QUEEN MARY, UNIVERSITY OF LONDON
Department of Law

The Evolution of Data Protection and Privacy in the Public Security Context
-
An Institutional Analysis of Three EU Data Retention and Access Regimes

Carolin Möller

Submitted in fulfilment of the requirements of the Degree of Doctor of Philosophy - **Ph.D. (Laws)**

Supervisors: Professor Valsamis Mitsilegas and Professor Ian Walden

I, Carolin Möller, confirm that the research included within this thesis is my own work or that where it has been carried out in collaboration with, or supported by others, that this is duly acknowledged below and my contribution indicated. Previously published material is also acknowledged below.

I attest that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge break any UK law, infringe any third party's copyright or other Intellectual Property Right, or contain any confidential material.

I accept that the College has the right to use plagiarism detection software to check the electronic version of the thesis.

I confirm that this thesis has not been previously submitted for the award of a degree by this or any other university.

Carolin Möller

19 March 2017

Abstract

Since nearly two decades threats to public security through events such as 9/11, the Madrid (2004) and London (2005) bombings and more recently the Paris attacks (2015) resulted in the adoption of a plethora of national and EU measures aiming at fighting terrorism and serious crime. In addition, the Snowden revelations brought the privacy and data protection implications of these public security measures into the spotlight. In this highly contentious context, three EU data retention and access measures have been introduced for the purpose of fighting serious crime and terrorism: The Data Retention Directive (DRD), the EU-US PNR Agreement and the EU-US SWIFT Agreement. All three regimes went through several revisions (SWIFT, PNR) or have been annulled (DRD) exemplifying the difficulty of determining how privacy and data protection ought to be protected in the context of public security. The trigger for this research is to understand the underlying causes of these difficulties by examining the problem from different angles.

The thesis applies the theory of 'New Institutionalism' (NI) which allows both a political and legal analysis of privacy and data protection in the public security context. According to NI, 'institutions' are defined as the operational framework in which actors interact and they steer the behaviours of the latter in the policy-making cycle. By focusing on the three data retention and access regimes, the aim of this thesis is to examine how the EU 'institutional framework' shapes data protection and privacy in regard to data retention and access measures in the public security context. Answering this research question the thesis puts forward three main hypotheses: (i) privacy and data protection in the Area of Freedom, Security and Justice (AFSJ) is an institutional framework in transition where historic and new features determine how Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU) are shaped; (ii) policy outcomes on Articles 7 and 8 CFREU are influenced by actors' strategic preferences pursued in the legislation-making process; and (iii) privacy and data protection are framed by the evolution of the Court of Justice of the European Union (CJEU) from a 'legal basis arbiter' to a political actor in its own right as a result of the constitutional changes brought by the Lisbon Treaty.

Acknowledgements

Before deciding to conduct a Ph.D. I was warned several times that it is a rather solitary journey. While this is has proven true in many respects, it neglects that the completion of this journey is only possible with the support of other people. I would like to express my gratitude to everyone who contributed to this research. First and foremost, I would like to thank my supervisors, Professor Valsamis Mitsilegas and Professor Ian Walden. I feel privileged that my Ph.D. has been supervised by two extremely knowledgeable and acclaimed academics. Their patience and constructive feedback were indispensible for the completion of my Ph.D. Valsamis has always spotted the common thread running through single components of my research and his feedback was crucial in guiding me towards the essential and innovative issues to be scrutinised. He supported me in building a coherent thesis and helped me to gain confidence in my work particularly in moments when I got lost in details. Ian's feedback - particularly on the data protection aspects- helped me to construct my arguments consistently and accurately. His views and ideas have motivated me to challenge conventional views and helped me to be more courageous in expressing my own interpretations. Second, I would like to thank the CSES team and in particular Jack Malan. Through my work at CSES I was not only able to finance my Ph.D., but I also learned about the secrets of evaluating EU legislation. In some instances my work at CSES inspired my Ph.D. research but above all it helped me to grow on a professional and personal level. I would also like to thank Jack and the other CSES partners for their general support and interest in my Ph.D. Third, I would like to thank my friends and colleagues at Queen Mary and other universities/institutions who have shown an interest in my work. I would particularly like to express my gratitude to the 14 interviewees who have kindly set some time aside to share their views on my research topic and to Emilio De Capitani who helped me to arrange some of those. The insights gained during these interviews provided me food for thought and allowed me to test my arguments. Last and most importantly, I would like to thank my friends and family for their emotional support. My friends in London and Germany always encouraged me to carry on even in difficult moments. My boyfriend Francesco stood always by my side through the last three years. Without his love, care and patience this Ph.D. would have been impossible. He always supported me on every aspect of this journey, cheered me up and brought light into my days and heart. My brother Marcell, by also doing a Ph.D., was always able to empathise with the ups and downs that I experienced. Most of all I am grateful to all the support offered by my parents, Inge and Dieter, for being the ones on my side not only in every step of my PhD but also in every step of my life. They encouraged me to find my own path and supported me in all respects. Words could never be enough to express my gratitude.

Abbreviations

AFSJ	Area of Freedom, Security and Justice
ATS	Automated Targeted System
ATSA	Aviation and Transportation Security Act
CBP	US Customs and Border Protection
CFREU	Charter of Fundamental Rights of the European Union (also referred to as 'Charter')
CFSP	Common Foreign and Security Policy
CJEU	Court of Justice of the European Union
COM	European Commission
DHS	Department of Homeland Security
DPD	Data Protection Directive (Directive 95/46/EC)
DRD	Data Retention Directive (Directive 2006/24/EC)
DRI	(i.e. Digital Rights Ireland) refers to C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others v. Ireland* of 8 April 2014.
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EP	European Parliament
EU	European Union
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
HI	Historical Institutionalism
HLCG	High-Level Contact Group on Data Protection
JHA	Justice and Home Affairs
LEA	Law Enforcement Agencies
MEP	Member of the European Parliament
MS	Member States of the European Union
NI	New Institutionalism
PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
PDBTS	High-Level Political Dialogue on Border and Transportation

PIU	Passenger Information Unit
PNR	Passenger Name Records
QMV	Qualified Majority Voting
RCI	Rational Choice Institutionalism
SI	Sociological Institutionalism
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEC	Treaty on the European Communities
TEU	Treaty on the European Union
TFEU	Treaty of the Functioning of the European Union
TFTP	Terrorist Financing Tracking Programme
TRIP	Traveller Redress Inquiry Program
US	United States of America

Table of Contents

CHAPTER 1 – INTRODUCTION

1. Objective(s) of the thesis

The aim of this thesis is to analyse how the EU institutional framework shapes data protection and privacy in regard to data retention and access measures for public security purposes. By following this overarching objective the thesis examines three data retention regimes in the EU that have been adopted for the purpose of fighting serious crime and terrorism: the Data Retention Directive (DRD), the EU-US SWIFT Agreement and the EU-US PNR Agreement. While two of those regimes have an external dimension, it has to be noted that the thesis assessed them mainly from an EU perspective rather than adopting a comparative approach. The reason for choosing those three case studies is their similarity in terms of the political and institutional context leading to their adoption, the nature of the legislation and the similarity in regard to the nature of safeguards on the rights to privacy and data protection. Besides the similarity they are also marked by differences. First, they concern different sets of data namely traffic, location, passenger and financial messaging data. Second, they combine an EU internal (DRD) and EU external (PNR, SWIFT) perspective. Third, the regimes have different levels of maturity. In *Digital Rights Ireland*, the Court of Justice of the European Union (CJEU) annulled the DRD for its disproportionate interference with Articles 7 and 8 CFREU. The other two regimes are still in force but there is no consensus among politicians, practitioners, academics and civil society on whether they are proportionate.[1] Fourth, while all three regimes are examples of where data is retained for public security purposes the nature of retention varies. In regard to the DRD, service providers need to indiscriminately retain data for a certain period of time while subsequent law enforcement access to the data is not regulated by the measure. In contrast, the PNR and SWIFT Agreements both regulate in the first instance transfer and access to data while laying down retention conditions after

[1] Note that Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis* of 21 December 2016 (hereinafter *Tele2 Sverige*) provide further clarity in regard to the legality of general data retention requirements while *Opinion 1/15* Request for an Opinion submitted by the European Parliament on the Draft Agreement between Canada and the European Union on the Transfer and Processing of Passenger Name Record data, forthcoming (hereinafter *Opinion 1/15*) will provide insights into the proportionality of the EU-Canada PNR Agreement. This will also have implications for the EU-US PNR Agreement.

the authorities obtained the data. Minding the common and distinct features of the three regimes, the relevance of the institutional framework and institutional actors in shaping data protection and private life is the subject of this thesis. Accordingly, the thesis is structured around the subsequent three hypotheses:

- **Hypothesis 1: '**Privacy and Data Protection in AFSJ' is an institutional framework in transition implying that both established as well as new institutional features co-exist and commonly determine how data protection and privacy is shaped in relation to public security.
- **Hypothesis 2:** The EU institutional framework enables EU legislative actors to pursue strategic preferences in the legislation-making process and thereby influences the way privacy and data protection is shaped in the public security context.
- **Hypothesis 3:** The transitional nature of the EU institutional framework contributed to the CJEU's evolution from a 'legal basis arbiter' to a political actor in its own right that increasingly determines substantial aspects relating to privacy and data protection in the public security context.

