem with the GDPR, a new regulation concerning the respect for private life and the protection of personal data in electronic communications has been developed to

[15] William J. Kohlert & Alex Colbert-Taylor 'Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles' (2014-2015) 31(1) Santa Clara Computer and High Technology Law Journal <http://digitalcommons.law.scu.edu/chtlj/vol31/iss1/3/> accessed 17 November 2017, 121.

replace the Directive on privacy and electronic communications (eDirective).[16] While the GDPR is grounded on Article 8 of the Charter of Fundamental Rights of the European Union [2007] OJ C-303/01 ('Charter') (protection of personal data), the upcoming ePrivacy regulation is based on Article 7, which protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. The protection of electronic communications is crucial on the IoT and the IoT is mentioned literally in the proposal text of the ePrivacy Regulation. The proposal states '[c]onnected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things) (…). In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications'.[17]Furthermore, the proposal text states that '[t]he principle of confidentiality should apply to current and future means of communication'[18], indirectly including IoT. Until the reform process finishes, the ePrivacy Directive remains applicable. The Directive is *lex specialis* in relationship to the GDPR.[19] However, regardless of the tight connection between the GDPR and ePrivacy, a

[16] 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), OJ L 201, 31.7.2002.

[17] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003 (COD), Rec 12.

[18] ibid. rec 1.

[19] Communication from the Commission to the European Parliament and the Council - Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018' COM(2018) 43 final.

deeper analysis of the ePrivacy Regulation falls outside the research themes of this dissertation.

1.3. Methodology and source material

1.3.1. Methodological pluralism

There is no universally applicable research methodology in the legal doctrine, leaving it up to the researcher to form his, or her, own search strategy and methodical approach.[20] Furthermore some suggest that it is wise for legal scholars 'to postpone the discussion of method' until 'the end of their academic work', since 'methodological problems require an amount of detachment and wisdom that is not likely to be acquired at an earlier stage'.[21] Hence, I have saved the discussion about method to this summarizing report instead of discussing it in each article separately. As further identified by *Georg Schwarzenberger* '[m]ethods are but tools, and tools ought to be chosen with special regard for the material to which they are to be applied'.[22] The material of this research is multiform and consists of both material that is purely focused on legislation, but also sociological and technology oriented source material, sometimes making the choice of method controversial.

Generally speaking, a scientific method consists of the researcher's 'logic of discovery' and 'logic of justification' of the scientific community.[23] The logic of discovery refers to the researcher's solitary and unique findings (innovations), whilst logic of justification needs to be possible to generalise and possible to repeat (control). A successful methodology makes it possible to transition from logic of discovery to logic of justification,

[20] Ari Hirvonen, *Mitkä metodit? Opas oikeustieteen metodologiaan* (Helsinki 2011) 7.

[21] Georg Schwarzenberger, 'The Inductive Approach to International Law' (1947) 60(40) Harvard Law Review 539, 539.

[22] ibid.

[23] Raimo Siltala, *Oikeudellinen tulkintateoria* (Jyväskylä 2004) 507.

and *vice versa*, in a way that creates variance to the research in the field.[24] In this study, more weight has been placed on the logic of justification than on unique innovations. This is also typical in the field of law, contrary to natural sciences, for example, where the logic of discovery usually is the main objective in the study.

The innovative and unique part of this study consists mainly of an analysis of whether the reformation of the EU data protection legislation is successful and how it should be interpreted in the future (*de lege ferenda*). The study also aims at contextualising legislation and at pointing out grey areas in valid law. Even though the GDPR is applicable at the time of the publication of this doctoral dissertation, the research was conducted prior to 25 May 2018 and the start of the application of the Regulation, rendering the study of the legislation challenging. Without proper judicial practice in place, it is difficult to draw a line between *lex lata* and *de lege ferenda.*[25] Furthermore, at the beginning of this doctoral research, the final version of the GDPR was not yet confirmed, which means that the legislation was both not yet applicable, as well as not even in effect yet. Thus, for the purpose of this study, the analysis of the GDPR, falls somewhere between *lex lata* and *de lege ferenda*. In the current state, however, the GDPR can be viewed as *lex lata*, whilst the application of the regulation, due to the short time that it has been applicable, still needs to be viewed as *de lege ferenda*.

The main aim of the study is to interpret and analyse the GDPR and its implications on smart technology and *vice versa*. Therefore, the legal dogmatic methodology is employed in the research. The research subjects of the legal dogmatic method are valid legal norms. Jurisprudence produces statements about the interpretation of the valid law. It

[24] Siltala *Oikeudellinen tulkintateoria* (n 23) 507.

[25] Lee A. Bygrave, *Data Protection Law Approaching Its Rationale, Logic and Limits* (Kluwer Law International 2002) 16.

is also possible but rare that the legal dogmatic statements actually claim something about the *de facto* validity of a legal norm. Instead, interpretive statements about the content of the law are usually presented, which is the methodological approach applied in this dissertation.[26] The legal dogmatic method also makes it possible to examine legal principles and to weigh them against each other.[27] This is an important tool in studying new legislation, since in the absence of existing precedents or a comprehensive doctrine, general legal principles often lead the way in interpreting the meaning of the norms *in casu*. Additionally, the effort to identify 'what is valid law' in a relatively new field of law, such as information law, it is sometimes appropriate to replace the question with 'what is valid law in a given context?'[28]

De lege ferenda research is indeed also sometimes called legal political (in Finnish 'oikeuspoliittinen') research. It focuses on identifying legislative solutions and approaches that upcoming legislation could be based on. As has been identified by *Antti Kolehmainen*, the *de lege ferenda* based solutions are often born as a bi-product of systematisation and interpretation in accordance with the legal dogmatic method.[29] Personal data protection legislation touches many areas in the society and relates to timely social issues, such as mass surveillance, rapid technological development, and fundamental privacy challenges. Therefore, a study about the GDPR also includes research into the social implications and issues that have led to the need for data protection legislation in the first place. *Urpo Kangas* has provided a methodological alternative to address such legal research issues,

[26] Siltala, *Oikeudellinen tulkintateoria* (n 23) 346.

[27] Hirvonen (n 20) 24.

[28] Bygrave, *Data Protection Law Approaching Its Rationale, Logic and Limits* (n 25) 15.

[29] Antti Kolehmainen 'Tutkimusongelma ja metodi lainopillisessa työssä' in Tarmo Miettinen (ed.) *Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta* (Edilex 2016) 108.

namely the 'problem-centred' jurisprudence (in Finnish 'ongelmakeskeinen lainoppi'). This method aims to analyse not only the legal provisions *per se*, but also how the law solves (or does not solve) the social legal issues that have put in motion the legislation process to begin with.[30] In conclusion, the method applied in this research is mainly legal dogmatic with elements of both 'legal-political' and 'problem-centred' methods. In fact 'methodolical pluralism' is common in legal research and brings pluralism to the research,[31] and it is especially well-suited for the field of, the ever-changing, information- and media law.

1.3.2. Source material

The target audience for this study is academics, researching EU legislation in the information and media law fields. Consequently, I have favoured sources written in English. However, the dissertation is an academic submission in Finland, and therefore the chosen doctrine of legal sources is a Nordic one and this necessitates the use of Nordic, and especially Finnish sources in this particular chapter.

Because of the fast development of technology and increased attention on human rights, data protection laws and instruments have been on the rise for decades.[32] Data protection research has consequently also given rise to an increasing amount of legal literature.[33] Among the ample quantity of available source material, focus in this study has been concentrated on material that is deemed by the author to be most relevant with regard to the specific research questions in each article. Furthermore I have prioritised new up-to-

[30] Urpo Kangas 'Minun metodini' in Juha Häyhä (ed.) *Minun metodini* (Porvoo 1997) 106-107.

[31] Hirvonen (n 20) 9.

[32] David Banisar and Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (1999) 18(1) John Marshall Journal of Computer and Information Law.

[33] Bygrave *Data Protection Law Approaching Its Rationale, Logic and Limits* (n 25) 14.

date sources. *Lee A. Bygrave* calls this a 'sampling strategy with respect to data protection'.[34] The sources of law need to be analysed in order to be able to differentiate between binding rules and subjective views and opinions. The doctrine of legal sources helps us in the determination of on what legal interpretation and findings should be based, as well as provides an indication of how to define the normative significance of material and place sources in a 'legal source hierarchy'.[35] In other words, the doctrine analyses the mutual relations between legal sources and defines the 'order of preference'.[36]

The doctrine consists of 'a descriptive and a normative part'. As has been identified by *Kaarlo Tuori* '[t]he descriptive doctrine focuses on the way the sources of law are in fact employed, whereas the normative part formulates normative guidelines for the identification and ordering of the sources'. He adapts the 'Scandinavian doctrine of the sources of law' that has been developed mainly by *Aleksander Peczenik*[37] and *Aulis Aarnio*[38]. According to the scholars, the sources of law can be divided into three groups: strongly obliging-, weakly obliging-, and permitted sources.[39] As the terms imply, the strongly obliging sources override the weakly obliging- and the permitted sources. However, weak sources can sometimes be overridden by permitted sources if it is based on cogent argumentation.[40] Legislation is a strongly obliging source, whilst travaux preparatories and precedents of supreme courts constitute weakly obliging sources. The

[34] Bygrave *Data Protection Law Approaching Its Rationale, Logic and Limits* (n 25) 14.

[35] Päivi Tiilikka, *Sananvapaus ja yksilön suoja* (Helsinki 2007) 27.

[36] Kaarlo Tuori, *Critical Legal Positivism* (Routlege 2017) 157.

[37] Aleksander Peczenik, *On Law and Reason* (Dordrecht: Kluwer 1989) 319-320.

[38] Aulis Aarnio, *The Rational as Reasonable* (Dordrecht: Kluwer 1987) 89-90.

[39] Tuori *Critical Legal Positivism* (n 36)158-159.

[40] Tiilikka (n 35) 28.

praxis of other (lower) courts and legal scholarship are only considered as permitted sources.[41]

The Constitution, international treaties, and EU legislation are placed above legislation in the source hierarchy. However, because of the scattered and varying nature of new EU rules relating to personal data protection, one could argue that the different sources cannot longer be separated in this field of law. Especially in Europe, the perspectives are 'gradually blurring as a result of an increasingly less formal and more substantive legal culture'.[42] However 'to successfully carry out the task of legal interpretation requires first having *some* working conception of legal systematics'.[43] Keeping that in mind, the EU has indeed brought with it challenges to the doctrine of legal sources; Whilst the legislation has kept its strongly obliging character, the judgments of the Court of Justice of the European Union ('CJEU') are in a central role in the development of EU legislation. In other words EU law can be seen as a combination of an Anglo-American common law system and the Roman-German system ruling on the Continent.[44] Especially in the Nordic countries, the importance of legislation appears in the importance that courts put on it as well as on the travaux preparatories. However, in EU law the praxis of the EU courts is seen as a more important source of law than the national travaux preparatories. Furthermore, the courts of EU member countries must apply EU norms instead of national legislation if a conflict

[41] Tuori *Critical Legal Positivism* (n 36) 157-158.

[42] Martijn Hesselink, 'A European Legal Method? On European Private Law and Scientific Method' (2009) 15(1) European Law Journal 20, 30.

[43] Raimo Siltala *Law, Truth, and Reason: A Treatise on Legal Argumentation* (Springer Turku 2011) 263.

[44] Kaarlo Tuori *Ratio ja voluntas* (Alma Talent Oy 2007) 253-254.

between the two occurs, and this may result in that the court praxis succeeds the preparatory works in the Nordic legal source doctrine in the future.[45]

The GDPR was not applicable during the writing process of this dissertation, creating uncertainty relating to the possible effects of the Regulation. As a result, an independent research grasp is required, as well as an inventive use of sources. Therefore the traditional sources of law have to make room for non-legal sources and less binding sources, such as 'permitted sources' in the analysis. However, I do not challenge the conventional doctrine of legal sources. I simply *use* the sources in the quantity that provides more space to the literature and other permitted sources. The wording of relevant legislation, namely the DPD and the GDPR, still remain the core material of the study. The main objectives of the DPD: the protection of the right to data protection and the achievement of an internal market, are also the core aims of the GDPR. This means that many of the articles of the DPD remain sound.[46] Hence, source material analysing, or discussing, the content of the DPD can be applied also to the GDPR, if the content has not considerably changed.

Much weight has been placed on the research covering opinions and reports of the 'Article 29 Working Party' ('WP29' or 'Working Party'), and hence it is in order to provide a description of the authority and impact of the decision making of the WP29. The full name of the WP29 is 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data'. It is an advisory body and it acts independently. The WP29 was established by Article 29 of the DPD, from which it also gains its short name 'WP29'. The WP29 consists of 'a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities

[45] Tuori *Ratio ja voluntas* (n 44) 253-254.

[46] COM (2010) (n1) 2.

established for the Community institutions and bodies, and of a representative of the Commission'.[47] The tasks of the WP29 are defined in Article 30 of the DPD. It shall examine questions covering the application of the national measures adopted under the DPD with the aim of harmonising the application in EU. The WP29 further provides 'recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community'.[48] It is clear that in the classic hierarchy of legal sources, the opinions of the Working Party are not as authoritative as the findings, for example, of the CJEU or the European Court of Human Rights ('ECtHR'). However judges of said courts have referred to opinions of the Working Party in their argumentation, thus giving some importance to the opinions and justifying the use of them as source also in this study.[49]

As of the application of the GDPR, the WP29 has been replaced by a new body, the European Data Protection Board ('Board').[50] The Board is an independent body of the EU and it consists of the heads of the Member States' supervisory authorities and the

[47] 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 OJ L 281 , 23/11/1995 p. 31-50 ('DPD'), art 29.

[48] DPD, art 30.

[49] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, Opinion of AG Campos Sánches-Bordona, paras 57 and 66; Case C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] OJ C 381, Opinion of AG Cruz Villalón, paras 30-40 and 62; Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, Opinion of AG Jääskinen, paras 30 and 57; Case C-131/12 *Google Spain SL and Google Inc v Agencia Espagnola de Proteccion de Datos (EPD) and Mario Costeja Gonzales* [2014] ECR I-317, Opinion of AG Jääskinen, paras 16, 31, 36, 55-56, 65, 71, 81, 83, 85, 88, 135; Case C-70/10 *Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs (SABAM)* [2011] ECLI:EU:C:2011:771, Opinion of AG Cruz Villalón, para 76.

[50] GDPR, arts 68-76.

'European Data Protection Supervisor' or its representatives. The Board's main task is to contribute to a consistent application of the GDPR in EU.[51]

1.4. Field of study

1.4.1. Information- and communication law

Personal data protection issues have slowly spread their tentacles into most fields of law and it may even be pointless to pin it to one specified field or sector. As a result, a study in data protection law needs to be drawn upon research within multiple fields of law. Yet, from a heuristic and pedagogic point of view,[52] it is sensible to place research into a category, and therefore it can be concluded that the underlying field of law that this dissertation focuses on is *information- and communication law*.