2. Methodological approach

While being guided by the overarching research question and the related hypotheses, the thesis applies three main research methodologies. First, primary sources will be examined. Primary sources are defined in this thesis as any source deriving directly from the EU institutional actors.[2] This includes the examination of EU and former EC Treaties as well as an analysis of secondary legislation such as the DRD, the various versions of the PNR and SWIFT Agreements and EU data protection legislation such as the Data Protection Directive, the e-privacy Directive, the Framework Decision 2008/977/JHA and the new data protection package.[3] It also includes the analysis of

[2] Note that since the thesis applies an approach accounting for political and legal assessments, primary sources are not only legally binding materials but also policy documents.
[3] 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 2016*, L 119 (hereinafter GDPR) and Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and

ECtHR and CJEU jurisprudence most notably *Digital Rights Ireland*, *Schrems*, *Tele2 Sverige*, *Opinion 1/15*[4] as well as other relevant CJEU as well as ECtHR cases. While a more detailed assessment of the relationship between the ECtHR and CJEU will follow in Chapter 3 it has to be noted from the outset that ECtHR case law is relevant for the purposes of the thesis since the ECHR is constitutionally enshrined in EU law[5] resulting in cross-fertilisation between ECtHR and CJEU jurisprudence. In addition to legislation and case law, policy documents of the European Council, the European Commission and the European Parliament will be assessed such as Commission Communications, EP Resolutions and Motions as well as Council Positions and reports. Not only official documentation but also informal and/or confidential documents are scrutinised such as letters exchanges between the institutional actors or recommendations of the institutional legal services. Most of the restricted material derives from '*Statewatch* observatories' which are online collections of restricted policy documents in relation to EU Justice and Home Affairs Policy which have been leaked.[6]

Second, secondary sources will be assessed which are defined as any source which does not immediately derive from EU institutional actors but which assesses the latter or any results thereof. This includes the review of academic literature both on theoretical aspects and on policy outcomes and their legality. Due to the relevance of both legal and political analysis the literature reviewed includes a wide range of topics and includes works of political scientists and legal academics. In addition to academic literature, secondary sources also include the views of relevant stakeholders such as opinions or recommendations of the European Data Protection Supervisor and opinions of the Article 29 Working Party. While those actors are positioned within the EU institutional setting, they are independent of the EU institutional actors and provide independent advice on policies and their legality. Assessment of other bodies also play a role, for example literature of UN bodies or NGO's have been accounted for to some extent. On certain occasions journalistic sources were used. For example,

---

repealing Council Framework Decision 2008/977/JHA *OJ 2016, L 119* (hereinafter Police and Criminal Justice Data Protection Directive).

[4] Note that according to Article 218 (11) TFEU the EP, the Commission or the Council may request an opinion of the CJEU on the legality of an international agreement. The CJEU opinion is binding and an agreement may not enter into force in case the CJEU opinion is negative unless the Agreement itself or the Treaties are amended. Only the AG Opinion has been published before the thesis has been finalised.

[5] Article 6 TEU and Article 52 (3) CFREU. Note however that the EU did not yet accede to the ECHR.

[6] The Statewatch observatories can be accessed via: http://www.statewatch.org/.

the information relating to the Snowden leaks or the SWIFT leaks were in the first instance analysed in journalistic publications.

Third, to a limited extent qualitative interviews have been conducted to gain an understanding of information not publicly available and to obtain views of stakeholders that are or were directly involved in the process of policy formation or review. The added value of the interviews is that they allow one to gain first hand information and interpretations of the emergence and legality of policies. In total, 14 interviews have been conducted mostly with EU Commission officials, current and former European Parliament officials and an official at the CJEU. Some interviews were also conducted with employees from the EDPS. In addition, one conversation has been held with an US representative and one of the interviewees was an investigative journalist specialising on surveillance measures. When references to interviews are made in the thesis, only the role of the interviewee will be mentioned while refraining from providing names since some interviewees wished to remain anonymous.

The thesis acknowledges that in order to answer the research question both political and legal considerations need to be accounted for. The approach of 'New institutionalism' (NI) facilitates such a dual assessment. Weiler argued that in order to understand constitutional development in the European Union the relationship between political power and legal norms is key.[7] NI defines institutions as the legal and normative frameworks guiding actions of political actors.[8] NI has been chosen since it allows the amalgamation of political science-based and legal analysis and it is able to unravel the complex interaction between political and legal processes. On the one hand NI emphasises the importance of 'institutions' allowing an in-depth analysis of the EU legal order relating to AFSJ and privacy/data protection. On the other hand, by arguing that institutions shape strategic preferences, NI helps to understand the behaviour of different EU institutional actors and thereby assesses why the three data retention regimes emerged and why institutional actors shaped privacy and data protection in a certain way. NI can be applied to understand the role of both the traditional legislation-making actors as well as the CJEU (as emerging political actor) in shaping certain policy outcomes ex-ante and ex-post. While the role of the CJEU in shaping political developments in regard to the three case studies will be assessed, it

[7] Weiler, J.H.H. (2001). The Transformation of Europe. *Yale Law Journal,* vol. 100 (8), p. 2408.
[8] The main features of NI theory are explained in Chapter 2 of this thesis.

is beyond the scope of the thesis to assess whether this potential role is intentional or unintentional. The latter would require a detailed assessment of preferences and the formation thereof of the single judges and the dynamics between the judges in respect to each ruling, which goes beyond the scope of the thesis.

3. Terminology

While a detailed account of terminology used in this thesis is available in the table of abbreviations, it is important to point out several key issues. First, key legislation and international agreements are labelled in the following way. Directive 2006/24/EC[9] is mostly referred to as the 'Data Retention Directive' or 'DRD'. Furthermore, the term 'SWIFT Agreement' refers to the 'Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program.' It has to be noted that there two versions of the SWIFT Agreement. While the term 'SWIFT I'[10] refers to the Agreement reached in 2009, the term 'SWIFT II'[11] refers to the Agreement of 2010. The thesis at hand does in almost all cases refer to the SWIFT II Agreement unless specified. It has to be noted that secondary literature either uses the term "TFTP Agreement" or "SWIFT Agreement". The reason for adopting the latter title is to avoid confusion between the US internal TFTP programme and the programme subject to the EU-US agreement. The term 'PNR Agreement' refers to the 'Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security'.[12] It has to be noted that there are four

[9] Directive 2006/24/EC 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 2006, L 105* (hereinafter Data Retention Directive or DRD).
[10] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program *OJ 2010 L 8/11,* (hereinafter: "SWIFT I").
[11] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program *OJ 2010 L 195/5,* (hereinafter: "SWIFT Agreement" or "SWIFT II").
[12] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security *OJ 2012 L 215*.

different versions of the PNR Agreement: 2004 PNR Agreement,[13] 2006 PNR Agreement,[14] 2007 PNR Agreement[15] and 2012 PNR Agreement.[16] If not further specified, reference is always made to the 2012 PNR Agreement. When referring to all three instruments commonly (i.e. the SWIFT and PNR Agreements and the DRD), reference is made to 'data retention and access regimes'. It has to be noted that while in all regimes access and retention for public security purposes takes place, there are differences regarding the timing and nature.[17]

Second, since the aim of this thesis is to assess data retention and access measures in the context of public security it is crucial to have an understanding of the latter concept. EU legislation and case law refers to various dimensions of security, such as 'international security'[18], 'national security'[19], 'internal security'[20] and 'public

[13] Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, *CE/USA/en 1*. See also: Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, (notified under document number C(2004) 1914), *OJ 2004 L 235;* Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, *OJ L 2004 183*.

[14] Council Decision 2006/729/CFSP/JHA of 16 October 2006 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (annexed Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security) *OJ 2006 L 298*. See also the letter exchange in relation to Agreement between the Council Presidency and the Commission and the Department of Homeland Security (DHS) of the United States of America, *OJ C 259*.

[15] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) (Annexed Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), *OJ 2007 L 204*.

[16] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security *OJ 2012 L 215.* See also: Council Decision of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security*, OJ 2012 L 215*.

[17] See section 1 of this chapter and introduction to Part III.

[18] Joined Cases C-402/05 P and C‑415/05 *P Kadi and Al Barakaat International Foundation v Council and Commission* of 3 September 2008, para. 363; and Joined Cases C‑539/10 P and C-550/10 *P Al-Aqsa v Council* of 15 November 2012, para. 130.

[19] The ECHR and ECtHR case law consider national security as legitimate ground for interfering with Article 8 (1) ECHR. For example, in *Klass and others v. Germany*, Application no. 5029/71, judgment of 6 September 1978 the ECtHR accepts terrorism as threat to national security. Under EU law 'national security' is considered to be at the heart of national sovereignty and beyond EU competence. Respectively, Article 4 (2) TEU states that national security is an essential state function and thus it remains the sole responsibility of the Member States.

security.'[21]. It is important to acknowledge the differences between these different concepts as they trigger different legal frameworks and justify different types of legal actions. For example, national security and internal security lie beyond the competences of the EU and they can thus not be used as justification for EU action.[22] Furthermore, 'international security' implies security on the international level but it can only be a justification for EU action if it serves security within Europe.[23] Minding these significant differences, all dimensions of security overlap in one point by referring to a status where 'harm or threat to the well-being of persons' is absent. The thesis understands and uses the term 'public security' in the latter way by understanding it as a desirable status in any democratic society where threats to life and well-being of persons are absent. All three case studies under scrutiny in the three case study chapters are measures that strive for maintaining or achieving a state of public security by preventing, detecting, investigating and prosecuting serious crime and terrorism.[24]

It is worth pointing out that 'security' has the status of a fundamental right. Both ECHR and CFREU stipulate that "[e]veryone has the right to liberty and security of person."[25] While both ECtHR and CJEU jurisprudence on those articles refer mostly to liberty, the CJEU has acknowledged that "Article 6 of the Charter lays down the right of any person not only to liberty, but also to security."[26] Apart from this statement, ECtHR and CJEU jurisprudence does not further elaborate on the security dimension of Articles 6 CFREU and 5 ECHR[27] and instead treats public

---

[20] The TFEU refers to internal security on some occasions, which essentially means national security (see Articles 71, 72 and 276 TFEU). In EU external relations discourse, 'internal security' refers to the security within the EU vis-à-vis third countries. See for instance: Report of the Council submitted to the European Council. European Union Priorities and Objectives for External Relations in the Field of Justice and Home Affairs. *Council Doc. 7653/00,* Brussels, 6 June 2000.

[21] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others v. Ireland* of 8 April 2014, (hereinafter Digital Rights Ireland or DRI), para. 41

[22] Article 4 (2) TEU

[23] This has been called "internal-external security nexus". See for instance: Eriksson, J. & Rhinard, M. (2009) The Internal External Security Nexus: Notes on an Emerging Research Agenda, *Cooperation and Conflict,* vol. 44 (3), pp. 243–267.

[24] The meaning of terrorism and serious crime is often not clear. The early PNR and SWIFT Agreements and the DRD do not specify the definition of terrorism and/or serious crime. In later agreements this has been rectified. For example, Article 4 (1) (a) of the 2012 PNR Agreement lays down guidelines on what counts as terrorist offence while in Article 4 (1) (b) other crimes covered by the Agreement are considered to be those that are transnational and lead to a sentence of imprisonment for at least three years.

[25] Article 6 CFREU and Article 5 (1) ECHR.

[26] *DRI*, para. 42. See also AG Opinion on *Tele 2 Sverige*, para. 163.

[27] Neither the explanatory memorandum to CFREU, nor academic literature seems to acknowledge the existence of the security dimension of Articles 6 CFREU and 5 ECHR. See: Explanations relating to

security as legitimate ground to limit the rights to privacy and data protection. Although taking note of the fundamental rights dimension, the thesis adopts the same approach as the CJEU by regarding public security as ground for limiting privacy and data protection.[28]

Third, in the thesis the word 'indiscriminate' is used multiple times. 'Indiscriminate' can be simply defined as a situation where discrimination of any sort is not used or exercised. In the case of data processing for public security purposes the term seems however to carry a tripartite meaning. First, the term 'indiscriminate' can be interpreted to show that all data is processed without *discriminating* against the amount of data that can *hypothetically* and which is *actually* processed under a given legal measure. The core of this meaning is to identify whether data processing happens on a large scale. Second, 'indiscriminate' can also refer to a situation where data processing is not limited according to its *usefulness for the purpose of fighting crime*. This interpretation keeps the concept very broad and blurred as multiple arguments can show that data is chosen in a '*sufficiently discriminate'* way to ensure usefulness. A third interpretation of indiscriminate refers to a situation where 'there is no evidence capable of suggesting' a link to serious crime.[29] This implies a narrower interpretation of the term where 'indiscriminate' refers to a situation where one does not distinguish between two groups of data subjects namely those of suspected criminals and innocent individuals. In this thesis both the first and third meaning of 'indiscriminate' are applied. While the second meaning is also important this aspect is mainly discussed when assessing whether data processing is justified and proportionate.

Fourth, whenever reference is made to the 'Court of Justice of the European Union' the change in terminology from pre- to post-Lisbon has to be minded. While pre-Lisbon the Court was labelled 'Court of Justice', post-Lisbon, the Court as a whole was renamed to 'Court of Justice of the European Union' while the term 'Court

---

the Charter of Fundamental Rights, *2007/C 303/02, OJ 2007, C 303/17*; Guide on Article 5 of the Convention Right to Liberty and Security, retrieved 04.01.2017 from http://www.echr.coe.int/documents/guide_art_5_eng.pdf; see also: Peers, S. et al (2014) *The EU Charter of Fundamental Rights: A Commentary*. Hart Publishing.

[28] This approach is aligned to the overarching focus of the thesis on the rights to privacy and data protection. Consequently these two rights are perceived as the starting point of the legality assessment. In case it is decided to treat security and privacy/data protection as competing fundamental rights a different outcome of the proportionality assessment might be conceivable. As far as the author of this thesis is aware, this has not been done in respect to the three case studies and should therefore be subject to further research.

[29] *DRI*, para. 58.

of Justice' is reserved for the supreme body of the Court. While this thesis refers to rulings that have been issued both pre- and post-Lisbon, the term 'CJEU' is used consistently throughout the thesis. Fifth, on multiple occasions, the interaction of institutional actors during the legislation making procedure is assessed. Most of the times, reference is made to the 'co-decision procedure' and/or 'ordinary legislation making procedure'. It needs to be noted that those two procedures are equivalent, which is the reason why both terms are used interchangeably. However, the Lisbon Treaty officially replaced the name from 'co-decision' to 'ordinary' legislation-making procedure.

Sixth, another important point is the use of the term 'institution'. As explained earlier, the thesis makes use of 'New institutionalism' which is a theoretical approach where the term 'institution' refers to the operating framework in which institutional actors interact. In the EU context, 'institution' is used to refer to the main policy-making bodies such as the EP, the Commission and the Council. In order to avoid confusion the thesis refers to (i) 'institutions' or 'institutional framework' when discussing the operating framework in which EU actors interact with each other, and (ii) 'EU institutional actors or player(s)', 'actor' or 'player' when referring to one, to all or to several actors such as the European Council, the Commission, the European Parliament and the CJEU. Further details on the meaning of 'institution' in the framework of this thesis are provided in Chapters 2 and 3.

Ultimately, the term 'political actorness' or 'CJEU as political actor' is used to assess the CJEU's influence on policy outputs beyond the influence in the specific case at hand. As explained further in Chapter 2, political actorness is used to elaborate on the extent and the conditions under which Court-generated principles, reasoning and interpretation impact the range of policy options, political agendas, and policy outputs. This is not to be confused with branches of judicial activism scrutinising whether the outcome of a judgment has been influenced by political rather than legal considerations.[30] In other words, 'political actorness' focuses on the political and/or legislative consequences of a judgment whereas some strands of judicial activism focus on analysing the driving force or motivation leading to a judgment.

[30] For an explanation of different dimensions of judicial activism, see: Canon, B.C. (1983) Defining the Dimensions of Judicial Activism, *Judicature*, vol. 66 (6), pp. 236, 239; or: Kmiec, K. (2004) The Origin and Current Meanings of Judicial Activism. *California Law Review*, vol. 92, p. 1441.

4. Structure

The first chapter provides an introduction to the thesis. This includes a discussion of the objectives, relevance and structure of the thesis. The second chapter explains 'New institutionalism' as the theoretical framework applied to this thesis. It provides an overview of the key features of institutionalism and how this is relevant for this thesis. The chapter also explains the theoretical foundation of the three hypotheses that seek to answer the overall research question.

Chapter three focuses on examining the institutional framework of privacy and data protection in AFSJ. More specifically privacy and data protection in AFSJ is analysed from a historical institutionalist perspective. It is shown that the institutional framework is marked by incremental transformation since some aspects of the institutional framework exhibit features of 'old paths' while others exhibit new structures. Turning points or so-called '*critical junctures'* have contributed to the transitional character of the institution while path-dependence led to the stickiness to former institutional habits. The transitional nature of privacy and data protection in AFSJ is relevant for understanding the second and third hypothesis and the case study chapters since it shapes the evolution of all three regimes. In addition, Chapter three also establishes a framework to analyse the legality of the DRD, SWIFT and PNR Agreements.

Chapters four, five and six analyse the three data retention and access regimes –the Data Retention Directive, the SWIFT and the PNR Agreements- against the overarching research question on how the EU institutional framework shapes data protection and privacy in the public security context. More specifically, each of those chapters assesses whether and to which extent the second and third hypothesis is confirmed. Ultimately, chapter seven draws general conclusions from the single case study chapters and provides some future perspectives.