There is no exact definition for what is meant by 'field of law'. However one way to look at it is as a classification of norms based on the object of the legislation.[53] Nevertheless, this view can be criticised, because the same norms can be classified into many different fields of law and therefore it might be more productive to categorise the field of law based on the object of the research instead of the object of the regulation.[54] This is, in my view, the best way to look at information- and communication law, which analyses and systematises legal norms that relate to information technology and communication in general. The fact that information- and communication law focuses on a

[51] GDPR, rec. 139; for a detailed list of the Board's tasks, see GDPR, art. 70.

[52] Kaarlo Tuori, 'Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota' (2004) 7-8 Lakimies 1196, 1202.

[53] Päivi Korpisaari, 'Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta' (2015) 7-8 Lakimies 987, 989; Tuori, 'Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota' (n 52) 1200.

[54] Korpisaari 'Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta' (n 53) 989-990.

specific subject matter does not mean, however, that it is automatically a 'field of law'. Otherwise one could just attach the word 'law' into any social phenomenon and we would have a new field of law. For example just by attaching the word 'law' to the word 'social media', does not mean that there is a legal field called 'social media law'.

Indeed there are criteria that can be used to define a field of law. The key element is that a field of law has its own 'general doctrines' (in Finnish 'yleiset opit').[55] Also, the meaning of the term 'general doctrine' is up for debate, but in general it means general legal principles (in Finnish 'yleiset oikeusperiaatteet') and fundamental concepts (in Finnish 'peruskäsitteet').[56] The aim of the general legal principles is to make law foreseeable and to create legal security, and in that way guaranteeing justness and fairness when interpreting the law.[57] Information- and communication law is not a 'classic' field of law such as constitutional law, labour law, or family law. It is a 'new-comer' in the fields of law together with similar fields such as 'sports law' or 'stock market law'.[58] Therefore it is reasonable, in a doctoral dissertation that is placed within the field of information- and communication law, to establish exactly what the field means and what makes it a field of law in the first place.

The general legal principles that make information- and communication law a 'field of law' have been analysed by different scholars with somewhat different views. *Ahti*

[55] Kimmo Nuotio, 'Oikeuslähteet ja yleiset opit' (2004) 7-8 Lakimies 1267, 1275.

[56] ibid; Tuori, 'Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota' (n 52) 1203.

[57] Tuori, 'Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota' (n 52) 1219.

[58] Päivi Korpisaari, 'Viestintäoikeus globaalissa yhteiskunnassa' in Päivi Korpisaari (ed.) *Viestintäoikeus nyt – Viestintäoikeuden vuosikirja 2014* (Forum Iuris 2015) 11.

Saarenpää has identified the following general legal principles to help define 'person- and information law' (in Finnish 'henkilö- ja informaatio-oikeus')[59]:

- The right to information
- The right to privacy
- The right to communication
- The right to data security
- The right to quality[60]
- The right to legal security

Following similar lines, *Päivi Korpisaari* has defined the following general legal principles to govern information- and communication law[61]:

- Freedom of expression, including the right to information
- The right to privacy
- The right-of-access principle
- The confidentiality principle
- Technology neutrality (in Finnish 'välineneutraalisuus')
- The principle of communication pluralism
- Ban of misuse of freedom of speech
- The respect of human dignity and integrity

As these lists make clear, fundamental rights play a crucial part in the field. That is also why this summarising report includes an analysis about the right to privacy as well as a

[59] Ahti Saarenpää, 'Verkkoyhteiskunnan oikeutta: johdatusta aiheeseen' (2000) 29(1) Oikeus 3, 14 (translation by author).

[60] I assume with this Saarenpää refers for example to the data quality principles found in the DPD and the GDPR.

[61] Korpisaari 'Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta' (n 53) 994-995 (translation by author).

reflection of the intersection between the right to privacy and personal data protection. Furthermore the general legal principles of a 'new field of law' need to be able to be fixed to normative material, precedents, and research,[62] something that this dissertation will discuss and contribute to.

1.4.2. Multidisciplinary research: technology and law

Writing about a subject that includes numerous technological facts is sometimes challenging for a lawyer. One needs to dive into technology and understand the underlying instruments, which form the object of the law and, by implication, the research at hand. At the same time, one must be careful not to go into the technology matter in too great detail, because that might shift the focus from the real subject: *law*. In preparation and groundwork for this dissertation I have read a great deal of non-legal source material, but avoided to open up too many technology-related definitions in the actual body type of the thesis. The aim is not to meander and as a consequence stray too far from the right subject.

For this research, I have received funding from three sources: 1) Emil Aaltosen säätiö for a project called 'Henkilötietojen suoja digitalisoituvassa yhteiskunnassa', which translates 'Protection of personal information in a digitalising society'; 2) Tekes, the Finnish Funding Agency for Innovation (nowadays called 'Business Finland'), for a project called 'MyGeoTrust', which is a consortium research project between the Finnish Geospatial Research Institute ('FGI'), which is a part of the National Land Survey and the Faculty of Law at University of Helsinki; and 3) the Academy of Finland for a project studying 'Information Security of Location Estimation and Navigation Applications' ('INSURE'). The core partners of the INSURE consortium are the FGI, Tampere University of Technology, Aalto University, and the University of Helsinki. The two latter

[62] Korpisaari 'Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta' (n 53) 992.

projects are multidisciplinary and have provided much insight into the technological side of the research themes.

On a more philosophical note, one can question the relationship between autonomous machines and the law. When the 'law as code meets law as literature', questions arise as to how legal rules can affect the behaviour of automated machines.[63] The underlying question relates to technology neutrality and the question of whether law is indeed technology neutral. Some scholars argue that 'to achieve a technology-neutral law, technology specific law is sometimes required'.[64] The GDPR is meant to be a technology-neutral regulation that applies to all technologies now and in the future. It is however crucial to prevent 'legal rules from privileging or discriminating specific technological designs in ways that would stifle innovation'.[65] This can be seen as a contradiction, because in many cases the data protection laws hinder technological innovation. For example, from an innovation-promoting point of view, personal data collection should be maximised in order to be able to exploit and utilise data to the maximum. However, looking at it from a privacy-enhancing perspective, all personal data collection aught to be minimised, a principle that has in fact been strengthened by the GDPR. The only way to solve this 'antithesis' seems to be enacting 'legislation at the right level of abstraction, to prevent the law from becoming out of date all too soon.'[66] There are also arguments, however, that data protection could actually promote innovation—but innovation that favours privacy. *Paul*

[63] Ugo Pagallo 'What Robots Want: Autonomous Machines, Codes and New Frontiers of Legal Responsibility' in Mireille Hildebrandt and Jeanne Gaakeer (eds) *Human Law and Computer Law: Comparative Perspectives* (Springer Dordrecht Heidelberg New York London 2013) 48.

[64] Mireille Hildebrandt and Laura Tielemans, 'Data protection by design and technology neutral law' 29(5) (2013) Computer Law & Security Review 509, 509.

[65] ibid.

[66] ibid.

Bernal has, for example, argued that privacy-invasive technology and business models are more likely to fail, as innovation must be to a degree with consent. He states that 'Privacy helps to foster trust, and in the longer term trust supports business'.[67]

2. The core matter and foundations of the study

2.1. The Internet of Things

2.1.1. Defining the IoT

This dissertation analyses the collection and processing of personal data in the context of the IoT. As stated in section 1.4.2. 'Multidisciplinary research: technology and law', as a legal scholar I must avoid going into too much technical detail and consequently stray from the main focus of the study. Therefore it is not my purpose in this dissertation to provide a comprehensive definition of the technical side of the IoT, but instead to provide a general description of the technology in order to be able to analyse what role it plays in the development of the EU data protection *legislation* reform.

In the beginning of my doctoral studies, six years ago, IoT was more like an abstract concept than a well-known technology that is actively in use. As with so many other technologies, also the IoT technology has taken major leaps forward in a very short amount of time and today it is safe to presume that most people in the Western world own or use at least one smart device either at home or at work. Even though there is no commonly accepted one definition for the IoT, many scholars and authorities have contributed with suggestions for definitions. It has been suggested that a man called *Kevin Ashton* formulated the term 'IoT' already in 1999 in the context of supply chain

[67] Paul Bernal, *Internet Privacy Rights - Rights to Protect Autonomy* (Cambridge 2014) 52.

management.[68] Since then many reports about the IoT have been written by multiple stakeholders[69], authorities and research groups.

The WP29 has defined the IoT as:

> [A]n infrastructure in which billions of sensors embedded in common, everyday devices – 'things' as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.[70]

The EU-funded project, CASAGRAS,[71] in turn, has defined IoT as

> [A] global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and involving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.[72]

---

[68] Kevin Ashton, 'That "Internet of Things" thing' (2009) RFiD Journal <www.rfidjournal.com/ article/ print/4986> accessed 19 February 2018.

[69] Stakeholders can, for example, be device manufacturers, application developers, social platforms, further data recipients, data platforms, and standardisation bodies.

[70] WP29, Opinion 8/2014 (n 7) 4.

[71] CASAGRAS is short for 'Coordination and support action for global RFID-related activities and standardisation'.

[72] European Commission, 'Internet of Things Factsheet Privacy and Security 2012' <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753> accessed 19 February 2018.

And, finally, in a report written to the White House, IoT was defined as[73]

> [A] term used to describe the ability of devices to communicate with each other using embedded sensors that are linked through wired and wireless networks. These devices could include your thermostat, your car, or a pill you swallow so the doctor can monitor the health of your digestive tract. These connected devices use the Internet to transmit, compile, and analyze data.

In a nutshell, the IoT is a system that connects everyday smart objects and –machines to the Internet.[74] The term IoT itself can be split in two words 'Internet' and 'Things'. In this context 'Internet' refers to the network where the communication happens, whilst 'Things' refers to the objects that are integrated to that network.[75] As examples of smart 'Things', this dissertation focuses on:

- Wearable computing, quantified-self devices, and domotics (Articles I and III)
- Smart toys and other smart devices targeted at children (Article II)
- Automated vehicles (Article IV)

[73] Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values' May 2014, <http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf> accessed 19 February 2018.

[74] Marie-Helen Maras, 'Tomorrow's Privacy – Internet of Things: security and privacy implications' 5/2 (2015) International Data Privacy Law 99, 99.

[75] Luigi Atzori and others, 'The Internet of Things: A Survey' (2010) 54 Computer Networks 2787 <http://elsevier.staging.squizedge.net/__data/assets/pdf_file/0010/187831/The-Internet-of-Things.pdf> 2789, accessed 11 May 2018.

IoT is a continuously growing component of big cities' infrastructure and properly managed, IoT technology can make life 'smarter, safer, and more sustainable'.[76] The vision of the IoT is that a so-called 'smart planet' will evolve out of the different IoT systems.[77]

2.1.2. Technology and human values: are ideas and values keeping up with technology?

Intellectual privacy is, as has been identified by *Neil Richards*, 'protection from surveillance or interference when we are engaged in the process of generating ideas – thinking, reading and speaking with confidants before our ideas are ready for public consumption'.[78] Smart devices process and monitor this kind of behaviour and habits. When monitored over time, entities such as Facebook and Google gain a comprehensive profile on each of us. These profiles can then be used possibly in harmful and discriminatory ways. When collected and processed personal data is taken out of context, it can instead of giving a more accurate impression of that person, lead to hasty and false conclusions. In a world where many state that nothing can permanently be forgotten,[79] people (data subjects) are deprived of their fundamental freedom to experiment and

[76] Maged N. Kamel Boulos and Najeeb M. Al-Shorbaji 'On the Internet of Things, smart cities and the WHO Healthy Cities' (2014) 13/10 International Journal of Health Geographics. <https://doi.org/10.1186/1476-072X-13-10> accessed 19 February 2018, 2.

[77] Hermann Kopetz, *Real-Time Systems. Design Principles for Distributed, Embedded Applications* (2nd edn, Real-Time Systems series, Springer Science & Business Media 2011 LLC) 309.

[78] Richards (n 5) 5.

[79] In theory '[a] data subject should have the right to have personal data concerning him or her rectified and a "right to be forgotten" where the retention of such data infringes this Regulation (GDPR) or Union or Member State law to which the controller is subject' GDPR, rec 65 and art 17.

change.[80] Having said that, the situation is at least complex and there are also arguments against the current consensus that 'information, once online, is there forever'.[81] *Meg Leta Ambrose* has, for example, quite convincingly argued that 'we do not know how permanent content on the Web is or what type of information lasts longer than it should, who produces it, or how it is maintained'.[82] To support her argument, she makes references to online books with dead links that no longer lead anywhere. The language of the catch phrase 'right to be forgotten' has also been criticised by scholars.[83] Many interpret it more as a right to obscurity, than to actual erasure of personal data.[84] However, a deeper understanding of the lifecycle of online information would require an 'interdisciplinary approach and the inclusion of research from telecommunications, information theory, information science, behavioral and social sciences, and computer sciences'[85], a concept, which is too nuanced to cover in a legal doctoral dissertation.

As mentioned in the introduction, in practice, the need for innovation often overrides the need for privacy regulation and some feel that data protection legislation stiffens innovation altogether. Innovation, and thus also economic competitiveness, has in a

---

[80] Daniel J. Solove: 'Speech, Privacy and Reputation on the Internet' in Saul Levmore and Martha Nussbaum (eds) *The Offensive Internet, Speech Privacy and Reputation* (Harward University Press 2010) 16.

[81] Meg Leta Ambrose 'It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten' (2013) 16 Stanford Technology Law Review 369, 369.

[82] ibid 420.

[83] See for example Evan Selinger and Woodrow Hartzog, 'Google can't forget you, but it should make you hard to find' Wired <https://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/> accessed 18 October 2018.

[84] Evan Selinger and Woodrow Hartzog, 'Google's action on revenge porn opens the door on right to be forgotten in US' The Guardian < https://www.theguardian.com/technology/2015/jun/25/googles-revenge-porn-opens-right-forgotten-us> 25 June 2015, accessed 18 October 2019.

[85] Leta Ambrose (n 81) 370.

way become a value, which needs to be balanced against privacy.[86] This view is simplistic, however, and fails to take the dynamic role of privacy into consideration. So-called 'innovative practice', which unfolds from an interaction between 'freedom and constraint', is also not simple.[87] According to *Julie E. Cohen* innovation thrives when circumstances gives away to random or unexpected encounters with new ideas in a way that does not restrict the 'freedom to tinker'. She concludes that it is 'modulation, not privacy, that poses the greater threat to innovative practice'.[88]

2.2. Many ways to define privacy

2.2.1. Privacy in a broad sense

Privacy, in a broad sense, is established on the idea of an individual and his or her relationship with society.[89] The notion of 'private and public spheres of activity' is based on the assumption that there is a community in which such classification is possible.[90] Such classification is not always realistic in a digitalised society, however. In a connected society, the line between private and public is easily crossed, sometimes without even noticing. The Internet has changed our view of privacy and the concept keeps evolving as new technologies, such as the IoT and 'Big Data'[91] become part of our everyday lives. In

---

[86] Julie E. Cohen 'What Privacy is for' in 'Synopsium: Privacy and Technology' (2013) 126 Harvard Law Review 1879, Chapter IV.

[87] ibid.

[88] ibid.