5. Why is this thesis relevant?

5.1 The increase of 'data driven' law enforcement practices and the effects

Throughout the last two decades the European Council adopted four roadmap policy programmes which set out the policy priorities in AFSJ. All of those programmes stress that any action undertaken by EU authorities has to be fundamental rights

compliant. The Tampere Programme mentioned that "[f]rom its very beginning European integration has been firmly rooted in a shared commitment to freedom based on human rights, democratic institutions and the rule of law."[31] This has been reiterated throughout the years in many different policy documents. Furthermore, also the latest roadmap programme mentions that "one of the key objectives of the Union is to build an area of freedom, security and justice (…) with full respect for fundamental rights"[32] Nevertheless, particularly since the Stockholm Programme policy makers have expressed the concern that it will become more challenging to "(…) ensure respect for fundamental rights and freedoms and integrity of the person while guaranteeing security in Europe."[33] This challenge particularly refers to the right to privacy and data protection as stipulated by the Charter of Fundamental Rights of the EU (CFREU) due to the increasing data-driven approach used by law enforcement authorities.

The omnipresence of personal data, which is an inherent feature of the information society, does neither spare criminals nor the law enforcement sector. Thus, public authorities were required to adapt to 21st century criminal challenges by adjusting investigative techniques. Data became a key to law enforcement activities since it offers as many or even more insights than for example traditional tapping or surveillance methods. At the same time, it is however significantly cheaper – a consideration which is particularly important in an era of economic austerity. This is even more so because data generated in the private sector can be misappropriated easily for law enforcement purposes. For instance, contractual relations of potential suspects[34] with online service providers can generate vast amounts of valuable data without necessarily generating costs to public authorities.[35] The cooperation between law enforcement agencies and the private sector was already observed by Garland in 1996.[36] He described this as 'responsibilization strategy' where acting upon crime is not done in a direct fashion through state agencies but indirectly by activating non-

[31] Tampere European Council Presidency Conclusions of 15 and 16 October 1999, para. 1.
[32] Council Conclusions of the European Council, *Council doc. EUCO 79/14* of the 27 June 2014, point 4, p.19.
[33] Stockholm Programme, *Council doc. 17024/09* of 2 December 2009, p. 4.
[34] It has to be noted though that not all useful data generated online needs to be necessarily derived from contractual relationships (e.g. collection of IP addresses in relation to internet searches).
[35] In some cases, LEAs may however be required to pay for data access. Furthermore, costs of data retention systems may need to be partially or completely borne by public authorities.
[36] Garland, D. (1996). The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society. *British Journal of Criminology*, vol. 36, pp. 445-71.

state agencies and organizations."[37] While Garland focuses on occasional requests, nowadays the dimensions have changed from occasional requests to constant reliance on data both via formal and informal channels.

There are various effects of 'data-driven' law enforcement activities. First, it may lead to the blurring of the boundaries between the public and private sector since law enforcement authorities make increasingly use of data held by companies. This has been described as the 'long arm' of law enforcement agents reaching out to privately held data in the fight against crime.[38] As shown later this is not only problematic for matters relating to the legitimacy/accountability of law enforcement activities but it also leads to regulatory challenges in a fragmented EU legal order. Second, in certain instances law enforcement agencies go beyond what is necessary for the sake of investigating a crime and instead make use of personal data to prevent crimes that may happen in the future.[39] This practice, which has been called 'speculative security practice',[40] is arguably fuelled both by mere technological possibilities[41] as well as by increasingly unpredictable threats and threat perceptions such as large-scale terrorism. Third and related to the previous point, another threat of 'data driven' law enforcement activities refers to *de facto* and *in abstracto* mass surveillance.[42] On the one hand, abuse of powers could lead to *de facto* mass surveillance where data is used excessively and indiscriminately for public security purposes or control purposes more generally. On the other hand, *in abstracto* mass surveillance is also concerning since the feeling of being under surveillance can have a *chilling effect* on data subjects both on privacy and other rights such as freedom of expression.[43] Fourth, the increasingly borderless nature of both data and criminal

[37] Ibid., p. 452. Note that the responsibilization strategy does not imply off-loading of state function or the 'privatisation of crime control' instead it represents a form of governing crime where the state retains its traditional functions but increases efficiency and output by developing new cooperation mechanisms with the private sector (see p. 454).
[38] Term used in relation to law enforcement access to data in the cloud: Walden, I. (2011). Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. *Queen Mary School of Law Legal Research Paper, No. 74/2011*. Retrieved 25.05.2016 from: http://ssrn.com/abstract=1781067
[39] It has to be noted that the boundary between 'investigating' and 'preventing' crime may be blurred in practice since sometimes the successful investigation of a crime is also the reason for preventing other crimes from happening.
[40] De Goede, M. (2012). *Speculative Security*. Minneapolis: University of Minnesota Press.
[41] Rosenbach, M. and Stark, H. (2015). *Der NSA Komplex. Edward Snowden und der Weg in die totale Überwachung*, Spiegel Buchverlag, p. 12.
[42] For an assessment of the relationship between privacy and surveillance see: Goold, J. (2009) *Surveillance and the Political Value of Privacy*. Amsterdam Law Forum.
[43] For example, the CJEU granted a prominent role to the perception of being under surveillance rather than surveillance *per se*: *DRI*, para. 37.

activity require an increased cooperation across borders. While on the EU level this amongst others impacts the degree of European integration in the AFSJ field, cooperation with non-EU countries has proven to trigger other concerns. As shown later, particularly law enforcement cooperation with the US is fraught with difficulties in regard to proportionality of security measures in light of fundamental rights. This was most prominently revealed with the Snowden leaks in 2013 which illustrated the wide-ranging nature of surveillance measures for security purposes adopted in the US.

As shown the transformation to an increasingly data-driven society has an impact on the way public security agencies operate. While this is necessary to keep pace with the transformation of society and thus crime itself it also led to challenges in regard to compliance with the rights to data protection and privacy. The thesis discusses this challenge by analysing the blurred boundary between on the one hand adequate adaptation of law enforcement practices in the information society and on the other hand new forms of fighting crime that are disproportionate in light of privacy and data protection.

5.2 The fluctuating nature of threat perception and the effects on EU cooperation in the public security context

In order to fully understand why certain public security measures are introduced on the EU level it is important to understand what is commonly perceived as a threat to public security.[44] In most cases, threat perception is in the first instance formed by events. For instance, it can be observed that in the Tampere Programme the fight against terrorism only plays a marginal role while it was lifted to a matter of 'new urgency' in the Hague Programme which was adopted shortly after 9/11. Thus, a large-scale terror event obviously leads to a different threat perception of terrorism. Nonetheless, the persistence and intensity of that threat perception largely depends on discourse of so-called 'securitizing actors' who are mostly the political leaders in a given nation-state[45] and the acceptance of such discourse by society.[46] The intersection of real threats and threat discourse can in a further step translate into legislative outcomes. It can often be observed that legislation in such a context

[44] For an overview of the perception of threat and security, see: Balzacq, T. (2005). The Three Faces of Securitisation: Political Agency, Audience and Context, *European Journal of International Relations* 11 (2), pp. 171 -201.
[45] Buzan, B. et al. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers, p. 21.
[46] Rieker, P. (2006). *Europeanization of National Security Identity: The EU and the Changing Security Identities of the Nordic States*. Routledge, p. 9

'securitises' more aspects than originally perceived as threat[47] and often fewer safeguards to individuals are granted. There are various examples for such a situation. For instance, when the Data Retention Directive was adopted in 2006 it can be argued that this was facilitated by the terror attacks in London and Madrid in the two previous years. Interestingly instead of being limited in scope to terrorism the Directive also applied to other forms of serious crimes. Another example is the PNR Directive, which was on the agenda for a long time but only the Paris attacks in 2015 facilitated its entry into force.[48] Similarly to the DRD it also covers serious crimes and thus goes beyond the very reason triggering its existence.[49]

As soon as the 'threat memory' and thus the discourse abates, new securitised legislation is less likely to be implemented and existing legislation is increasingly criticised due to a lack of necessity and fundamental rights compliance. The latter developments are also often steered by specific events. Accordingly, threat perception can be directed towards the government authorities where authorities themselves are considered to be a threat to civil liberty of the society. Major events triggering the emergence of this threat perception can for instance be leaks about secret governmental measures that have a negative impact on fundamental rights. 'Securitizing actors' who lead the discourse in this case are mainly civil society organisations, the media and to a lesser extent parts of the government apparatus (with an exception of Parliaments). For example a large-scale event raising concerns about government actions are the Snowden revelations about global surveillance regimes in 2013. The scandal and the discourse had a long-term impact on public security legislation that was in place. Arguably it had some impact on why and how

[47] In those instances, security develops to a type of 'universal good' implying that it can lead to state mobilization on a wide range of issues. See: Wæver, O. (1995). Identity, Integration and Security: Solving the Sovereignty Puzzle in EU Studies. *Journal of International Affairs*, vol. 48 (2), pp. 46-86.
[48] Apart from fighting crime, PNR data has also been considered to be useful for border control leading to the securitisation of migration. Further details, see for example: Huysmans, J. (2000) The European Union and the Securitization of Migration. *Journal of Common Market Studies*, vol. 38, pp. 751–777. See also: Marin, L. and Spena, A. (2016) Introduction: The Criminalization of Migration and European Dis(Integration), *European Journal of Migration and Law,* vol. 18 (2), pp. 147-156.
[49] It has to be noted that terrorism is regarded as distinct from other serious offences since terrorism mostly attempts to undermine the structure of a nation-state and thus threatens national security. Thus, the legitimacy of adopting measures for the purpose of safeguarding the security of a nation state may differ from measures concerning other forms of crime. The difference is evidenced by the fact that the EU has competence to act when serious crime is at stake but in relation to terrorism the situation is more blurred since Article 4 (2) TEU mentions that national security is the sole responsibility of the Member States. Apart from the distinctiveness of terrorism and serious crime, in practice the offences often overlap.

the CJEU annulled the DRD, which in turn might also influence future and existing laws.

It can thus be argued that political reality and public security priorities in the EU are steered by opposing threat perceptions that are in turn fuelled by events and respective discourse. Over the years, priorities and the nature of legislation thus swings like a pendulum between two opposing poles of (perceived) threats.[50]

The thesis spans several peaks of this securitisation cycle since the PNR and SWIFT Agreements originated after the 9/11 terror attacks while the DRD was adopted in the aftermath of the London and Madrid bombings. On the other side of the pendulum the Snowden revelations, and the CJEUs annulments of the DRD and the Safe Harbour Agreement are counter movements to the previous securitisation trend. The thesis aims to analyse how privacy and data protection are shaped in the public security context by acknowledging the securitisation cycles but by going beyond them when analysing proportionality.

5.3 The added value of the thesis

Many scholars have found an interest in studying the Data Retention Directive, the PNR Agreements, the SWIFT Agreements as well as AFSJ in general resulting in the publication of a plethora of articles, reports, case comments and books.[51] The large volume of academic literature shows on the one hand that those regimes are of a particularly interesting nature. On the other hand, this shows that they provide ample opportunity to study different angles of those regimes rendering each of those publications an original contribution in its own right. For example, while some scholars focused on assessing the legality of the regimes both from a procedural and substantial point of view, others have specialised on the interplay between policy actors during the legislation making procedures. The PNR and SWIFT regimes also feature in EU external relations literature, both from a legal and political science point of view.

By taking into account a large proportion of the relevant literature on those regimes the originality of this thesis lies in the holistic approach taken to analyse the impact of those regimes on privacy and data protection. The thesis does not only

[50] Interview with EDPS official
[51] A substantial part of this literature has been reviewed in this thesis. An overview can be found in the annex.

assess the purely legal implications of those regimes due to the author's belief that law cannot be understood as an 'independent organism' but instead it has to be regarded as integral part of the social system.[52] Thus, political and legal dynamics as well as the overall institutional framework that embraces privacy and data protection in the public security context are assessed.

Furthermore, a large proportion of existing literature does not take the latest developments into account (particularly recent CJEU case law). These new developments are crucial in changing the narrative and adding novel considerations. Most importantly, the recent developments shift the focus on the role of the CJEU in substantially influencing privacy and data protection in relation to data retention and access regimes. This adds an interesting aspect to the debate by addressing the political actorness of the CJEU and thus the balance of power between legislators and courts.

6. Limitations

It has to be noted that the thesis is subject to certain limitations. First of all it only focuses on a limited sample of data retention and access regimes for public security purposes in the EU, namely the DRD, the PNR and SWIFT Agreements. While the reasons for choosing those three case studies have been outlined earlier one has to acknowledge that also other large scale data retention and access regimes could have been interesting to assess such as SIS II, VIS, EURODAC, or the EU-Canada and EU-Australia PNR Agreements. Therefore, the findings only apply to the three case studies and generalisations of the findings to other regimes may not always be appropriate. Second, the thesis is limited *ratione temporis* to December 2016. This is important to acknowledge since both CJEU judgments as well as political developments continue to have a significant impact on the further development of EU public security legislation (e.g. current discussions on the e-privacy Directive) as well as the legality of various instruments (e.g. a legal challenge in Ireland of the Privacy Shield). It can be expected that this trend will continue and additional legislative instruments and case law in the near future will emerge, which cannot be taken into consideration.

[52] Term used by Shapiro, M. (2002). Judicial Jusrisprudence. In: Shapiro, M. & Stone Sweet, A. (2002). *On Law, Politics & Judicialization*. Oxford University Press, p. 1.

Ultimately, the theoretical approach applied to this thesis is also subject to certain limitations. While a more detailed overview of all limitations of NI is provided in chapter two, it suffices here to mention that the application of each theoretical approach involves certain limitations and can never explain each single aspect of legal and/or political realities.

PART I - NEW INSTITUTIONALISM, AND THE COMPLEXITY OF THE EU INSTITUTIONAL FRAMEWORK

CHAPTER 2 – NEW INSTITUTIONALISM: A HOLISTIC APPROACH EMBRACING POLITICAL AND LEGAL REALITIES

Introduction

The aim of this chapter is to provide an overview of 'New Institutionalism' being the theoretical approach applied in this thesis. More specifically, the three core hypotheses seeking to answer the overall research question are based on some underlying assumptions of NI. Thus it is necessary to set out the key features of NI as they structure the research in the subsequent chapters. It has to be noted that New Institutionalism has been mainly applied to assess policy outcomes by focusing on the interaction of legislators with given institutions before policies are adopted. However, in this thesis, NI is not only applied to analyse the behaviour of legislators but also to assess the role of the CJEU. This is important since in regard to all three case studies the CJEU's role is crucial in determining the legislative development.

The first part of this chapter provides an overview of the 'theoretical environment' in which New Institutionalism is situated. Furthermore, it explains why NI was chosen over other approaches. The second section provides an overview of the three branches of institutionalism and explains their relevance for the thesis. Fourth, limitations of NI are examined and ways are suggested to mitigate those limitations. Ultimately, three hypotheses in accordance with NI will be presented offering a structural framework for the assessment of privacy and data protection in AFSJ and the analysis of the three case studies.

1. Embedding New Institutionalism in a wider context

1.1 An overview of the theoretical landscape

There are various ways to conceptualise why certain policy outcomes are preferred over others, why they took a specific form and why they persist over time. In this thesis policy outcome refers to the way privacy and data protection is shaped in the public security context. Since this thesis deals with three EU data retention and access regimes an obvious choice is to assess the emergence of those legal instruments through European integration theory. This theory is not a single conceptualisation but

rather an umbrella concept for multiple different approaches aiming to assess how and why EU integration took place. More specifically, European integration theory has been defined as a " (…) field of systematic reflection on the process of intensifying political cooperation in Europe and the development of common political institutions, as well as on its outcome. It also includes the theorization of changing constructions of identities and interests of social actors in the context of this process."[53] The traditional and most renowned branches of European integration theory are neofunctionalism[54] and the opposing theory of (liberal) intergovernmentalism[55]. These two approaches emerged during the early days of the existence of the EU and focus mainly on assessing how and why EU Member States give up sovereignty to the EU as supranational actor.

Neofunctionalism developed shortly after the formation of the European Coal and Steel Community where various policy decisions of Member State authorities provided successively more competences to the EU level.[56] In this context, neofunctionalism argues that European integration started from modest sectoral beginnings and then gained momentum resulting in more ambitious integration in other areas. In other words, neofunctionalists ascribe a snowball-effect to EU integration where integration 'spills over' from one policy field to another. In contrast, intergovernmentalism developed as a response to the 1965 "empty chair crisis"[57] which questioned the stability and continuation of European integration. Intergovernmentalism criticises the neofunctionalist assumption that autonomous 'spill over' determines EU integration. Instead, intergovernmentalists assume that Member State authorities remain in control over which competencies are rendered to

[53] Wiener, A. & Diez, T. (2009) Introducing the Mosaic of Integration Theory. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. OUP, p. 4

[54] For an overview of the theory and the most important literature, see: Niemann, A. & Schmitter, P. (2009). Neofunctionalism. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. Oxford University Press; See also: Pollack, M. (2014) Theorising EU Policy-Making. In: Wallace, H., Wallace, W. & Pollack, M. (2014). *Policy-making in the European Union*. OUP.

[55] For an overview of the theory and the most important literature, see: Moravcsik, A. & Schimmelfennig, F. (2009). Liberal Intergovernmentalism. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. Oxford University Press; See also: Pollack, M. (2014). op. cit.

[56] One of the first writings on neofunctionalism is: Haas, E. B.(1958) *The Uniting of Europe.* Stanford University Press (reprinted 2004 by University of Notre Dame Press). See also: Haas, E.B. (1961). European Integration: The European and Universal Process, *International Organization*, vol. 4, pp. 607–46.