[89] Wacks (n 6) 235-236.

[90] ibid.

[91] According to the *Gartner IT Glossary*, '[b]ig data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making'. *Gartner IT Glossary*, 'Big data' available at <http://www.gartner.com/it-glossary/big-data> accessed 22 February 2016; Interested readers

the context of new technology, many feel that privacy and the values it represents are outdated and at worst hindering innovation and knowledge.[92] People generally understand privacy in different ways and therefore it is difficult to define precisely. The concept of privacy is agent-relative, which makes it hard to provide one universal definition for it.[93]

In their classical article 'The Right to Privacy' from 1890, Judges *Louis D. Brandeis* and *Samuel D. Warren* argued that the right to privacy is a 'right to be let alone'.[94] *Brandeis'* and *Warren*'s argument is based on a right to protection from newspapers and gossip. Nonetheless, it has been argued that this theory is inconsistent with 'a society committed to free speech and robust public debate'.[95] The 'right to be let alone' as the essence of privacy has also been criticised by *Raymond Wacks*, who argues that it is 'a sweeping phrase which is as comprehensive as it is vague'. He continues by noting that if the right to privacy consisted of 'being let alone' it would mean that 'every physical assault would constitute an invasion of privacy'.[96]

In a theoretical discussion regarding the nature of privacy, two main points of view can be identified. The scholars supporting the so called 'reductionist school', consider that privacy consists of a 'cluster of freestanding interests', which cannot necessarily always be associated with each other.[97] According to this school, privacy discussions should be 'reduced to talk about its disparate elements to avoid suggesting that there is something

---

can read more about Big Data in: Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (New York 2013).

[92] Cohen (n 86) 1904.

[93] Patrick O'Callaghan, *Refining Privacy in Tort Law* (Springer-Verlag Berlin Heidelberg 2013) 25.

[94] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 5 Harvard Law Review, V.IV.

[95] Richards (n 5) 4.

[96] Wacks (n 6) 216.

[97] O'Callaghan (n 93) 8.

distinct about it'.[98] The right clusters can overlap and same rights can belong to multiple clusters at the same time.[99] The other interpretation is that privacy is a 'unitary, conceptually distinct right or interest'. Scholars supporting this view believe that privacy has 'a distinct moral value'.[100] Indeed, most scholars view privacy as 'a conceptually distinct interest or right'.[101] *Jeffrey H. Reiman* has, for example, noted that 'there is indeed something unique protected by the right to privacy. And we are likely to miss it if we suppose that what is protected is just a subspecies of the things generally safeguarded by property rights and personal rights'.[102] He continues by stating that if we miss it 'there may come a time when we think we are merely limiting some personal or property right in favour of some greater good, when in fact we are really sacrificing something of much greater value'.[103]

In addition to the legal debate about privacy's 'conceptual distinctness' there are also disagreements about the values of privacy.[104] Questions arise such as 'does privacy have any value peculiar to itself' and 'should we be talking about the value of privacy in the first place?' These issues relating to privacy's 'normative identity' is closely attached to the discussion between the reductionists and those opposing it.[105] This discussion,

[98] J.C. Inness, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press 1992) 29.

[99] ibid 21; O'Callaghan (n 93) 9.

[100] ibid.

[101] O'Callaghan (n 93) 10.

[102] Jeffrey H. Reiman 'Privacy, Intimacy and Personhood' (1976) 6(1) Philosophy & Public Affairs 26, 28.

[103] ibid.

[104] Inness (n 98) 18.

[105] ibid.

according to *J.C. Inness*, cannot be bypassed since 'privacy cannot lack *and* possess a distinctive value at the same time'.[106]

A privacy taxonomy

According to *Daniel Solove*, a contemporary privacy scholar and taxonomist, the term privacy is 'best used as a shorthand umbrella term for a related web of things'. He further claims that 'in fact, it can obfuscate more than clarify'.[107] *Gary Marx* presents a similar interpretation. In his view we should, rather than trying to define privacy, understand it as 'a family of concepts encompassing personal information'.[108] Following in *William Prosser's* footsteps, *Solove* proposes taxonomy of privacy to 'clear the fog of confusion' that privacy envelopes. Instead of concentrating on the term 'privacy', he focuses on 'activities that pose privacy problems', those being:[109]

1. Information collection,
2. Information processing,
3. Information dissemination, and
4. Invasion.

These four 'basic groups' are further divided into subcategories. In *Solove's* model, information collection begins with the data subject, whose life the privacy problems mostly affect. The problems that collection poses are 'surveillance' and 'interrogation'. The second group 'information processing' describes issues that arise during data processing after the collection. It consists of 'aggregation', 'identification', 'insecurity', 'secondary

[106] Inness (n 98) 21.

[107] Daniel J. Solove, '"I've got Nothing to Hide" and Other Misunderstandings of Privacy'(2007) 44 San Diego Law Review 745, 760.

[108] Gary T Marx and Glenn W Muschert, 'Personal Information, Boarders and the New Surveillance Studies' Annual Review of Law and Social Science Science 3 (2007) 375; Richards (n 5) 9.

[109] Daniel J. Solove, *Understanding Privacy* (Harward University Press 2009) 10-11 and 101.

use', and 'exclusion'. The third group, 'information dissemination' is divided into 'breach of confidentiality', 'disclosure', 'exposure', 'increased accessibility', 'blackmail', 'appropriation', and 'distortion'. This is the step in which the 'data holder' transfers the data to other stakeholders. The last group, 'invasion', refers to invasions of the individual's rights. It is split into two categories 'intrusion' and 'decisional interference'.[110] Indeed *Solove* makes a convincing point, and in a technology context it seems like a good approach to shift focus from norms to a challenge-based analysis.

In practice, however, personal data collection and -processing already interfere with the rights of the data subject, making *Solove*'s taxonomy more theoretical than practical. Even though focusing on challenges instead of norms sounds clever, in reality norms form the basis for determining where the line between legal and illegal data collection and processing runs. Therefore *Solove*'s challenge-based analysis works well in non-legal academic discussion, but in a legal dissertation applying the legal dogmatic method, norms still remain the most important base for analysis. This way of looking at privacy also fits well in the aim and methods of this study: Indeed, the aim is to look at privacy and data protection challenges through the lens of invasions, as defined by Solove. Nonetheless, the invasions consist of personal data collection and processing unifying Solove's 'activities that pose privacy problems' into one broader category.

2.2.2. Privacy as protection of personal information

Data protection laws are to some extent safeguarding privacy.[111] *Serge Gutwirth* and *Paul De Hert* have called data protection 'a catch-all term for a series of ideas with regard to the

[110] Solove *Understanding Privacy* (n 109) 103.

[111] Lee A. Bygrave 'The Place of Privacy in Data Protection Law' (2001) 24(1) University of New South Wales Law Journal 277, 277.

processing of personal data'.[112] Indeed many of the fundamental human rights conventions are quite abstract. The combination of international conventions, however, such as the 'European Convention on Human Rights' ('ECHR') and the 'Charter of Fundamental Rights of the European Union' ('Charter') together with more precising legislation, such as the DPD, the GDPR and national legislation, forms a relatively extensive principle-oriented, but simultaneously dense, framework of privacy and personal data norms.[113] Privacy and personal data legislation provides people with rights to manage their own personal data and to make decisions about the use of them.[114] According to *Solove*, these rights primarily consist of 'rights to notice, access, and consent regarding the collection, use, and disclosure of personal data'. *Solove* calls this so-called control of personal data 'privacy self-management'.[115] However he criticizes the approach since it is based on an assumption that people are 'fully informed and rational', which clearly is not (at least always) the case.[116] *Julie E. Cohen* has noted that 'in fact, the liberal self who is the subject of privacy theory and privacy policy making does not exist'.[117] She too, criticizes the classification of privacy as 'control' of information, saying that privacy cannot be reduced

[112] Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S., Y. Poullet, P. De Hert, J. Nouwt & C. De Terwangne (eds) *Reinventing data protection?* (Springer Science, Dordrecht 2009) 3-44, 3.

[113] Mikael Koillinen, 'Henkilötietojen suoja itsenäisenä perusoikeutena' (2012) 42(2) Oikeus 171, 172.

[114] Daniel J. Solove, 'Introduction: Privacy Self-management and the Consent Dilemma' (2013) 126 Harvard Law Review 1879, 1880.

[115] ibid.

[116] ibid 1883.

[117] Cohen (n 86) 1904.

to ‘a fixed condition or attribute (…) whose boundaries can be crisply delineated by the application of deductive logic’.[118] In her view, privacy is ‘fundamentally dynamic’.[119]

In accordance with liberal political theory, the ‘liberal self’ is autonomous and has ‘abstract liberty rights’ as well as capacity to make informed choices in ways that is not influenced by the cultural context.[120] According to *Cohen* ‘the idea of privacy as a defensive bulwark for the autonomous self is an artefact of a pre-existing cultural construction’. She states that everybody belongs to some culture and social context. Furthermore she claims that privacy is not a fixed condition, but a dynamic one.[121]

2.2.3. Is right to privacy just abstract and symbolic without a material side?

As has been noted, privacy has a variety of meanings. Reading different scholars’ arguments on privacy, one can conclude that privacy can mean almost anything in practice. When ‘privacy’ is discussed without proper definitions and without precision, the whole concept waters down. One can ask that if privacy means almost anything, then will it mean almost nothing in practice?[122] Some scholars feel that so called ‘abstract concepts’, such as free speech (and privacy) ‘do not have any “natural” content but are filled with whatever content and direction one can manage to put into them.’[123] People are generally aware of the content of words about values such as liberty. However, the words are vague enough to leave room for ‘reasonable disagreement’ about what they represent. Thus the words

[118] Cohen (n 86) 1906.

[119] ibid.

[120] ibid.

[121] ibid.

[122] Richards (n 5) 8.

[123] Stanley Fish, *There’s no such Thing as Free Speech and it’s a Good Thing, Too* (e-book version, Oxford University Press 1994) 90.

'project universality but allow for reasonable pluralism'.[124] Yet surely, even abstract concepts such as privacy aught to have some content. This content can be a 'shared experience', but it does not mean that the word has the same meaning for everybody. It seems that when more people use the word 'privacy', the amount of competing and conflicting meanings grows subsequently.[125]

Privacy can be seen as a phenomenon meaning the habits and practices the privacy concept brings, or it can be viewed as a *right*. A phenomenon is seldom clearly defined, while rights are usually clearly established. In order to secure legal certainty, clear articulation about privacy as a right is needed. One way to look at it is to see privacy as a value, which needs protection, which in turn happens with the help of legal instruments. The law then defines what rights and protections each of us is entitled to.[126] Privacy is a global concern. Almost every nation has direct or indirect legislation or rules that protect privacy, usually enshrined in the constitution.[127] There are also multinational privacy guidelines and frameworks regulating privacy. In addition, privacy is a human right and an 'assertion of personal freedom' but it is not an absolute right.[128] Indeed sometimes privacy needs to yield to other fundamental rights or it needs to be balanced against public interest and other values. In the digitalised society of today, information, which would in a

[124] O'Callaghan (n 93) 1.

[125] ibid 4.

[126] Mirelle Hildebrandt, 'Privacy and Identity' in E. Claes, A. Duff & S. Gutwirth (eds) *Privacy and the criminal law* (Antwerp/Oxford, Intersentia, 2006) 61-104, 63.

[127] Solove, *Understanding Privacy* (n 109) 2-3.

[128] Gregory J. Walters, *Human Rights in an Information Age: A philosophical Analysis* (University of Toronto Press 2001) 133; Absolute rights are rights which cannot be balanced against the needs of other individuals or against any general public interest e.g. freedom from torture in ECHR, art. 3. See Council of Europe, 'Some definitions' <www.coe.int/en/web/echr-toolkit/definitions> Accessed 10 May 2018.

traditional meaning be seen as private, is constantly shared with an incomprehensibly big audience. It is difficult or perhaps even impossible to define who controls the data, who has access to it, and how far the collection can go.[129] This is something that the GDPR aims to solve or at least improve, however.

Privacy is defined and regulated in multiple international and national pieces of legislation. In a way this legislation defines the right to privacy and to data protection.[130] However, if we annihilated all laws regarding rights to privacy and personal data protection, people would presumably still respect these rights (at least to a certain extent). This probably stems from the underlying moral value that privacy in fact has. Making such conclusion would probably place me in the category of those scholars who oppose the reductionists. As has been noted by *Solove*, 'privacy seems to encompass everything, and therefore it appears to be nothing in itself'.[131] In order to understand the intersection between technology and privacy, we need to analyse and conceptualise privacy in the new digitalized environment. It is important that legal scholars and other jurists keep in mind that in today's society, it is likely that everybody and everything is being monitored at all times with help of smart device technology. It is impossible to turn back time. Instead we need to accept and adapt.

[129] Ruben Rodrigues 'Privacy on Social Networks: Norms, Markets, and Natural Monopoly' in Saul Levmore and Martha Nussbaum (eds) *The Offensive Internet, Speech Privacy and Reputation* (Harward University Press 2010) 237.

[130] See section 7.3.2. of the summarising report.

[131] Solove, *Understanding Privacy* (n 109) 7.

2.3. The GDPR – reasons and objectives

Parts of the text in this section were published in an article written as part of the background research for this doctoral dissertation: 'The background and nature of data within EU data protection law with reference to new technology'.[132]

2.3.1. Aims of the GDPR

The reasons behind the European data protection reform initiative was set out by the Commission in a Communication in 2010.[133] In the Communication, the Commission recognizes that the DPD 'enshrines two of the oldest and equally important ambitions of the European integration process: the protection of fundamental rights and freedoms of individuals and in particular the fundamental right to data protection, on the one hand, and the achievement of the internal market – the free flow of personal data in this case – on the other'.[134] The Commission further acknowledges that the 'twofold objective is still valid and the principles enshrined in the Directive remain sound'. Nevertheless, the Commission also realises that globalisation together with vast technological development and elaborate collection of data has raised questions about whether the DPD can cope with the new challenges.[135] After a careful review of the DPD, the Commission identified some issues with the existing legislation, some of those being: a 'need to clarify and specify the application of data protection principles to new technologies', the 'lack of sufficient harmonisation between (EU) Member States' legislation on data protection', issues relating to 'allocation of associated (stakeholder) responsibility', and the need for better ensuring

[132] Jenna Mäkinen, 'The background and nature of data within EU data protection law with reference to new technology' in Päivi Korpisaari (ed) *Oikeus, tieto ja viesti: Viestintäoikeuden vuosikirja 2015* (Helsinki 2016) 103-119.

[133] COM (2010) (n1).

[134] ibid 2-4.

[135] ibid.

enforcement of data protection rules.[136] These are also the core issues discussed in the articles forming this dissertation. As a result, the Commission undertook to propose a new EU data protection legislation to better cope with modern data protection issues, which we now know as the GDPR.