[57] The period from July 1965 to January 1966 has been considered as a halt of European integration and was labelled the "empty-chair crisis". See: Ludlow, N. P. (2006) De-commissioning the empty chair crisis: The community institutions and the crisis of 1965-6. In: Wallace, H., Winand, P. and Palayret, J.M., (eds.) *Visions, Votes and Vetoes: the Empty Chair Crisis and the Luxembourg Compromise Forty Years On*. Peter Lang.

the EU level and which are not. Some theorist even pointed out that EU Member State governments do not only remain in control but also that they are strengthened through the negotiations triggering the integration process.[58] In the 1980s, Andrew Moravcsik further developed intergovernmentalism into a fully-fledged theory known as 'liberal governmentalism'.[59] Both neo-functionalism and (liberal) intergovernmentalism are often-used theories explaining the process of integration either by focusing on the role of national governments and domestically grown interests in driving integration or the role of spill over in intensifying integration. They are thus useful to understand why a specific policy field is regulated on the EU level and whether/which national interests are most prevalent in driving this process.[60] In this way these two branches of European integration theory explain European integration from an overarching perspective and are particularly useful in assessing the formation of policy fields in the initial stages of the formation of the EU. [61] By focusing on causes as to why and whether Member States give up sovereignty they do not account for some EU level governance processes which developed throughout the years and are unique to EU legislation-making. Since the aim of this thesis is to understand the way privacy and data protection is framed in respect to data retention and access regimes on EU level this theory thus seems to be too one-dimensional.

Besides neofunctionalism and (liberal) intergovernmentalism, the boost of EU integration through the Single Market Act in the 1980s triggered the emergence of other approaches that have been classified as being part of European integration

---

[58] Milward, A.S. (2000), *The European Rescue of the Nation-State*, Routledge; Milward, A.S. & Lynch, F. M. B. (1993) *The Frontiers of National Sovereignty: History and Theory 1945–1992*. Routledge.

[59] In contrast to intergovernmentalism, liberal intergovernmentalism sets out three main elements: (i) a notion of national preference formation where national preferences are formed domestically including national and personal interests of chiefs of states, (ii) an intergovernmental model of EU-level bargaining where agreements reflect the relative power of each Member State, and (iii) a model of institutional preferences stressing the role of EU institutional actors in offering credible commitments for member state governments. For more details, see: Moravcsik, A. (1993). Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach, *Journal of Common Market Studies*, vol. 31, pp. 473–524. See also: Moravcsik, A. (1998), *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht.* Cornell University Press.

[60] In regard to Justice and Home Affairs, both neo-functionalist and intergovernmental interpretations can be found in: Bendel, P., Parkes, R. and Ette, A. (2011) *The Europeanisation of Control: Venues and Outcomes of EU Justice and Home Affairs Cooperation*.Lit Verlag. For an intergovernmental account of Justice and Home Affairs, see: Uçarer, E. M. (2013) Area of Freedom, Security, and Justice. In: Cini, M. & Perez-Solorzano Barragán, N. (eds.) *European Union Politics*. Oxford University Press. Press. See also: Labayle, M. (2013). The New Commission's Role in Freedom, Security and Justice in the Post-Lisbon Context. New Era or Missed Opportunity? In: Chang, M. & Monar, J. (eds.) *The European Commission in the Post-Lisbon Era of Crises*. College of Europe Studies No.16.

[61] Wiener, A. & Diez, T. (2009), op. cit., p. 4.

theory.[62] The most relevant approaches that have been used to explain policy outcomes are: the 'governance approach', 'policy network analysis' and 'constructivism'. The first of these approaches aims to assess how governance functions in the EU. While doing so governance is conceptualized as an "(…) extremely complex process involving multiple actors pursuing a wide range of individual and organizational goals, as well as pursuing the collective goals of the society."[63] Minding this process, the governance approach is particularly concerned with assessing the cooperation between government and social actors and the impact of this cooperation on policy outcomes. 'Policy outcomes' in this context mainly refers to assessing which style of governance is preferred, (such as a strictly 'regulatory style of governing'[64] or governance through softer means such as the Open Method of Coordination or other more voluntary mechanisms).[65] Given that two of the case studies examined in this thesis (PNR and SWIFT) are international agreements, it is worth mentioning that in recent years the governance approach has also been used to conceptualise the EU's external relations. This approach has been called 'external governance' and explains how the EU as an entity itself interacts with third parties and how the EU projects internal solutions to third parties.[66] Respectively, some scholars have assessed how EU governance is exported to third countries[67] while others concentrate on the form the 'rule transfer' takes and whether/how third countries adopt them.[68] While the external governance approach provides interesting insights, it seems not to be appropriate in the context of PNR and SWIFT. First, the

[62] ibid.; In this thesis, only approaches assessing policy outcome are mentioned. For an overview of all European integration theories, see: Pollack, M. (2014). op. cit.
[63] Peters, G & Pierre, J. (2009). Governance Approaches. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. OUP, p. 92. As noted by Peters and Pierre, not all governance scholars regard the process in this way. Some scholars only focus on the governance role of informal actors (e.g. NGOs, private sector individuals).
[64] This means that governance is taking place mainly by the introduction of binding legislation.
[65] The Open Method of Coordination is a soft governance tool aiming to spread best practice and achieve convergence towards EU goals. For more details, see for example: Szyszczak, E. (2006). Experimental Governance: The Open Method of Coordination. *European Law Journal*, vol. 12 (4), pp. 486–502.
[66] Lavenex, S. (2004) EU external governance in 'wider Europe'. *Journal of European Public Policy*, vol. 11 (4), p. 695.
[67] Here the emphasis is on *what* is exported to third countries. In other words, the focus is on the 'substance of governance modes', and the extent to which it affects policy-making processes in external states, see: Schimmelfennig, F. and Sedelmeier, U. (2004). Governance by Conditionality: EU Rule Transfer to the Candidate Countries of Central and Eastern Europe. *Journal of European Public Policy*, vol. 11 (4), p. 670. See also earlier literature, such as: Kohler-Koch, B. and Eising, R. (1999) *The Transformation of Governance in the European Union*, Routledge; Peters, G. (2000) Governance and comparative politics. In Pierre, J. (ed.), *Debating Governance*, Oxford University Press, pp. 36–53.
[68] Here the focus is on *how* rule transfer takes place and more specifically which form it takes. See: Schimmelfennig, F. and Sedelmeier, U. (2004), op. cit.

approach assumes that the EU actively and consciously establishes a proactive foreign policy. However, as shown in the chapters on PNR and SWIFT, EU policy can be regarded as rather reactive in the first years of cooperation where the strategy is based exclusively on the actions of the US as a third country. Second, the approach mainly focuses on modes of interaction and thus does not provide sufficient instruments to understand how and why the rights to privacy and data protection are shaped in a specific way.[69]

Another approach grouped under European integration theory is called 'policy networks analysis' connoting a "cluster of actors, each of which has an interest, or "stake" in a given (...) policy sector and the capacity to help determine policy success or failure."[70] Analysts adhering to this approach seek "(…) to explain policy outcomes by investigating how networks, which facilitate bargaining between stakeholders over policy design and detail, are structured in a particular sector."[71] While doing so, they follow three basic assumptions: (i) networks are frequently non-hierarchical since governance is based on mutuality and interdependence between public and non-public actors; (ii) the policy process is always dependent on the specific policy field and it can thus not be generalized; (iii) while governments remain ultimately in charge of governance, networks are able to influence the shaping of a specific policy area before decisions are taken.[72] Ultimately, a further approach grouped under European integration theory is called 'constructivism' and it is considered to be a concept that is 'notoriously difficult' to describe.[73] Broadly speaking, constructivism is based on the assumption that "(…) human agents do not exist independently from their social environment and its collectively shared systems of meanings ('culture' in a broad sense)."[74] Therefore, scholars applying a constructivist approach argue that institutions shape behaviours as well as preferences and identities of national actors and governments as a whole.[75] This idea contradicts classical theories (such as

[69] On the advantages and disadvantages of the governance approach, see Wolff, S. (2012) *The Mediterranean Dimension of EU Internal Security*. Palgrave, p. 24.
[70] Peterson, J. and Bamberg, E. (1999) *Decision-making in the European Union*. Palgrave, p.8.
[71] Peterson, P. (2009). Policy Networks. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. OUP, p. 105.
[72] Ibid.
[73] Term used by: Pollack, M. (2014). Theorising EU Policy-Making. In: Wallace, H., Wallace, W. & Pollack, M. (2014). *Policy-making in the European Union*, Oxford University Press.
[74] Ibid.
[75] See, for example: Sandholtz, W. (1993) Choosing Union: Monetary Politics and Maastricht. *International Organization*, vol. 47 (1), pp. 1-39. Christiansen, T., Jørgensen, K.E. and Wiener, A. (eds) (2001) *The Social Construction of Europe*. Sage Publications; Lewis, J. (2005) The Janus face of

(liberal) intergovernmentalism and neofunctionlism), which follow a rationalist ontology and are agency focused.[76] Apart from seeking to explain how preferences and identities of EU actors are shaped, constructivism has also been applied when examining the external relations of the EU.[77]

All above-mentioned approaches are rather 'meta-theoretical orientations' than fully-fledged theories and have certain limitations.[78] The governance approach is mostly focused on re-framing corporatism and other forms of interest intermediation.[79] In this way it focuses mainly on the influence of non-state actors on policy outcomes. This is not only difficult to assess (as they are not part of the formal decision making procedure) but also provides only a very limited account of how policies emerge. In regard to policy network analysis, even its proponents acknowledge that the approach does not answer many important questions about European governance and policy formation.[80] Ultimately, social constructivism is limited in scope since it does not produce a set of mid-range propositions when explaining policy outcomes.[81] The fact that all three approaches focus on a particular aspect of policy formation does not render them meaningless. In fact, all three approaches are valuable tools providing a partial account of why a certain policy outcome materialized while other potential outcomes do not. At the same time, however, it needs to be acknowledged that these approaches are not sufficient to provide an all-encompassing account of policy outcomes and persistence. Consequently -while not being adequate as leading theories- these three approaches can usefully be combined with more mature theories. It has to be noted that aspects of the governance, policy network and constructivism approaches are all reflected in

---

Brussels: socialization and everyday decision making in the European union, *International Organization*, vol. 59 (4), pp. 937–72.