Six years after the communication given in 2010, and with the answer book in hand, the Commission has given a statement 'on the final adoption of the new EU rules for personal data protection'. The Commission has stated that thanks to the GDPR, data subjects will have more control over their personal data. This will be manifested in better information about how the data subjects' data is being collected and processed, the right to know without delay about possible data hacks, and through the strengthening of 'the right to be forgotten'.[137] Furthermore, data portability will make it easy for citizens to transfer data from one service provider to another.[138] According to the Commission, businesses will benefit from the changes brought by the new regulation, by promoting legal certainty through one single applicable law across the EU. The Commission also declares the GDPR 'future-proof: technologically neutral and fit for innovation and big data analytics',[139] something that some of the articles in this doctoral dissertation discusses and questions.

[136] COM (2010) (n1) 2-4.

[137] GDPR, art 17.

[138] European Commission, 'Joint Statement on the final adoption of the new EU rules for personal data protection' Brussels, 14 April 2016 <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm> accessed 31 January 2018.

[139] ibid.

2.3.2. Defining personal data

Personal data protection stands for a state in which a person is more or less inaccessible to others, especially on an informational plane.[140] The DPD and the GDPR apply only to information, which falls within the definition of 'personal data'. Consequently, since the adoption of the DPD, privacy scholars and European data protection authorities have attempted to identify what is actually meant by 'personal data'.[141] The objective of data protection regulation is to protect individual citizens against unjustified collection, storage, use, and dissemination of their personal details.[142] Data protection can be seen as a growing body of rules and principles that need to be taken into account by legislators when drafting laws and by controllers and processors of personal data. This growth is constant, as new rules and principles are called for every time new challenges arise due to new technological developments, such as the rise of IoT technology and biometrics.[143] There are many visions of the possible interests underlying data protection and their order of importance, ranging from autonomy, informational self-determination, balance of powers, informational division of powers, through integrity and dignity, to democracy and pluralism.[144] It is therefore challenging to define the ultimate interests of data protection.

[140] Lee A. Bygrave, 'Digital Rights Management and Privacy - Legal Aspects in the European Union' in E. Becker et al. (eds) *Digital Rights Management* (Springer-Verlag Berlin Heidelberg 2003) 418–446, 420.

[141] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (WP136, 20 June 2007).

[142] Peter Hustinx, 'Data protection in the European Union' (2005) 2 Privacy & Informatie 62, 62.

[143] De Hert and Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' (n 112) 2.

[144] ibid.

Any information

Any kind of information can be personal data provided that it relates to a person. The term 'personal data' includes information about an individual's private and family life *stricto sensu*, but it also covers information regarding activities, habits, and lifestyle, such as working relations or the economic or social behaviour of the individual.[145] The wordings of the GDPR itself supports this interpretation. However, it must be recognised that this concept of private and family life is extremely broad.

In theory, personal data may encompass a great deal of data, which has, *prima facie,* little direct relationship to a particular person. Accordingly, information may be 'personal' even if it must be combined with other data in order to allow a person to be identified.[146] Data collected by smart devices are an example of this: the business idea of IoT stakeholders is often to offer new applications and services through the collection and the further combination of data on individuals, with the aim, for example, of measuring users' environment-specific data or specifically observing and analysing their habits. In other words, the IoT usually implies the processing of data that relate to 'identified or identifiable' natural persons, thereby qualifying as personal data in the sense of Article 4 of the GDPR (Article 2 of the DPD). The data generated by the IoT in combination with modern data analysis techniques and cross matching may lend itself to secondary uses unrelated to the original purpose assigned to the data processing.[147] Third parties requesting access to data collected by other parties may want to utilise it for totally different purposes from those stated when the subject of the data consented to data collection. In practice, this

[145] WP29, Opinion 4/2007 (n 141) 6.

[146] Bygrave 'Digital Rights Management and Privacy - Legal Aspects in the European Union' (n 140) 426.

[147] WP29, Opinion 8/2014 (n 7) 7.

means that what may seem 'insignificant' data, for example information from the accelerometer on a smart phone, can be used to derive other information with a totally different meaning, in this case, say, data on an individual's driving habits.[148]

Today, location data is also a popular 'commodity' between stakeholders. A mobile phone's location data, to give an example, can be used to analyse how people move in a retail centre. The fact that Article 4 of the GDPR mentions location data as a personal identifier implies that such data might always be considered personal. However as has been discussed in Article IV of this dissertation, not all location data qualifies as personal data. Location data can furthermore become sensitive personal data when the location of an individual is monitored over time. Moreover, sensors in the street or in shops can capture the media access control Address ('MAC address')[149] of the mobile phones of passers-by. In general, a MAC address does not itself identify a specific individual and thus is not necessarily always considered personal data, but it could be used to track repeated visits, which may lead to the identification of the individual, thereby transforming the information into highly personal data.[150]

EU legislative bodies have interpreted the term 'personal data' in wide terms. In the original communication regarding the DPD in the 1990s, the Commission already stated that 'as in Convention 108, a broad definition is adopted in order to cover all information

[148] WP29, Opinion 8/2014 (n 7) 7.

[149] 'A MAC address is the (unique) physical ID number that is assigned to every network card on every computer'. See Denny Cherry, *The Basics of Digital Privacy - Simple Tools to Protect Your Personal Information and Your Identity Online* (Elsevier Inc. Online Resource 2014) ch 3.

[150] British Information Commissioner's Office, 'Big Data and Data Protection' <https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf> accessed 22 February 2016, 9.

which may be linked to an individual'.[151] Moreover, information does not have to be true to be protected as personal data. For example, in their definitions of personal information, Australia and Singapore explicitly state that protection extends to both true and false data. However, the (literal) definition of personal information in most data protection legislations, including the DPD and the GDPR, does not address this matter.[152] Consequently, one may ask whether this omission in the DPD and the GDPR means that protection is only guaranteed for data that is true. Nevertheless, it can be inferred that the articles allowing individuals to access and correct any false data pertaining to themselves[153] means that false data also fall within the scope of the DPD and the GDPR.

Accordingly, the WP29 has stated that the DPD covers both true and false data, with this principle also extending to views and opinions. The WP29 finds that since data protection rules already allow for the possibility that information is incorrect, and provide the subject of the data with the right to access that information, and take appropriate measures to challenge it, this means that incorrect data also falls within the scope of the data protection legislation.[154]

---

[151] European Commission, 'Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security' (COM (90) 314 final (13.9.1990) <http://aei.pitt.edu/3768/1/3768.pdf> accessed 23 February 2016, 19.

[152] William B. Baker and Anthony Matyjaszewski, 'The changing meaning of "personal data"' featured story in *the Official News Letter of the International Association of Privacy Professionals* 11(3) (April 2011) <https://iapp.org/media/pdf/publications/advisor04_11_print.pdf> accessed 23 February 2016.

[153] The data quality principles in GDPR, art 5, for example, state that personal data must be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy")'. The predecending data quality principles can be found in DPD, art 6.

[154] WP29, Opinion 4/2007 (n 141) 6.

Identifiable person

The definition of personal data in both the DPD and the GDPR has three main aspects: 1) it is 'any information'; 2) it relates to a 'natural person'; and 3) that person must be 'identified or identifiable'.[155] In the context of technological development, the identifiability factor proves to be the most relevant. A natural person can be considered 'identified' when he or she is distinguished from all other members of a group. In other words, data will usually not be personal if they can only be linked to a group of persons as opposed to one single person.[156] Accordingly, a natural person is 'identifiable' when that person has not yet been identified but identification is nevertheless possible.

The possibility of identification therefore forms a threshold for determining whether information is personal data and within the scope of the GDPR (and the DPD). Thus, the mere possibility of identification can be enough for data to become personal information. Usually identification is achieved through particular pieces of information (identifiers), which are closely linked to a particular individual, like name, height, clothing or profession.[157] These identifiers are mentioned in Article 2 of the DPD in the definition of 'personal data'.[158] In the GDPR, the article relating to the definition of personal data has been modified as follows (changes in italics):

Article 2(a) of the DPD:

> 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified,

[155] See DPD, art 2 and GDPR, art 4.

[156] Bygrave 'Digital Rights Management and Privacy - Legal Aspects in the European Union' (n 140) 426.

[157] WP29, Opinion 4/2007 (n 141) 12.

[158] DPD, art 2.

> directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Article 4(1) of the GDPR:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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.*

As can be seen, new examples of identifiers have been added to the definition of personal data: name, location data, online identifiers, and genetic identity. In particular, the inclusion of online identifiers and genetic factors demonstrates that technological development has been taken into account by the regulators.

Even information about physical objects can qualify as personal data if it can be linked to an individual.[159] Identification of objects that belong to individuals can, in turn, lead to a collection of information about habits, behaviour, and interests.[160] When these

[159] Hon and others, 'The Problem of Personal Data in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 1' (2011) Paper No. 75 Queen Mary University of London, School of Law Legal Studies Research Paper 14.

[160] For further information, see European Commission: 'IoT Privacy, Data Protection, Information Security' <http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC4QFjAA&url=http%3A%2F%2Fec.europa.eu%2Finformation_society%2Fnewsroom%2Fcf%2Fdae%2Fdocument.cfm%3Fdoc_id%3D1753&ei=QDV2U62JE6uX0QW124H4Aw&usg=AFQjC

data are connected to data from other objects, new knowledge may be created that is previously unknown even to the person himself. Additionally, collecting data on objects may allow individuals to become more easily identifiable. Online identifiers provided by devices, applications such as cookie identifiers, or radio frequency identification tags can leave traces which, when combined with other information received by servers, may be used to create profiles of individuals, leading ultimately to their identification.[161]

There has been some debate over whether a so-called 'relative' or 'absolute' approach should be followed with respect to the scope of personal data. According to the absolute approach, account should be taken of the means used by '*any other person'*. In other words, any situation where the combination of data from one or multiple sources allows the linking of that data to a natural person is considered 'personal data'. This means that as soon as data qualifies as 'personal data' for one person, it also qualifies as 'personal data' for any other person. Nevertheless, some scholars reject the absolute interpretation of personal data, instead arguing that personal data is a relative concept,[162] whereby the same data can be anonymous for one person while being identifiable for another data holder. According to this approach, the emphasis should be on the likely uses of the data and the ability of the data holder to link the data to identified individuals.

NHoRL11Ce0INElpI0SALOzVlFHcwQ&bvm=bv.66699033,d.d2k&cad=rja> 3, accessed 9 February 2016.

[161] GDPR, rec 24.

[162] For examples, see DLA Piper, 'EU study on the Legal analysis of a Single Market for the Information Society New rules for a new age?' (November 2009) <https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjNivDtt5XLAhUBLhQKHf8FCKsQFggkMAE&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdae%2Fdocument.cfm%3Fdoc_id%3D842&usg=AFQjCNFA_-PY3mF0GltQEFhEaOKUCeZ9FQ> accessed 26 February 2016. See also references used in the study.

Under the DPD, this is indeed the stance taken, as the identifiability criterion is not met simply by the existence of an isolated and purely theoretical possibility of identification. Identification must, in other words, be possible through methods deemed reasonably likely to be used in the circumstances in question.[163] Here the central issue is whether it is possible to define the kind of data that are considered too 'burdensome' to use. In order to ascertain whether means are 'reasonably likely' to be used to identify an individual, account should be taken of all the objective factors, including the costs of and the amount of time required for identification. Additional factors include available technology at the time of processing and technological development.[164]

This identifiability 'test' is in fact not new and has been in use in data protection cases since day one. Already in its 1992 commentary on the amended proposal for the DPD, the Commission stated that a person might be identified indirectly by, for example, a car number plate.[165] Later, in 2010, the Finnish Data Protection Board analysed the question of whether a car number plate constituted personal data, allowing the identification of the owner of the car through the use of reasonable means. The board concluded that as it was possible to retrieve a car owner's information by sending a text message with the number plate information to several well-known service providers, and as it was also possible to collect the information online for only 3.5 Euros, it was cheap and

[163] DPD, rec 26.

[164] GDPR, rec 23.

[165] Commission, 'Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data' COM(92) 422 final - STN 287 (15 October 1992) 9.

easy to retrieve information about the car owner based on the number plate and hence car number plates shall be seen as personal data within the scope of personal data law.[166]

2.3.3. The legal instruments leading to the GDPR

European Convention on Human Rights

Article 8 of the ECHR guarantees respect for private and family life, home and correspondence, and lays down the conditions under which restrictions to this right are permitted. Throughout its jurisprudence, the ECtHR has examined many situations involving the issue of data protection,[167] and it has concluded that personal data protection is part of the right to privacy. The Commission and ECtHR have taken a broad, evaluative view of the ambit of Art. 8 of the ECHR. This is in accordance with their intention to apply the ECHR as a 'living instrument, which (...) must be interpreted in light of present-day conditions'.[168] According to *Lee A. Bygrave*, it is nevertheless wrong to characterise data protection law as being solely concerned with privacy. He supports this argument by stating that data protection instruments are expressly concerned with setting standards for the quality of personal information. He argues that even though adequate quality of information can serve to secure the privacy of individuals, it is broken down into a

[166] Decision 1/2010 of the Finnish Data Protection Board <http://www.finlex.fi/fi/viranomaiset/ftie/2010/20100001> accessed 25 February 2016; See also Olli Pitkänen, Päivi Tiilikka, Eija Warma, *Henkilötietojen suoja* (Alma Talent 2013) 45.

[167] See for example: ECtHR, *Malone v. The United Kingdom*, No. 8691/79, 2 August 1984; ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007; ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978; ECtHR, *Uzun v. Germany*, No. 35623/05, 2 September 2010; ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987; ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008.

[168] 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, 252.

multiplicity of interests, such as the validity, integrity, availability, relevance, and completeness of data, that have little direct connection to privacy values.[169] To conclude, it can be stated that if personal data protection were to be seen as solely a part of the right to privacy, this would narrow the scope of the information protected. This, in turn, would represent a threat to personal data protection, which aims to prevent the misuse of all data that can be linked to a natural person.[170] That being said, information that can be categorised as private, and hence covered by the right to privacy, is always personal data if it can be connected to an identified person.[171]

Convention 108

The emergence of information technology at the end of the 1960s created a growing need for more detailed rules to safeguard individuals' personal data'.[172] Several challenges, presented partly by new developments in information processing, required resolution in order to ensure that the ECHR and national laws sufficiently protected peoples' privacy and personal data.[173] EU regulatory bodies had noticed that the ECHR took a defensive

[169] Bygrave 'The Place of Privacy in Data Protection Law' (n 111) 281.

[170] De Hert and Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' (n 112) 25.

[171] Pitkänen and others (n 166) 23-24.

[172] Council of Europe, *Handbook on European data protection law* (Publications Office of the European Union, Luxemburg 2014) 15 <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> accessed 10 February 2016.

[173] One such problem was that the right to a private life did not necessarily include all personal data, thereby leaving a large proportion of data insufficiently safeguarded. Also the right of access to data on oneself was not covered by the concept of the right to privacy as expressed in Article 8; See Paul De Hert & Serge Gutwirth, 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the

approach to privacy and found that more positive action was necessary. At the level of European policy-making, it was commonly agreed that a more dynamic approach was needed for problems related to personal data.[174] In 1981, a Convention for the protection of individuals with regard to the automatic processing of personal data[175] ('Convention 108') was opened for signature. Convention 108 provides guarantees on the collection and processing of personal data. It also outlaws the processing of 'sensitive'[176] data. The convention clarifies the right of individuals to know what information pertaining to them is stored, and it regulates the free flow of personal data between states.[177]

The DPD

Since the end of the 1990s, Convention 108 has been amended and modernized with the aim of reinforcing the protection of privacy in the digital arena, and strengthening the Convention's follow-up mechanism. The DPD is designed to give substance to and expand the principles of the right to privacy already contained in Convention 108.[178] The DPD used Convention 108 as a starting point, but it clarified it in many respects and also added new elements. For example, the DPD defined the tasks of independent supervisory authorities and the nature of their cooperation at the European level.[179] In practical terms, the DPD is the most influential regulatory instrument on data protection for the EU as a whole. It goes the furthest in terms of providing prescriptive guidance on data protection

virtual residence' in Institute For Prospective Technological Studies - Joint Research Centre, o.c., 111-162 <ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf> 118, accessed 10 February 2016.

[174] ibid.

[175] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108 Strasbourg, (28 January 1981).

[176] Such as race, political views, health, religion, sexual orientation or criminal records.

[177] Council of Europe, *Handbook on European data protection law* (n 172) 16.

[178] ibid 17.

[179] Hustinx (n 142) 63.

across a wide range of sectors, including new technology.[180] As has been identified by *Viviane Reding*, the former Vice-President of the Commission, the DPD 'set a milestone in the history of the protection of personal data in the European Union'. She founds this argument by concluding that it 'enshrines two of the oldest and equally important ambitions of the European integration process: the protection of fundamental rights and freedoms of individuals (in particular, the fundamental right to data protection), and the achievement of the internal market—the free flow of personal data in this case'.[181]

The 1966 International Covenant on Civil and Political Rights (ICCPR) (art. 17) is one of the other main international instruments. Together with the other aforementioned European regulations, it provides much of the formal normative basis for data protection instruments such as the DPD. However, the case law developed pursuant to the Covenant as well as the Convention 108 has, to date, added little to the principles found in the DPD and in some respects falls short of them.[182]

The Charter of Fundamental Rights of the European Union

When the Lisbon treaty was signed, the right to respect for private and family life, home and communications also became a fundamental right according to the Charter.[183] Article 7 of the Charter states that '[e]veryone has the right to respect for his or her private

[180] Bygrave 'Digital Rights Management and Privacy - Legal Aspects in the European Union' (n 140) 424.

[181] Viviane Reding, 'The European data protection framework for the twenty-first century' (2012) 2(3) International Data Privacy Law 119, 120.

[182] Bygrave 'Digital Rights Management and Privacy - Legal Aspects in the European Union' (n 140) 424.

[183] Charter of Fundamental Rights of the European Union [2007] OJ C-303/01 ('Charter').

and family life, home and communications'.[184] In addition to the Article on privacy, the Charter contains a separate Article on protection of personal data:

> Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

There has been much discussion about whether bringing a separate Article to protect personal data brings surplus value in addition to Article 7. However this falls outside the scope of this study. Primarily, however, data protection legislation also protects and covers information that does not necessarily fall within the scope of the right to privacy, hence giving it significance.[185]

Soft law – OECD Guidelines

There is also non-binding soft law guiding personal data protection. The first international guideline promoting the right to privacy was created by the Organisation for Economic Co-operation and Development ('OECD') in 1980.[186] The 'OECD Guidelines on

[184] Charter, art 7.

[185] Koillinen (n 113) 181; See also Case C-28/08 P *European Commission v The Bavarian Lager Co. Ltd.* [2010] ECR I-06055, sec 118.

[186] OECD, 'Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data' C(80)58 FINAL (23 September 1980) <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 6 February 2018.

the Protection of Privacy and Transborder Flows of Personal Data' has acted as a model for many later legislations relating to privacy such as the DPD.[187] The role of the OECD guidelines can clearly be seen for example in the data quality principles in Art. 6 of the DPD and Art. 5 of the GDPR. The 'basic principles' laid down by the OECD are the 'Collection Limitation Principle', 'Data Quality Principle', 'Purpose Specification Principle', 'Use Limitation Principle', 'Security Safeguards Principle', 'Openness Principle'Individual Participation Principle', and the 'Accountability Principle'.[188] The OECD guidelines have since been revised and updated in 2013 (OECD Privacy Guidelines (2013)'). In the spirit of time, two subjects are highlighted in the updated Guidelines: 'A focus on the practical implementation of privacy protection through an approach grounded in risk management' and '[t]he need to address the global dimension of privacy through improved interoperability'.[189] The exact same motives are the reasons behind the GDPR, ie. the need for a more risk-based approach and the need for harmonisation.

2.3.4. The GDPR drafting process

The DPD was drafted in an era before big data and IoT. As a result of the changed technological climate, the EU legislators decided it was time for a comprehensive reform of the EU data protection rules. In addition to the DPD being out-of-date, the national laws in EU member states, that are based on the DPD, were varied and scattered making the legal

[187] OECD, '30 Years After: the Impact of the OECD Privacy Guidelines' (March 2010) <http://www.oecd.org/sti/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm> accessed 6 February 2018.

[188] OECD, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (n 186) Part two.

[189] OECD, 'Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' (2013) C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79 <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> accessed 26 April 2018.

certainty questionable. The first draft of the GDPR ('GDPR 2012') was proposed by the Commission in January 2012.[190] Following the Commission's proposal, the European Parliament ('Parliament') released its amended version in 2013,[191] and it adopted its first reading on the proposed GDPR in March 2014.[192]

After this, the European Council ('Council') agreed on a 'General Approach' in 2015[193] enabling the 'Trilogues', which is the final stage of EU legislation, to begin.[194] The altogether ten trilogue meetings between the three EU bodies[195] were held in 2015 and resulted in the final conclusion of the process in December 2015. The final version of the GDPR was published in the EU Official Journal ('OJ') 4 May 2016.[196] The GDPR entered into force on the twentieth day following the OJ publication i.e. 25 May 2016 and after a

[190] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final ('GDPR 2012' or '2012 proposal').

[191] The task was assigned to its 'Committee on Civil Liberties, Justice and Home Affairs' ('LIBE'). See LIBE Report A7-0402/2013 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN> accessed 26 April 2018.

[192] European Parliament, 'Legislative train schedule' <http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-general-data-protection-regulation> accessed 30 January 2018.

[193] Council of the European Union, General approach to the GDPR 9565/15 (11 June 2015) <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf> accessed 26 April 2018.

[194] GDPR Portal < https://www.eugdpr.org/the-process.html> accessed 29 January 2018.

[195] European Parliament, Council of the European Union and the European Commission.

[196] GDPR.

two year 'grace period', the regulation has been applicable throughout the EU from 25 May 2018.[197]

The proposal for the GDPR is based on Article 16(1) of the Treaty on the Functioning of the European Union ('TFEU')[198] that states that '[e]veryone has the right to the protection of personal data concerning them'. The Article goes on with providing that the 'European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.'[199] In other words, the TFEU does not specify the type of legal instrument to be used; leaving it up to the EU legislative bodies to chose between a directive and a regulation.[200] The choice of using a regulation, which has direct effect in member states,[201] instead of a directive can be seen as a drastic measure by some. The reason behind the choice of instrument is the aim of harmonising the data protection legislation in the member states. Some view this choice of instrument as unprecedented, since regulations are usually used in more niche fields.[202] As identified by *De Hert* and *Papakonstantinou* this 'signals an important qualitative change:

[197] GDPR, art 99.

[198] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326 ('TFEU').

[199] TFEU, art 16(2).

[200] Reding (n 181) 120.

[201] TFEU, art 288.

[202] See for example Paul De Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 Computer Law & Security Review 179, 182.

data protection is no longer perceived as a local phenomenon (…) Conversely, data protection is considered from now on an EU concern, to be regulated directly at EU level (…)'.[203] The advantages of a directly applicable regulation are greater legal certainty, improved protection of individuals, and freer flow of personal data within the EU.[204]

2.3.5. The transition period and the EU case law

The reform process has lasted six years. During this time the world around us has changed and technology has developed even further. In the run up to the GDPR, the CJEU has processed a few major cases dealing with data protection issues and assumably indirectly influencing the GDPR drafting process: the '*Google Spain'* case,[205] the '*Digital rights Ireland'* case,[206] the '*Weltimmo case'*[207] and the '*Safe Harbour Agreement case'* or '*Schrems case'*.[208] In the *Google Spain* case, the CJEU dealt with questions relating to a

[203] ibid.

[204] Reding (n 181) 121.

[205] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.

[206] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238 (*Digital rights Ireland* case). In the *Digital rights Ireland* case, the Court mainly analysed the so-called 'Data retention directive,' in the end deeming the Directive invalid, and will therefore not be examined in further detail in this study focusing on the DPD and the GDPR; Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105 13 April 2006) ('Data retention directive').

[207] Case C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] OJ C 381.

[208] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

search engine's role and responsibilities under EU data protection legislation. The key questions were whether the activities Google carries out in compiling its search results constitute activities covered by the DPD. The court analysed, in particular, whether Google was a data controller undertaking data processing under the DPD. Furthermore, the case handled questions relating to the territorial application of the DPD. An important issue analysed by the court was also whether the data subject can request a search engine to remove personal data on the grounds of the DPD.[209] The overall outcome was that Google's activities are indeed covered by the DPD. Furthermore the Court stated that data that is inaccurate, inadequate, irrelevant or 'excessive in relation to the purposes of the processing', out of date or 'kept for longer than is necessary' ought to be removed by the data controller.[210] The Court made a reference to Articles 7 and 8 of the Charter, stating that 'in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name'.[211] The *Google Spain* case has been broadly discussed by scholars and many have criticized the CJEU for not being thorough enough, especially relating to the relationship between privacy and freedom of journalism and the freedom of expression, once they had the

[209] Case C-131/12 *Google Spain SL and Google Inc v Agencia Espagnola de Proteccion de Datos (EPD) and Mario Costeja Gonzales* [2014] ECR I-317, para 20.

[210] Case C-131/12 *Google Spain SL and Google Inc v Agencia Espagnola de Proteccion de Datos (EPD) and Mario Costeja Gonzales* [2014] ECR I-317, para 92.

[211] Case C-131/12 (n 210) ruling.

chance to clarify many unclear matters.[212] However it can be concluded that the Court took the praxis in the direction of the aim of the GDPR of strengthening and establishing a so called 'right to be forgotten'.

The *Weltimmo* case dealt with the issue of a 'one-stop-shop regulation within the EU'. The key issues of the case related to the applicability of national laws of a member state (Article 28 of the DPD) and the authority of the data protection authorities of member states (Article 4 of the DPD). The outcome of the ruling was a conclusion that companies must comply with local data protection laws if they processes data 'through stable arrangements' in that member country. On the question of regarding the authority of the data protection authority ('DPA'), the Court stated that a local DPA cannot impose penalties on the basis of an other member country's law, but should instead request the relevant other member state's DPA to act. The GDPR makes an attempt to correct the

[212] See for example: Christopher Wolf, 'Impact of the CJEU's Right to Be Forgotten: Decision on Search Engines and Other Service Providers in Europe' (2014) 21 Maastricht Journal of European and Comparative Law 547, 552; Paul De Hert and Vagelis Papakonstantinou, 'Comment Google Spain Addressing Critiques and Misunderstandings One Year Later' (2015) 22(4) Maastricht Journal of European and Comparative Law 624, 631; The Editorial Board of The Washington Post, 'UnGoogled: The disastrous results of the "right to be forgotten"' (July 2014) <https://www.washingtonpost.com/opinions/ungoogled-the-disastrous-results-of-the-right-to-be-forgotten-ruling/2014/07/12/91663268-07a8-11e4-bbf1-cc51275e7f8f_story.html?noredirect=on&utm_term=.bab701f82ca6> accessed 15 April 2018; Daniel Solove, 'What Google Must Forget: The EU Ruling on the Right to Be Forgotten', Linkedin (13 May 2014) <https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten> accessed 15 April 2018; A. Mantelero, 'The EU Proposal for a General Data Protection Regulation and the Roots of the "Right to be Forgotten"' (2013) 29 Computer Law & Security Review; Jeffrey Rosen, 'The Right to Be Forgotten' The Atlantic (July/August 2012) <https://www.theatlantic.com/magazine/archive/2012/07/the-right-to-be-forgotten/309044/> accessed 15 April 2018.

unclear situation regarding the division of local DPAs.[213] However, a further analysis on the one-stop-shop falls outside the scope of this dissertation.

The *Safe Harbour Agreement case* ruling declared the 'Safe Harbour scheme'[214] for EU-USA data transfers invalid. An Austrian student *Max Schrems*, who wanted to prohibit Facebook Ireland from transferring his personal data to the USA, initiated the case. He claimed that especially after the Snowden revelations, the USA did not 'ensure adequate protection of personal data'.[215] The CJEU declared the Safe Harbour scheme invalid.

In addition, Advocate Generals ('AG's) have made direct references to the GDPR, in the CJEU's soft-case law. In fact, the GDPR had its first direct referral in CJEU in the '*Manni case*'[216] in 2016. The case concerned whether 'the right to be forgotten[217]' also applies to personal data of an entrepreneur recorded in public companies registers.[218] Forming the debut of the GDPR in CJEU case law, AG *Bot* stated in the conclusions of the case:

> [f]inally, I observe that the foregoing analysis is in step with Article 17(3)(b) and (d) of 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

[213] GDPR, rec 117-138 and arts 4(21-22), 51-62.

[214] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) OJ L 215 , 25/08/2000 p. 7-47 ('Decision 2000/520').

[215] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] (n 208) para 28.

[216] Case C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* [2017] ECLI:EU:C:2017:197 ('Manni case').

[217] DPD, art 12; GDPR, art 17.

[218] Manni case (n 216) para 24.

> and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation). Under that provision, the right to erasure of personal data or 'right to be forgotten' does not apply where the processing is necessary 'for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller', or 'for archiving purposes in the public interest.[219]

Following the Manni case, further AGs have made references to the GDPR. The GDPR was mentioned in Opinion of AG *Bobek* delivered on 26 January 2017 in Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme',*[220] Opinion of AG *Kokott* delivered on 30 March 2017 about the case *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálnycúrad finančnej správy,*[221] Opinion of AG *Kokott* delivered on 20 July 2017 in Case C-434/16 *Peter Nowak v Data Protection Commissioner,*[222] Opinion of AG *Bot* delivered on 24 October 2017 in Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the*

[219] Case C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* [2017] para 101.

[220] Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* [2016] OJ C 111, 29.3.2016, p. 10–1, Opinion of AG Bobek, para 15 and footnotes.

[221] Case C-73/16 *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálnycúrad finančnej správy* [2017] ECLI:EU:C:2017:253, Opinion of AG Kokott, paras 2, 41 and 43.