[76] Haas, E.B (2001). Does Constructivism Subsume Neofunctionalism? In: Christiansen, T. et al. (eds) *The Social Construction of Europe*. Sage, pp. 22-31.

[77] A constructivist account of EU external relations is: Manners, I. (2002) Normative Power Europe: A Contradiction in Terms? *Journal of Common Market Studies*, vol. 40, pp. 235–258.

[78] Ibid.

[79] See, for instance: Frederickson, H.G. (2006) Whatever Happened to Public Administration? Governance, Governance Everywhere. In: Ferlie, E., Lynn, L.E., and Pollitt, C. (eds) *Oxford Handbook of Public Management.* Oxford University Press.

[80] Cowles, M.G. and Curtis, S. (2004) Developments in European Integration Theory: The EU as "Other". In Cowles, M.G. and Dinan, D. (eds) *Developments in the European Union*. Palgrave, pp. 296-309.

[81] Risse, T. (2009). Social Constructivism and European Integration. In: Wiener, A. & Diez, T. (eds.) *European Integration Theory*. OUP, p. 144.

NI.[82]

1.2 Shifting the focus to institutions

Having provided an overview of why certain branches of European integration theory are less appropriate to assess policy outcomes in the case of PNR, SWIFT and the DRD, in the following it will be explained why 'New Institutionalism'[83] –also being considered to be a branch of European Integration theory[84]- is applied in this thesis. While it has been argued that NI is not a fully-fledged theory –similar to the approaches mentioned above- the advantage of focusing on institutional aspects is that they offer tools to understand what mechanisms drive policy outcomes.[85] Thus, NI helps to understand how privacy and data protection is shaped in the public security context. Peterson and Shackleton claim that understanding political dynamics always begins with the understanding of the involved institutions and the policy actors.[86] This is even more relevant when assessing policies in the EU. Since the EU is neither a state nor a traditional international organisation, the institutional actors have a special status in a sense that a reciprocal relationship between a supranational body and 28 individual national systems exists. Furthermore, the EU institutional actors are in several instances the link between its Member States and the wider international community.

Therefore, it is relevant to assess their role in those international policy processes.[87] This appraisal of the importance of both institutions and the behaviour of actors operating within institutions is an indication of the recent tendency to evaluate

[82] For example, the notion of 'transgovernmentalism' is closely related to the policy network approach while the notion of 'norm-taking' is closely related to constructivism.
[83] Note that before the emergence of "New Institutionalism", literature on formal institutions such as rules and legislation existed and has been labelled "old institutionalism". (See: Bell, S. (2002) Institutionalism. In: Summers, J. (Ed.), *Government, Politics, Power And Policy In Australia*, pp. 363-380.) Nevertheless, this so-called "old institutionalism" was mainly descriptive and not concerned with theory building. Therefore, instead of reacting to "Old Institutionalism", "New Institutionalism" mainly reflects "(…) a gradual and diverse re-introduction of institutions into a large body of theories (such as behaviourism, pluralism, Marxism, and neorealism) in which institutions had been either absent or epiphenomenal (…)." See: Pollack, M. A. (2009). The New lnstitutionalisms and European Integration. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. OUP, p. 125.
[84] Note that although NI has been categorised as European integration theory it originally developed outside the EU context and was only later found to be applicable to the EU. See: Pollack, M. A. (2009), op.cit.
[85] Wolff, S. (2012), op. cit. p. 24.
[86] Peterson, J. & Shackleton, M. (2012). The EU's institutions: an overview. In: Peterson, J. & Shackleton, M. (eds.) *The institutions of the European Union*. Oxford University Press, pp. 1-19.
[87] ibid.

and analyse EU political dynamics through the lens of institutionalism. According to NI, institutions and the interaction of supranational players such as the European Commission, the EP and the CJEU undeniably plays an important role for the formation of political debate, for the expectations of significant actors and for policy outcomes.[88]

2. An overview of New Institutionalism and its three branches

2.1 The origin and key features of New Institutionalism

Institutionalism mainly developed as a reaction to behavioural perspectives that were influential in political science during the 60s and 70s.[89] Behaviouralism was not regarded as adequate because it was regarded as: (i) too contextual by perceiving social forces to be the only factor determining political life; (ii) too reductionist by regarding politics as the accumulation of individual decisions; (iii) utilitarian by ascribing calculated self-interest mainly to the agents making political decisions; and (iv) instrumentalist in assuming that decisions about allocating resources rather than decisions about the allocation of meaning is at stake in politics.[90] In contrast to behaviouralism, the focus on institutions has been regarded as an attractive solution since it would: "deemphasize the dependence of the polity on society in favour of an interdependence between relatively autonomous social and political institutions; deemphasize the simple primacy of micro processes and efficient histories in favour of relatively complex processes and historical inefficiency; deemphasizes metaphors of choice and allocative outcomes in favour of other logics of action and the centrality of meaning and symbolic allocation."[91] While emerging from the same roots, there are three different branches of institutionalism. It has to be noted that in more recent years, there have been attempts to add a fourth institutionalism to the three original branches.[92] For example, in order to account better for policy change, 'discursive'

[88] Vanhoonacker, S. (2011). The Institutional Framework. In: Hill, C & Smith, M. (eds.) *International Relations and the European Union*. Oxford University Press, pp. 76-100.
[89] Hall, P. A. & Taylor R. (1996). Political Science and the Three New Institutionalisms, *MPIFG Discussion Paper 96/6*, p. 5
[90] Reyners, J. (2015). Is there a fourth institutionalism? Ideas, Institutions, and the Explanation of Policy Change. In: Hogan, J. & Howlett, M. (eds.) *Policy Paradigms in Theory and Practice Discourses, Ideas and Anomalies in Public Policy Dynamics*. Palgrave.
[91] March, J. & Olsen, J. (1984) The New Institutionalism: Organizational Factors in Political Life. *The American Political Science Review*, vol. 78 (3), p. 738.
[92] Reyners, J. (2015). op. cit.

institutionalism has been developed.[93] While acknowledging the existence and relevance of this new approach, the thesis only assesses the original three branches, as they are more appropriate to the interdisciplinary approach of this thesis attempting to reconcile legal and political research. In the following, the key aspects of institutionalism and their relevance for this thesis will be outlined. Afterwards, the distinct features of the three different branches of NI will be explained in the subsequent sections.

2.1.1 How are 'actors' defined in the NI context?

It is necessary to conceptualise the meaning of 'institution' and 'actor'. Particularly, in the EU context, 'actors' are commonly referred to as EU institutions (i.e. the European Parliament, the European Commission, the European Court of Justice, the European Council) whereas NI uses the term 'institution' to refer to the 'operating framework' of those actors.[94] As pointed out in Chapter 1, in order to avoid confusion the thesis refers to (i) 'institutions' or 'institutional framework' when discussing the operating framework in which EU actors interact with each other, and (ii) 'EU institutional actors or player(s)', 'actor' or 'player' when referring commonly to all or several actors such as the European Council, the Commission, the European Parliament and the CJEU.

2.1.2 What does 'institution' mean?

Institutionalists generally accept that institutions are 'operating frameworks' that organise actions of policy actors into predictable and reliable patterns.[95] However, there is no generally accepted notion of what this 'operating framework' is comprised

[93] See: Schmidt, V. A. (2008): Discursive Institutionalism: The Explanatory Power of Ideas and Discourse. *Annual Review of Political Science*, vol. 11, pp. 303-36; Hay, C. (2008) Constructivist institutionalism. In: Rockman, B, Rhodes, R. & Binder, S. (eds). *The Oxford Handbook of Political Institutions*, pp.56- 74. Oxford University Press.

[94] In other words, institutions are the rules that guide the relationship and interaction between actors. See: Farrell, H. and Heritier, A. (2003). Formal and Informal Institutions under Co-decision: Continuous Constitution-Building in Europe. *Governance: An International Journal of Policy, Administration and Institutions*, vol. 16(4), p. 581.