[222] Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:582, Opinion of AG Kokott, paras 3 and 48; See Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994, paras 11-13 and 57-61.

presence of Facebook Ireland Ltd,[223] and Opinion of AG *Bobek* delivered on 23 January 2018 Case C-530/16 *European Commission v Republic of Poland*.[224]

From the recent CJEU case law and the increasing importance placed on the GDPR by AGs, a conclusion can be drawn that EU case law has been quite active during the 'grace period' leading to the applicability of the GDPR. Indeed the CJEU has made big efforts to protect EU citizens' personal data in modern and new circumstances, even though this has meant that the Court has had to stretch the provisions of the DPD to their breaking point. The Court and the AGs have seen to it that concepts, such as 'the right to be forgotten', 'extraterritoriality'. and 'international data transfers' have been discussed in light of the GDPR, hence putting the new regulation in a relatively strong position already before it became applicable.[225]

3. Discussion about the findings of the study

3.1. Summary of publications

3.1.1. Data quality, sensitive data, and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things

The first article that was written as part of this doctoral dissertation provided background information and definitions of the relationship between personal data protection and the IoT

[223] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the presence of Facebook Ireland Ltd* ECLI:EU:C:2017:796 [2017], Opinion of AG Bot, paras 103, 135 and footnotes.

[224] Case C-530/16 *European Commission v Republic of Poland* OJ C 14, 16.1.2017, p. 24–25, Opinion of AG Bobek, para 49, footnote 16.

[225] De Hert and Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (n 202) 180-181.

technology. Furthermore the legal challenges and requirements that IoT imposes to personal data protection legislation were introduced and discussed. Following the WP29,[226] focus was placed on already existing technologies: wearable computing; domotics; and quantified-self devices. Several themes and provisions were introduced that were to recur in subsequent articles of the dissertation later on: issues relating to joint controllership; sensitive data; and data quality principles. At the time when the article was written, the final version of the GDPR was not yet completed and therefore the applicable law discussed in the article is the DPD. Under the DPD, a controller is defined as someone who 'alone or jointly with others determines the purposes and means of the processing of personal data', whilst a processor is a 'legally separate entity that processes personal data on behalf of the controller'.[227] The article discusses the grey areas of the concept of joint personal data controllership and criticizes prudently the broad interpretation possibilities that are left for the interpreter of the law. The article also mentions some suggestions that the 'binary distinction between controllers and processors should be abolished and replaced by the more nuanced principle of end-to-end accountability'.[228]

Accountability also correlates with the personal data protection principles defined in Article 6 of the DPD: the fairness principle; purpose limitation principle; data minimisation principle; and the necessity principle. The article describes the conflict of interests between the EU legislation (together with the data subjects) and the IoT stakeholders. Stakeholders often feel that strict data protection principles stifle innovation and that the obligations imposed by the principles are not easy to integrate in 'real-life' situations, whilst the WP29

[226] WP29, Opinion 8/2014 (n 7).

[227] DPD, art 2.

[228] WK Hon and others, 'Who is Responsible for Personal Data in Cloud Computing? The Cloud of Unknowing, Part 2' (2011) Queen Mary University of London, School of Law Legal Studies Research Paper No. 77/2011, 24.

has stated that the principles play an 'essential role in the protection of personal data'.[229] As one possible solution to this dilemma, a new 'accountability principle' was introduced.

The third grey area introduced in the article is processing of sensitive personal data. Sensitive personal data means special categories of personal data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; data concerning health, or data concerning a natural person's sex life or sexual orientation'.[230] Sensitive data merits higher protection than 'ordinary personal data'. The principle rule of the DPD is that processing of sensitive personal data is prohibited.[231] However IoT applications and devices often rely on the possibility to process such data. Especially quantified-self devices' basic idea is to process and mine data relating to health and well-being, which almost always constitute sensitive data. Adding to the confusion, personal data may change their quality over time: information that is not sensitive at the time of collection may become sensitive over time. A conclusion is drawn that all personal data may potentially be sensitive depending on the context and therefore the distinction between personal data and sensitive personal data may not be tenable in the context of the

[229] WP29, Opinion 8/2014 (n 7) 16-17.

[230] GDPR, art 9; Also see DPD, art 8. 'Genetic data' and 'biometric data for the purpose of uniquely identifying a natural person' are new categories that have been added to the classification. This reflects the technological development and new IoT technologies being used in data processing.

[231] DPD, art 8; Sensitive personal data may be processed if the data subject has given his 'explicit consent to the processing of that data' or sometimes if 'the processing relates to data that has been made public by the data subject himself'.

IoT.[232] In light of the final version of the GDPR, it can be noted that the GDPR leaves 'a margin of manoeuvre for member states' to stipulate specific rules for processing of sensitive data. This means that the GDPR allows member states to legislate and determine 'more precisely the conditions under which the processing of (sensitive) personal data is lawful'.[233]

3.1.2. The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges

Article II, 'The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges' describes and analyses the personal data protection mechanisms offered by EU legislation to children, with a specific reference to the context of smart devices within the IoT. Further, the article aims 'to expose the need for a clearer interpretation of children's data protection rights in an IoT context'.[234] The article continues the discussion from Article I relating to data quality principles, and security and legitimacy issues. The example IoT technologies have been narrowed down, similar to Article I, to a discussion about smart toys, apps, and domotics. The article also describes and illustrates the legal data protection environment for children.

The fundamental principle that safeguards children's right to data protection and privacy is that of the 'best interest of the child'.[235] The principle has been enshrined in the UN Convention On The Rights Of The Child (1989) ('Convention') and later many other

[232] Jenna Mäkinen, 'Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things' (2015) Information & Communications Technology Law 24/3, 276.

[233] GDPR, rec 10.

[234] Lindqvist, 'The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges' (n 14) 85.

[235] ibid 88.

international charters have reaffirmed the principle.[236] The DPD does not clarify at what age children can start dealing with their own personal data, creating difficulties for parents and IoT stakeholders, who want to (and have to) apply data protection rules. The GDPR, in turn, introduces a special provision for the protection of children's personal data.[237] According to Article 8 of the GDPR '[t]he processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.'

Article II raises questions 'as to whether EU politicians and policy makers have actually considered the specific rights and needs for children, both in terms of data protection, and the right to access and use digital media' when drafting the new Article 8 of the GDPR.[238] Even after the introduction of the final version of the GDPR, uncertainty prevails relating to the definition of 'who is a child' in the eyes of the EU data protection legislation? Since the member states can choose among different age limits in their national laws, also the harmonisation effect of the Regulation weakens. Until the given age limit, parents are, according to the GDPR, entitled to consent to data collection and processing on their children's behalf. By implication, this also means that they can administer the children's communications. In Article II, a question is therefore raised as to whether it is morally correct for parents to 'spy on their children' up to a certain age limit. After all, the

[236] See for example The Convention on Contact Concerning Children; and the Charter, art. 24.

[237] GDPR, art 8.

[238] Lindqvist, 'The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges' (n 14) 89.

UN Convention On The Rights Of The Child (1989) ('the Convention') provides that '[n]o child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or corre- spondence, nor to unlawful attacks on his or her honour and reputation.'[239] A conclusion can be drawn that a child is entitled to privacy also within his or her own family. It is furthermore undefined what exactly is a verifiable parental consent in practice. Currently stakeholders use multiple verification methods. Some just need the parents to tick a box or reply to an email, but some may require quite strict measures, such as scanning a passport or using facial recognition. The article discusses the issue of the divided practices and suggests that sometimes the collection of consent can be 'excessive in relation to the purposes for which it is collected'.[240]

A further challenge to children's data protection, identified in Article II, is the possibility that limiting children of a certain age from interacting online or receiving information may, in some cases, limit their freedom of expression. The arguably simplistic phrasing of Article 8 of the GDPR, prevents those children who are under the given age limit from using certain forms of communication without their parents prior consent. There is also a risk for double dealing, because in practice it is quite clear that most stakeholders are aware of the fact that their services and platforms are used by much younger children than what is actually allowed in the stakeholders' user terms. What the Article II also criticises, is the hasty writing process of the Article 8 towards the end of the GDPR reform process. In the GDPR 2012, the Commission originally proposed a fixed age limit of 13 years.[241] The Commission based this age limit on the fact that this would not 'impose

[239] Convention, art. 16.

[240] Lindqvist, 'The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges' (n 14) 97.

[241] GDPR 2012, art. 8.

undue and unrealistic burden upon providers of online services and controllers'[242] because the age limit is the same as the one in use in the USA.[243]

As in Article I, the data quality principles are brought up as playing a key role in children's personal data processing. Principles such as fairness, lawfulness, and transparency are difficult to implement and oversee when dealing with items that are meant to be as unobtrusive as possible, such as smart toys. The principles of data minimisation and accuracy stated in GDPR, Article 5, require that data must be kept up to date. This forms a significant challenge when handling children's data, because children are always developing and changing both mentally and physically. Article II also highlights some security issues relating to IoT devices aimed at children. Overall, the conclusion is that stakeholders have been lax with security and designing privacy into smart toys.

In the 'The way forward' chapter of Article II, the Article seeks the establishment of specific verifiable parental consent methods in order to both protect children and to simplify the situation for stakeholders. The article also puts faith in the strengthening of the accountability principle, through the GDPR. When stakeholders need to be able to verify and demonstrate data protection compliance, stakeholders will have more motivation to do all in their power to comply with the GDPR.

[242] European Commission, 'Commission Staff Working Paper Impact Assessment' SEC (2012) 72 final (Brussels, 25 January 2012) <http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf> 68 accessed 8 February 2018.

[243] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 ('COPPA').

3.1.3. New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability, and liability in a world of the Internet of Things?

The GDPR expands the obligations of personal data processors and brings challenges to the contractual relationships between data processors and data controllers. This theme is discussed in Article III of the dissertation 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' that was published in the International Journal of Law and Information Technology in January 2018. The main focus of the article lies on the changes to data controllers' and –processors' rights and obligations, brought by the GDPR. Again the key technology that acts as the arena for the contractual relationships discussed is the IoT. The article starts off by setting the scene for contractual relationships in an IoT context. The article presents examples of contracts related to domotics in order to illustrate the legal challenges in IoT contracting. In general, it can be concluded that on the IoT multiple stakeholders usually share the responsibility for personal data management. The structure usually consists of a data controller, who outsources data processing to many processors, who are specialized in processing big masses of data. The initial data processors can then in turn further delegate some of its processing work to 'sub-processors'. In this complex chain of data processing, the responsibilities of the different actors are at times difficult to pinpoint and to oversee. This setup also obscures who carries the accountability responsibilities towards data subjects and the authorities.

The key Article of the GDPR, which is put under the microscope, is Article 28 that includes many of the new data processor obligations. Article III identifies that Article 28 is a 'long and detailed article with many cross-references to other parts of the Regulation,

creating possible confusion about the correct application of the Article'.[244] The article outlines that Article 28(3) of the GDPR limits the contracting parties' contractual freedom. In the interpretation adopted in the article, contractual freedom means a freedom to determine 'whether or not to enter into a contract'; with whom one enters a contract; and 'the terms of the contract'.[245]According to Article 28(3) of the GDPR, personal data processing must be governed by a contract, and the Article further provides a list of required elements that the processing contract must include. In this way, the Article affects the freedom of contract by setting strict rules about both the entering into contract and the content of said contracts. The positive side of things is that limiting contractual freedom in this case, can simplify contracting mechanisms and reduce later disagreements between the contracting parties.[246] In the IoT context, this can in fact have a big practical impact when dealing with multi-layered contracts dealing with substance relating to goods, services, and digital content, that exist both online and offline.[247]

Another highlighted challenge in the IoT contracting scenario is the misconception that a data controller is always a stronger party than the data processor. Article 28(3)(a) of the GDPR states that a processor shall process personal data 'only on documented instructions from the controller'. However, in the IoT supply chain, the practical reality is often turned on its head. It is common that a processor specialises in processing big masses

---

[244] Jenna Lindqvist 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' International Journal of Law and Information Technology 26 (2018) 45, 52.

[245] Lee A. Bygrave, *Internet Governance by Contract* (Oxford University Press 2015) 114.

[246] Juha Pöyhönen, *Sopimusoikeuden järjestelmä ja sopimusten sovittelu* (Suomalaisen Lakimiesyhdistyksen julkaisuja 1988) 94.

[247] Jenna Lindqvist 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' (n 244) 53.

of data and then sells this service to multiple data controllers. In this context, the controller becomes the processor's client and usually it is the processor who then stipulates the contractual terms and not the other way around. The GDPR's 'instructions requirement' becomes unpractical in these situations, since it is focusing on controllers, while in reality the processor gives the instructions. Article II claims that not enough scrutiny has been given to these new kinds of relationships, between controllers and processors, in the data protection law reform process.

Furthermore some decisions by the legislators, to add obligations twice over in the GDPR, are questioned in the article. The issue is that some of the requirements of a processing agreement set out in Article 28, already derive straight from the wording of the law, making it unclear what the surplus value of adding it twice over in the contract is. To provide an example, both the processor and the controller are required, directly by Article 32 of the GDPR, to implement appropriate security measures to ensure the security of the processing. Simultaneously, Article 28(3)(c) requires that the processing contract must stipulate that 'the processor shall take all measures pursuant to Article 32'. Another example of the same thing twice as problematic, can be seen in Article 28(3)(d), which summed up states that the processing contract must stipulate that the processor respects the conditions set out in paragraphs 2 and 4 of Article 28. However the said paragraphs bind the processor already as is, making the double requirements feel like exaggeration.

In the same line as the previous articles, this article also highlights the importance of accountability. Accountability includes aspects such as demonstrating compliance and holding relevant records. The accountability principle has been included in the processing contract requirements by stating that '[t]he processor shall make available to the controller

all information necessary to demonstrate compliance…'.[248] The fulfilment of this obligation can be measured by for example processor audits. The article emphasizes that in practice this may be difficult to carry out, since professional data processors often store data from multiple clients in the same location, and allowing one controller access would result in security risks. A further issue regarding accountability in an IoT contracting context is that as it is enshrined in the GDPR that accountability is only required from the data controller. This implies that if a liability issue arises, processors are not liable deriving from the law. However, if the accountability obligations have been properly included in the processing instructions, the contract can form accountability liability also for the processor. Liability for accountability shall not be mixed up with liability for damage: Under the DPD, solely the data controller carries liability for potential damage,[249] but the GDPR brings liability obligations also to the data processor in certain circumstances.[250] The underlying aim of the new arrangement is to secure effective compensation for possible damages for the data subjects.

Overall, the article shows that the GDPR brings many comprehensive new requirements to processing contracts. The conclusion is however that the GDPR is hard to reconcile with IoT goods and services in places. The underlying issue, in my opinion, is the confusing new concept of goods. On the IoT so-called 'products' consist of hardware, software and services and are constantly developing and changing form. What makes it even more complicated is that the products exist both online and offline. It is therefore natural that it is challenging for data processors and –controllers to draft appropriate contracts that would satisfy the requirements set by the GDPR.

[248] GDPR, art 28(3)(h).

[249] DPD, art 23.

[250] GDPR, art 82.

3.1.4. Automated vehicles and personal location data in a smart world – an EU perspective

Article IV focuses on the collection and processing of 'personal location data' with smart machines. The subject is approached through the example of smart vehicles, as part of the IoT. As in the preceding articles forming the dissertation, Article IV also focuses on collection of personal (location) data executed by private actors. The article begins by identifying the core privacy and data protection implications that automated vehicles pose to data subjects. The article continues to define key terminology and concepts, such as 'personal location data' and 'automated vehicle'. In line with the other articles forming this dissertation, a closer examination to some of the Articles of the GDPR is conducted, using a certain technology, in this case, automated vehicles, as a reference point. Lastly, grey areas are mapped out, and the future of the intersection between automated vehicle technology and data protection legislation, is discussed.

Personal location data means, in the context of the article, location data that relates to an identifiable data subject.[251] The definition is derived from combining the definitions of 'personal data' and 'location data'. Smart machines such as automated vehicles are usually connected to a natural person and as a consequence, the machine's geographical location gives away the data subject's location by implication. It is however noted that not all location data constitute personal data. Furthermore, an automated vehicle can reveal personal data at one point of its lifecycle, but not be connected to a data subject in another.

The definition of 'automated vehicles' that has been used for the purpose of this article, has been borrowed from the American 'Autonomous Vehicle Team' at the

[251] Jenna Lindqvist, 'Automated vehicles and personal location data in a smart world – an EU perspective' (under peer review 2018).

University of Washington: 'An "autonomous vehicle" is a motor vehicle equipped with autonomous technology that can drive the vehicle without the active physical control or monitoring of a human for any duration of time'.[252] The article presents a few practical scenarios for how autonomous vehicles can be built and what they may be used for.

The underlying issue, with collection and use of personal location data, is that when combined with other pieces of information, the location of a person can actually reveal quite sensitive information about a data subject, and thus raise serious privacy concerns. When a person's location is derived from his or her movements, conclusions can be drawn about health, religion, lifestyle, and even sexual preference. Machines that collect location data can also introduce more 'traditional' security problems, such as the risk for burglary or stalking. In light of recent developments in the EU, including the alarming rise of terrorist attacks, smart vehicles pose a new unforeseen security risk as they can be hacked and used to cause serious damage through remotely fiddling with the brakes, for example. Profiling has also been identified as a data protection challenge that would be strengthened by the use of automated vehicles. Stakeholders can utilise personal location data, derived from automated vehicles, for example by placing an in-car advertisement that is based on the passenger's profile on the data subject's route. Furthermore, the actual route of the automated vehicle can be adjusted in accordance with the passenger's profile, taking the passenger to shops where it is likely that the data subject ends up making an unplanned stop to shop.

---

[252] Autonomous Vehicle Team, Technology Law and Policy Clinic. ' Autonomous Vehicle Law Report and Recommendations to the ULC Based on Existing State AV Laws, the ULC's Final Report, and Our Own Conclusions about What Constitutes a Complete Law' School of Law University of Washington <https://www.law.washington.edu/clinics/technology/reports/autonomousvehicle.pdf> accessed 14 February 2018.

In Article IV, I have chosen to approach these issues by discussing them in relation to some of the Articles of the GDPR, that deal with lawful processing (Article 6), and data quality principles (Article 5). The study regarding lawful processing is narrowed down into the paragraphs of Article 6 that concern private stakeholders. In other words, the grounds that relate to public interests have been left outside the scope of the study.

The alternatives, for requirements to process and collect personal data, are consent, performance of a contract, and legitimate interest. According to Article 6, of the GDPR, at least one of the requirements must apply, in order for processing to be lawful. In use of smart machines, it is however likely that many of the grounds apply at the same time. Even though one could presume that a user of an autonomous vehicle understands that, in order to communicate with its surroundings, the vehicle must collect and process location data, the main principle in use of smart devices, is that the default should be that location services are 'off' and that users can then give their informed consent to the location data processing.[253] Autonomous vehicles usually function through transmission and reception of data to and from its surroundings, and therefore a conclusion is drawn that consent may not be the most practical way for a location data processor to ensure the lawfulness of processing, because this might prove burdensome for the stakeholders.

Similar to consent, contract also proves to be an inefficient way of establishing lawfulness of personal location data processing, in the context of automated vehicles. The reason for this is that contract, as a ground for processing, must not be extended 'to justify the processing of data going beyond what is necessary'.[254] In practice, the data that a smart

[253] Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices' (WP 185, 16 May 2011) 14.

[254] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent' (WP187, 13 July 2011) 8.

machine needs, changes continuously and is therefore quite hard, if not impossible, to define in a contract between the data controller or –processor and the data subject.

This leaves us with the ground of 'legitimate interest', which according to Recital 47 of the GDPR, 'could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller'. Another requirement, identified in Recital 47 of the GDPR, for 'legitimate interest' to be an applicable ground for processing, is that 'a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place'. A conclusion is drawn that legitimate interest seems to be the processing ground that is best suited for securing legal grounds for personal location data processing, in use of automated vehicle technology. However the study does not suggest deserting consent and contract as grounds in specific situations.

Indeed, the fact that so many situations and contractual, as well as non-contractual, relationships between the parties on the IoT need to be analysed *in casu*, highlights the importance of data quality principles, such as proportionality, purpose limitation, data minimisation, and necessity.[255] One of the core aims of the principles is to help balance out different parties', such as the data controller's and data subject's, interests.[256] The study notes that in the IoT context, where data is collected and processed in immense amounts and where the methods and reasons for collection keep changing, most of the time the data quality principles cross boarder with each other. For the same reason, it is difficult to apply

[255] GDPR, art 5.

[256] Lee A. Bygrave 'Core principles of data protection' (2001) 7(9) Privacy Law and Policy Reporter 169 <http://www.austlii.edu.au/au/journals/PrivLawPRpr/2001/9.html> accessed 14 February 2018.

the principles in practice. Automated vehicles and other smart machines function if anything, in a way that requires data maximisation as opposed to data minimisation, which is a condition for processing under the GDPR. This contradiction will only become more confusing as the IoT technology develops further.

3.2. Overarching common factors and conclusions

The main research question of this study is: *Is the GDPR fit to deal with new technologies such as the IoT?* And in the concluding section of this summarising report an answer can be derived, being '*It remains to be seen'*. I base this answer on the following:

Throughout the four articles forming this dissertation, my central objective has been to put the GDPR to the test and see if it is fit to deal with IoT technology. I have done this by analysing the challenges that the IoT poses on EU data protection legislation and by identifying grey areas. Even though I have approached the issue from different perspectives in each article, all of them still end with the same conclusions ― in the IoT context there are no clear all purpose solutions, but most decisions and analyses need to be made on an *in casu* basis. Furthermore, it has become clear that core principles, such as fairness, transparency, data minimisation, and accountability play a crucial role when solving legal issues in the field of ever-changing IoT technology.

The study has helped identify a few shortages in the GDPR, some of which, after later reflexion, have proved to be found by other scholars too.[257] Firstly, there is a risk that the GDPR brings a misapprehension that the Regulation gives data subjects more control over their personal data than they actually do. Furthermore, the aim of simplifying the EU

[257] See for example Bert-Jaap Koops 'The trouble with European data protection law' International Data Privacy Law 4(4) (2014) 250; Paul De Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (n 202) 269.

data protection legislation, that is one of the aims of the reform, has proven to not be as successful as could have been hoped for, when reading the documents leading up to the GDPR. The DPD consists of 34 Articles, whilst the GDPR has altogether 99 Articles. The length of the Regulation alone, implies that we are talking about a complicated legislation: There is a risk that stakeholders and data subjects cannot properly understand the text. A conclusion can also be drawn that in adding so much detail into the Regulation it is meant to be fairly comprehensive. This in turn, as identified by *Bert-Jaap Koops* 'stretches data protection to the point of breaking and makes it meaningless law in the books'.[258] However, as has been identified in Article III, the GDPR includes vague terminology, such as 'insofar as this is possible'[259] and 'taking into consideration available technology'[260] leaving room for interpretation and as a consequence not really changing the *status quo* that much. Article III also shows, that when discussing contractual relationships in the IoT sphere, too much faith has been put into data controllers' know-how and actions. In the view of this study, it is an out-dated approach to assume that the controllers are always superior to the data processors.

The highlighted importance of a risk-based approach and accountability is present in all articles. At the time of the publication of Article I, the final version of the GDPR was not yet available and the paper suggested that more emphasis should be placed on a new principle of accountability. With the answer book in hand, these hopes have been fulfilled, at least to an extent.[261] In general, the themes of Article I; The changing of personal data quality in different stages of processing, the relationship between the data controller and the

[258] Koops (n 257) 250.

[259] GDPR, art 28.

[260] GDPR, arts 8, 17,

[261] DPD, arts 6 and 22-24; The accountability principle was however visible in the DPD already, although it wasn't expressly named.

data processor, and the concept of accountability are themes that recur in all the other following articles of the dissertation.

After the introduction of the reformed GDPR, some of the grey areas have been clarified. The accountability principle has been added as a literal addition to the data quality principles[262] and data processors have received more obligations.[263] The core issue with joint controllership, that is identified in Article I, is that the DPD forms a risk that either none of the stakeholders takes responsibility for mistakes towards the data subject, or that it is at least unclear to the data subject regarding whom to contact with issues regarding their personal data. The GDPR addresses this and brings changes to data controllers' and data processors' rights and obligations.[264] This topic is discussed in detail in Article III, which was written after the final version of the GDPR was known. As pointed out in Article IV, it can however be concluded that, even with the new Article 28 in place, confusion about the distribution of liability between different stakeholders prevails in many cases.

The updated data quality principles appear in all of the articles I-IV. In a situation where a case-by-case solution is needed, the principles are supposed to guide us to a correct and balanced outcome. The study shows, however, that there is a contradiction between theory and reality in this context. The legislator demands more respect for the principles, whilst the stakeholders dealing with the 'real world' fail to find a way to implement and apply the principles in practice: Personal data shall be minimised, but in fact it is being maximised. Data should be collected fairly and transparently, while in fact invisible sensors and algorithms collect data, often unnoticed. Data is supposed to be kept relevant and up to

[262] GDPR, art 5.

[263] GDPR, art 28.

[264] GDPR, art 28.

date, but data subjects change continuously, making it difficult for data controllers to distinguish between relevant and out-dated data. This issue has especially been underlined in Article II regarding children's personal data. The same article also discusses the issue with harmonisation: Harmonisation between the EU member states is one of the key aims of the data protection reform. However, in many instances much leeway has been left for the particular member countries, possibly obscuring the harmonisation effect. Article 8 of the GDPR is a perfect example of a failure in harmonisation. When the Regulation gives member states four different age limits to choose from, it is not harmonising the rules, but in fact making the situation even more complicated than it was under the DPD.

In its current state, it seems that the GDPR brings many new obligations and rules to stakeholders, but leaves them without simple ways to actually apply them in practice. We should see the GDPR as an opportunity, however, and not as an obstacle. As has been identified by *Paul De Hert* and *Vagelis Papakonstantinou* '[t]he Regulation is offering the tools with which to address problems of the past and boldly face the future; the use we make of them is entirely up to us'.[265] Even though the study shows that harmonisation of the data protection legislation, among EU member countries, will not be ideal, it will still be improved.[266] Future research into this topic will show how the member states have chosen to use their margin of appreciation, when it comes to, for example, age limits and processing of sensitive personal data. The technology will continue to develop and only time will tell how the new Articles of the GDPR fit their purpose, when facing future technical requirements, in a world one can only assume that will increase the need for

[265] De Hert and Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (n 202) 194.

[266] Peter Blume, 'The myths pertaining to the proposed General Data Protection Regulation' (2014) 4(4) International Data Privacy Law 269, 269.

personal data intensive processing. Now that the GDPR has become applicable, we will see how the careful criticism of this study holds and how member states and courts solve issues. Hopefully we will witness how member state legislation, together with instructions from the authorities and court decisions, slowly cover the grey areas identified in this study. At the publication of this doctoral dissertation, only a half year has passed since 25 May 2018, and the application of the GDPR. Hence, this study is indeed published at exactly the right time, linking the past EU data protection legislation to the reformed one, and highlighting weak points of the Regulation in a *de lege ferenda* manner.

4. Bibliography

Aarnio, Aulis, *The Rational as Reasonable* (Dordrecht: Kluwer 1987).

Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (WP136, 20 June 2007).

-- 'Opinion 13/2011 on Geolocation services on smart mobile devices' (WP 185, 16 May 2011).

-- 'Opinion 15/2011 on the definition of consent' (WP 187, 13 July 2011).

-- 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (WP 223, 16 September 2014).

Ashton, Kevin, 'That "Internet of Things" thing' (2009) RFiD Journal <www.rfidjournal.com/article/ print/4986> accessed 19 February 2018.

Atzori, Luigi and others, 'The Internet of Things: A Survey' (2010) 54 Computer Networks 2787 <http://elsevier.staging.squizedge.net/__data/assets/pdf_file/0010/187831/The-Internet-of-Things.pdf> accessed 11 May 2018.

Autonomous Vehicle Team, Technology Law and Policy Clinic, 'Autonomous Vehicle Law Report and Recommendations to the ULC Based on Existing State AV Laws, the ULC's Final Report, and Our Own Conclusions about What Constitutes a Complete Law' School of Law University of Washington <https://www.law.washington.edu/clinics/technology/reports/autonomousvehicle.pdf> accessed 14 February 2018.

Baker, William B and Matyjaszewski, Anthony, 'The changing meaning of "personal data"' featured story in *the Official News Letter of the International Association of Privacy Professionals* 11(3) (April 2011) <https://iapp.org/media/pdf/publications/advisor04_11_print.pdf> accessed 23 February 2016.

Banisar, David & Davies, Simon, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (1999) 18(1) John Marshall Journal of Computer and Information Law.

Bernal, Paul, *Internet Privacy Rights - Rights to Protect Autonomy* (Cambridge 2014).

Blume, Peter, 'The myths pertaining to the proposed General Data Protection Regulation' (2014) 4(4) International Data Privacy Law 269.

British Information Commissioner's Office, 'Big Data and Data Protection' <https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf> accessed 22 February 2016.

Bygrave, Lee A, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology 247.

-- ‘Core principles of data protection’ (2001) 7(9) Privacy Law and Policy 168 <http://www.austlii.edu.au/au/journals/PrivLawPRpr/2001/9.html> accessed 11 May 2018.

-- ‘The Place of Privacy in Data Protection Law’ (2001) 24(1) University of New South Wales Law Journal 277.

-- *Data Protection Law Approaching Its Rationale, Logic and Limits* (Kluwer Law International 2002).

-- ‘Digital Rights Management and Privacy - Legal Aspects in the European Union’ in E. Becker et al. (eds) *Digital Rights Management* (Springer-Verlag Berlin Heidelberg 2003) 418–446.

-- *Internet Governance by Contract* (Oxford University Press 2015).

Case C-28/08 P *European Commission v The Bavarian Lager Co. Ltd.* [2010] ECR I-06055.

Case C-70/10 *Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs (SABAM)* [2011] ECLI:EU:C:2011:771, Opinion of AG Cruz Villalón.

Case C-131/12 *Google Spain SL and Google Inc v Agencia Espagnola de Proteccion de Datos (EPD) and Mario Costeja Gonzales* [2014] ECR I-317.

Case C-131/12 *Google Spain SL and Google Inc v Agencia Espagnola de Proteccion de Datos (EPD) and Mario Costeja Gonzales* [2014] ECR I-317, Opinion of AG Jääskinen.

Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, Opinion of AG Jääskinen.

Case C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] OJ C 381.

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

Case C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] OJ C 381**,** Opinion of AG Cruz Villalón.

Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, Opinion of AG Campos Sánches-Bordona.

Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA ‘Rīgas satiksme’* [2016] OJ C 111, 29.3.2016, p. 10–1, Opinion of AG Bobek.

Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the presence of Facebook Ireland Ltd* ECLI:EU:C:2017:796 [2017], Opinion of AG Bot.

Case C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* [2017] ECLI:EU:C:2017:197.

Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:582, Opinion of AG Kokott.

Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994.

Case C-530/16 *European Commission v Republic of Poland* [2017] OJ C 14, 16.1.2017, p. 24–25, Opinion of AG Bobek.

Case C-73/16 *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálnycúrad finančnej správy* [2017] ECLI:EU:C:2017:253, Opinion of AG Kokott.

Charter of Fundamental Rights of the European Union [2007] OJ C-303/01 ('Charter').

Cherry, Denny, *The Basics of Digital Privacy - Simple Tools to Protect Your Personal Information and Your Identity Online* (Elsevier Inc. Online Resource 2014).

Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 ('COPPA').

Cohen, Julie E, 'What Privacy is for' in 'Synopsium: Privacy and Technology' (2013) 126 Harvard Law Review 1879.

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final ('GDPR 2012' or '2012 proposal').

Commission, 'Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data' COM(92) 422 final - STN 287 (15 October 1992).

Commission, Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance) OJ L 215 , 25/08/2000 p. 7-47 ('Decision 2000/520').

Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326 ('TFEU').

Council of Europe, 'Some definitions' <www.coe.int/en/web/echr-toolkit/definitions> Accessed 10 May 2018.

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108 Strasbourg (28 January 1981).

Council of Europe, *Handbook on European data protection law* (Publications Office of the European Union, Luxemburg 2014) 15 <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> accessed 10 February 2016.

Council of the European Union, 'General approach to the GDPR' 9565/15 (11 June 2015) <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf> accessed 26 April 2018.

De Hert, Paul and Gutwirth, Serge, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S., Y. Poullet, P. De Hert, J. Nouwt & C. De Terwangne (eds) *Reinventing data protection?* (Springer Science, Dordrecht 2009).

-- 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence' in Institute For Prospective Technological Studies - Joint Research Centre, o.c., 111-162 <ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf> accessed 10 February 2016.

De Hert, Paul and Papakonstantinou, Vagelis, 'Comment Google Spain Addressing Critiques and Misunderstandings One Year Later' (2015) 22(4) Maastricht Journal of European and Comparative Law 624.

-- 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 Computer Law & Security Review 179.

Decision 1/2010 of the Finnish Data Protection Board <http://www.finlex.fi/fi/viranomaiset/ftie/2010/20100001> accessed 25 February 2016.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105 13 April 2006) ('Data retention directive').

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), OJ L 201, 31.7.2002.

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 OJ L 281 , 23/11/1995 p. 31-50 ('DPD').

DLA Piper, 'EU study on the Legal analysis of a Single Market for the Information Society New rules for a new age?' (November 2009) <https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjNivDtt5XLAhUBLhQKHf8FCKsQFggkMAE&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdae%2Fdocument.cfm%3Fdoc_id%3D842&usg=AFQjCNFA_-PY3mF0GltQEFhEaOKUCeZ9FQ> accessed 26 February 2016.

ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978.

ECtHR, *Malone v. The United Kingdom*, No. 8691/79, 2 August 1984.

ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987.

ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007.

ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008.

ECtHR, *Uzun v. Germany*, No. 35623/05, 2 September 2010.

European Commission, 'Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security' (COM (90) 314 final (13.9.1990) <http://aei.pitt.edu/3768/1/3768.pdf> accessed 23 February 2016.

-- 'Communication from the Commission to the European Parliament and the Council - Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018' COM(2018) 43 final.

-- 'A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final.

-- 'Commission Staff Working Paper Impact Assessment' SEC (2012) 72 final (Brussels, 25 January 2012) <http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf> 68 accessed 8 February 2018.

-- 'Internet of Things Factsheet Privacy and Security 2012' <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753> accessed 19 February 2018.

-- 'Joint Statement on the final adoption of the new EU rules for personal data protection' Brussels, 14 April 2016 <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm> accessed 31 January 2018.

-- 'IoT Privacy, Data Protection, Information Security' <http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC4QFjAA&url=http%3A%2F%2Fec.europa.eu%2Finformation_society%2Fnewsroom%2Fcf%2Fdae%2Fdocument.cfm%3Fdoc_id%3D1753&ei=QDV2U62JE6uX0QW124H4Aw&usg=AFQjCNHoRL11Ce0INElpI0SALOzVlFHcwQ&bvm=bv.66699033,d.d2k&cad=rja> 3, accessed 9 February 2016.

European Parliament, 'Legislative train schedule' <http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-general-data-protection-regulation> accessed 30 January 2018.

Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values' May 2014, <http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf> accessed 19 February 2018.

Fish, Stanley, *There's no such Thing as Free Speech and it's a Good Thing, Too* (e-book version, Oxford University Press 1994).

Froomkin, Michael A, 'The death of privacy?' (2000) 52 Stanford Law Review 1461.

Gartner IT Glossary, 'Big data' available at <http://www.gartner.com/it-glossary/big-data> accessed 22 February 2016

GDPR Portal < https://www.eugdpr.org/the-process.html> accessed 29 January 2018.

Gregory, J Walters, *Human Rights in an Information Age: A philosophical Analysis* (University of Toronto Press 2001).

Hesselink, Martijn, 'A European Legal Method? On European Private Law and Scientific Method' (2009) 15(1) European Law Journal 20.

Hildebrandt, Mirelle, 'Privacy and Identity' in E. Claes, A. Duff & S. Gutwirth (eds) *Privacy and the criminal law* (Antwerp/Oxford, Intersentia, 2006) 61-104.

-- and Tielemans, Laura, 'Data protection by design and technology neutral law' 29(5) (2013) Computer Law & Security Review 509.

Hirvonen, Ari, *Mitkä metodit? Opas oikeustieteen metodologiaan* (Helsinki 2011).

Homepage of EU GDPR <https://www.eugdpr.org> last accessed 21 December 2017.

Hon, WK and others, 'The Problem of Personal Data in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 1' (2011) Paper No. 75 Queen Mary University of London, School of Law Legal Studies Research Paper 14.

-- 'Who is Responsible for Personal Data in Cloud Computing? The Cloud of Unknowing, Part 2' (2011) Queen Mary University of London, School of Law Legal Studies Research Paper No. 77/2011.

Hustinx, Peter, 'Data protection in the European Union' (2005) 2 Privacy & Informatie 62.

Inness, JC, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press 1992).

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238 ('Digital rights Ireland case').

Kamel Boulos, Maged N and Al-Shorbaji, Najeeb M, 'On the Internet of Things, smart cities and the WHO Healthy Cities' (2014) 13(10) International Journal of Health Geographics.

Kangas, Urpo, 'Minun metodini' in Juha Häyhä (ed.) *Minun metodini* (Porvoo 1997).

Kohlert, William J and Colbert-Taylor, Alex, 'Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles' (2014-2015) 31(1) Santa Clara Computer and High Technology Law Journal <http://digitalcommons.law.scu.edu/chtlj/vol31/iss1/3/> accessed 17 November 2017.

Koillinen, Mikael, 'Henkilötietojen suoja itsenäisenä perusoikeutena' (2012) 42(2) Oikeus 171.

Kolehmainen, Antti 'Tutkimusongelma ja metodi lainopillisessa työssä' in Tarmo Miettinen (ed.) *Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta* (Edilex 2016).

Koops, Bert-Jaap, 'The trouble with European data protection law' International Data Privacy Law 4(4) (2014) 250.

Kopetz, Hermann *Real-Time Systems. Design Principles for Distributed, Embedded Applications* (2nd edn, Real-Time Systems series, Springer Science & Business Media 2011 LLC).

Korpisaari, Päivi, 'Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta' (2015) 7-8 Lakimies 987.

Korpisaari, Päivi, 'Viestintäoikeus globaalissa yhteiskunnassa' in Päivi Korpisaari (ed.) *Viestintäoikeus nyt – Viestintäoikeuden vuosikirja 2014* (Forum Iuris 2015).

Kuner, Christopher, 'Data Protection Law and International jurisdiction on the Internet (Part1)'(2010) 18 International Journal of Law and Information Technology 176.

Lessig, Lawrence *CODE* (Version 2.0 Basic Books, New York 2006).

Leta Ambrose, Meg, 'It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten' (2013) 16 Stanford Technology Law Review 369

LIBE, Report A7-0402/2013 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN> accessed 26 April 2018.

Lindqvist, Jenna, 'The Internet of Toys is no child's play: Children's data protection on internet of things and in digital media: new challenges' In Tobias Bräutigam & Samuli Miettinen (eds.) *Data Protection, Privacy and European Regulation in the Internet Age* (Helsinki 2016) Forum Iuris 84.

-- 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' International Journal of Law and Information Technology 26 (2018) 45.

-- 'Automated vehicles and personal location data in a smart world – an EU perspective' (under peer review 2018).

Mantelero, A, 'The EU Proposal for a General Data Protection Regulation and the Roots of the "Right to be Forgotten"' (2013) 29 Computer Law & Security Review.

Maras, Marie-Helen, 'Tomorrow's Privacy – Internet of Things: security and privacy implications' 5/2 (2015) International Data Privacy Law 99.

Marx, Gary T and Muschert, Glenn W, 'Personal Information, Boarders and the New Surveillance Studies' Annual Review of Law and Social Science Science 3 (2007) 375.

Mayer-Schönberger, Viktor and Cukier, Kenneth, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (New York 2013).

Mäkinen, Jenna, 'Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things' (2015) 24(3) Information & Communications Technology Law 276.

-- 'The background and nature of data within EU data protection law with reference to new technology' in Päivi Korpisaari (ed) *Oikeus, tieto ja viesti: Viestintäoikeuden vuosikirja 2015* (Helsinki 2016) 103.

Nuotio, Kimmo, 'Oikeuslähteet ja yleiset opit' (2004) 7-8 Lakimies 1267.

O'Callaghan, Patrick, *Refining Privacy in Tort Law* (Springer-Verlag Berlin Heidelberg 2013).

OECD, '30 Years After: the Impact of the OECD Privacy Guidelines' (March 2010) <http://www.oecd.org/sti/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm> accessed 6 February 2018.

-- 'Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data' C(80)58 FINAL (23 September 1980).

-- 'Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' (2013) C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79 <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> accessed 26 April 2018.

Pagallo, Ugo, 'What Robots Want: Autonomous Machines, Codes and New Frontiers of Legal Responsibility' in Mireille Hildebrandt and Jeanne Gaakeer (eds) *Human Law and Computer Law: Comparative Perspectives* (Springer Dordrecht Heidelberg New York London 2013).

Peczenik, Aleksander, *On Law and Reason* (Dordrecht: Kluwer 1989).

Pitkänen, Olli, Tiilikka, Päivi, Warma, Eija, *Henkilötietojen suoja* (Alma Talent 2013).

Pöyhönen, J, *Sopimusoikeuden järjestelmä ja sopimusten sovittelu* (Suomalaisen Lakimiesyhdistyksen julkaisuja 1988) 94.

Reding, Viviane, 'The European data protection framework for the twenty-first century' International Data Privacy Law 2(3) (2012) 119.

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 95/46/EC (General Data Protection Regulation) OJ L 119/1 4.5.2016, p. 1–88 ('GDPR').

Reiman, Jeffrey H, 'Privacy, Intimacy and Personhood' (1976) 6(1) Philosophy & Public Affairs 26.

Richards, Neil, *Intellectual privacy rethinking civil liberties in the digital age* (Oxford University Press 2015).

Rodrigues, Ruben, 'Privacy on Social Networks: Norms, Markets, and Natural Monopoly' in Saul Levmore and Martha Nussbaum (eds) *The Offensive Internet, Speech Privacy and Reputation* (Harward University Press 2010) 237.

Rosen, Jeffrey, 'The Right to Be Forgotten' The Atlantic (July/August 2012) <https://www.theatlantic.com/magazine/archive/2012/07/the-right-to-be-forgotten/309044/> accessed 15 April 2018.

Saarenpää, Ahti, 'Verkkoyhteiskunnan oikeutta: johdatusta aiheeseen' (2000) 29(1) Oikeus 3.

Schwarzenberger, Georg, 'The Inductive Approach to International Law' (1947) 60(40) Harvard Law Review 539.

Selinger, Evan and Hartzog, Woodrow, 'Google can't forget you, but it should make you hard to find' Wired <https://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/> accessed 18 October 2018.

-- 'Google's action on revenge porn opens the door on right to be forgotten in US' The Guardian < https://www.theguardian.com/technology/2015/jun/25/googles-revenge-porn-opens-right-forgotten-us> 25 June 2015, accessed 18 October 2019.

Siltala, Raimo, *Oikeudellinen tulkintateoria* (Jyväskylä 2004) 507.

-- *Law, Truth, and Reason: A Treatise on Legal Argumentation* (Springer Turku 2011).

Solove, Daniel J, '"I've got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745.

-- *Understanding Privacy* (Harward University Press 2009).

-- 'Speech, Privacy and Reputation on the Internet' in Saul Levmore and Martha Nussbaum (eds) *The Offensive Internet, Speech Privacy and Reputation* (Harward University Press 2010).

-- 'Introduction: Privacy Self-management and the Consent Dilemma' (2013) 126 Harvard Law Review 1879.

-- 'What Google Must Forget: The EU Ruling on the Right to Be Forgotten', Linkedin (13 May 2014) <https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten> accessed 15 April 2018

The Editorial Board of The Washington Post, 'UnGoogled: The disastrous results of the "right to be forgotten"' (July 2014) <https://www.washingtonpost.com/opinions/ungoogled-the-disastrous-results-of-the-right-to-be-forgotten-ruling/2014/07/12/91663268-07a8-11e4-bbf1-cc51275e7f8f_story.html?noredirect=on&utm_term=.bab701f82ca6> accessed 15 April 2018.

Tiilikka, Päivi, *Sananvapaus ja yksilön suoja* (Helsinki 2007).

Tuori, Kaarlo, 'Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota' (2004) 7-8 Lakimies 1196.

-- *Ratio ja voluntas* (Alma Talent Oy 2007).

-- *Critical Legal Positivism* (Routlege 2017).

Wacks, Raymond, *Law, Mortality and the Public Domain* (Hong Kong University Press 2000).

Warren, Samuel D and Brandeis, Louis D, 'The Right to Privacy' (1890) 5 Harvard Law Review, V.IV.

Wolf, Christopher, 'Impact of the CJEU's Right to Be Forgotten: Decision on Search Engines and Other Service Providers in Europe' (2014) 21 Maastricht Journal of European and Comparative Law 547.

5. Appendix: Original publications