[95] Streeck, W. & Thelen, K. (2005) Introduction: Institutional Change in Advanced Political Economies. In: Streeck, W. & Thelen, K. (eds.) *Institutional Change in Advanced Political Economies*. Oxford University Press, p. 9.

of. Not only do different branches of institutionalism have different views on the precise meaning of an 'institution' but also within each branch academics have developed different understandings of the meaning of 'institutions'. March and Olsen -who can be considered to have set the trend to analyse policy outcomes by applying NI – argued that institutions are "relatively stable collection of practices and rules defining appropriate behaviour for specific groups of actors in specific situations".[96] Being an advocate of the sociological institutionalist (SI) branch, Bulmer argued that "beliefs, paradigms, codes, cultures and knowledge" are belonging to the concept of institution.[97] From a historical institutionalist (HI) perspective, Thelen and Steinmo define institutions as "(…) formal or informal procedures, routines, norms and conventions embedded in the organisational structure of the polity or political economy. They can range from the rules of a constitutional order or the standard operating procedures of bureaucracy to the conventions governing trade union behaviour or bank-firm relations."[98] In HI terms it has also been argued that institutional rules encompass aspects such as institutional legacy and institutional culture.[99]

This thesis defines the notion of 'institution' as the legal framework that structures legislation-making when privacy and data protection for public security purposes is at stake. Respectively, the thesis takes a holistic view by including constitutional rules on privacy and data protection; secondary legislation laying down more practice-oriented rules; procedural rules applicable to legislation-making when data protection and privacy for public security purposes is at stake; and CJEU and ECtHR case law. Streeck and Thelen share this understanding and mention that so-called 'formal institutions' are 'formalised rules that may be enforced by calling upon a third party.'[100]

However, the thesis also acknowledges the importance of 'derivatives' of formal institutions. For example, ad hoc and informal modes of governance (such as the High-Level Contact Group on data protection between the EU and US[101]) are not

[96] March, J.G. and Olsen, J. (1998). The Institutional Dynamics of International Political Orders. *International Organizations*, vol. 52 (4), p. 948.
[97] Bulmer, Simon J. (1998) New institutionalism and the governance of the Single European Market, *Journal of European Public Policy*, vol. 5 (3), p. 369.
[98] Hall, P. A. & Taylor R. (1996), op. cit. p. 5. Referring to: Thelen, K. and Steinmo, S. (1992). Historical Institutionalism in Comparative Politics. In: Steinmo et al. (eds). *Structuring Politics*, p. 2 ff.
[99] Wolff, S. (2012), op. cit. p. 24.
[100] Streeck, W. & Thelen, K. (2005) op. cit., p. 10.
[101] Explained below in Chapter 5 (section 2.3).

formal institutions (in a sense that their outputs are enforceable) however since formal institutions grant spaces for the establishment of such frameworks they do play a role in shaping the behaviour of actors. Another example is the importance of normative paradigms and beliefs which derive from constitutional rights. In the context of the thesis two conflicting normative paradigms can be identified. On the one hand, the belief that 'public security' is of primary importance in a well-functioning democratic society is a normative paradigm often followed by the Council and partially by the Commission.[102] On the other hand, the belief that civil liberties –including privacy and data protection- are pivotal in guaranteeing the rule of law in democratic societies is the normative paradigm to which the EP and other non-legislating actors (such as the Article 29 Working Party and the EDPS) are subjected to.[103] It would be too simplistic to argue that actors are subject to either one or the other paradigm as in practice actors are subject to both but to varying degrees.

2.1.3 The notion of 'preference'

In NI literature the concept of 'preference' is important. On the one hand, there are 'fundamental preferences' which are the foundation of any action and emerge from aspects such as wellbeing, utility and desire.[104] On the other hand there are 'strategic considerations' which account for limitations posed by the institutional framework and the interaction between different actors.[105] While the fundamental preferences are important to get an overarching view on how preferences are formed and pursued in the institutional context, the thesis exclusively focuses on strategic considerations. This is mainly since an analysis of the former requires an assessment of Member State or personal positions, which goes beyond the scope of this thesis. Furthermore, fundamental preferences are inherently difficult to detect and to prove.

2.1.4 The key questions New Institutionalism seeks to answer

[102] Enshrined in Article 6 CFREU and Article 5 ECHR.
[103] Enshrined in Articles 7 and 8 CFREU and Article 8 ECHR.
[104] Hall, P.A. (2007) Preference Formation as a Political Process: The Case of the Monetary Union in Europe. In: Katznelson, I. & Weingast, B. (eds). *Preferences and Situations: Points of Intersection between Historical and Rational Choice Institutionalism*. Sage Foundation, p.154.
[105] ibid.

All branches of institutionalism research the same overarching questions while answering them in different ways: First, one question of NI relates to how the different actors behave. Depending on the branch of institutionalism, the answers to this range from instrumental human behaviour and strategic calculation to behaviour driven by familiar patterns.[106] Second, another core research question concerns what institutions are and what they do. Depending on the branch, institutions are regarded to provide actors certainty about present and future behaviour of other actors or to provide moral and cognitive templates for the activities of the other actors.[107] Ultimately, a last research question of institutionalists relates to the question of why do institutions persist over time? While one branch argues that institutional patterns give individuals better results in contrast to acting alone, the other branch argues that institutions are resistant to change because actors internalise them and take them for granted.[108] The three hypotheses set out later in this chapter and which guide the thesis focus on all three sub-question by focusing on the assessment of the complex institutional framework applicable to privacy and data protection in the public security context and by assessing how institutional actors interact with the institutional framework and with each other.

2.2 Historical Institutionalism (HI)

In contrast to the other branches, HI emphasises mainly the role of institutions and how they evolve over time instead of focusing on the actors within the institutions. The core research question of HI refers to why institutions persist over time and consequently assesses founding moments shaping policy and politics.[109] The respective claim is that institutions are "(…) relatively persistent features of the historical landscape and one of the central factors pushing historical development along a set of paths."[110] Thus, early HI literature focuses mainly on explaining how

[106] Hall, P. A. & Taylor R. (1996). *Political Science and the Three New Institutionalisms*, p. 7/8.
[107] Ibid.
[108] Ibid.
[109] Solingen, E. and Ozyurt, S. (2006). 'Mare Nostrum? The Sources, Logic, and Dilemmas of the Euro-Mediterranean Partnership'. In: Adler, E. et al. (eds) *The Convergence of Civilizations: Constructing a Mediterranean Region. Toronto*. University of Toronto Press, pp. 51-82.
[110] Hall, P. and Taylor, R. (1996), op. cit. p. 9. See also: Collier, D. and Collier, R. (1991) *Shaping the Political Arena*. Princeton University Press; Downing, M. (1992) *The Military Revolution and Political Change: Origins of Democracy and Autocracy in Early Modern Europe*. Princeton, University Press;

paths are produced. For instance, it has been emphasised that 'state capacities' and 'policy legacies' have an impact on subsequent policy choices.[111] In addition, it has also been argued that past lines of policy influence subsequent policy by mobilising societal forces to organise along some lines instead of others, to adopt particular identities, and to develop interests in policies that are costly to change.[112] Respectively, HI highlights "(…) unintended consequences and inefficiencies generated by existing institution in contrast to images of institutions as more purposive and efficient."[113]

To explain institutional persistence, HI employs a variety of concepts. Most prominently, HI introduced the concept of *path-dependence* suggesting that institutions are path-dependent since similar paths are reproduced over a period of time and due to the resistance towards institutional innovations or reform.[114] For instance, the policy processes leading to the DRD reveal some features of path dependence since the paradigm related to data retention developed over a long period of time even before specific events triggered further intensifications of the policy discussions.[115] Another example is the *path-dependent* CJEU interpretation of the correlation between privacy and data protection. By following the standards set by the ECtHR, the CJEU does not fully acknowledge the fundamental rights status of data protection and thus sticks to the "path" created by the ECtHR.[116] HI however acknowledges that there are certain events that might have the potential to disrupt a policy path. HI argues that these events are in most cases not changing the policy path if a specific shock/event leaves the possibility open to stick to the 'path'.[117] This means that whenever the costs of change are higher than continuing the original path

---

Krasner, S. (1988) Sovereignty: An Institutional Perspective, *Comparative Political Studies,* vol. 21, pp. 66-94.

[111] Weir, M. and Skocpol, T. (1985) State Structures and the Possibilities for 'Keynesian' Responses to the Great Depression in Sweden, Britain and the United States. In: Evans, P. et al. (eds.) *Bringing the State Back In*. Cambridge University Press, pp. 107–163.

[112] Pierson, P. (1994) *Dismantling the Welfare State?* Cambridge University Press; Jenson, J. (1989) Paradigms and Political Discourse: Protective Legislation in France and the United States Before 1914. *Canadian Journal of Political Science,* vol. 22 (2), pp. 235-258.

[113] Hall, P. and Taylor, R. (1996), op. cit., p. 10. See also: March, J. and Olsen, J. (1984) The New Institutionalism: Organizational Factors in Political Life, *American Political Science Review*, vol. 78, pp. 734–749 and North, D. (1990) *Institutions, Institutional Change and Economic Performance.* Cambridge University Press.

[114] Wolff, S. (2012), op. cit. p. 31.

[115] See Chapter 4 of this thesis.

[116] See Chapter 3 of this thesis.

[117] Hogan, J. (2006) Remoulding the Critical Junctures Approach. *Canadian Journal of Political Science*, vol. 39 (3), pp. 657-79.

the latter option is chosen; a process that has been labelled '*increasing returns*'.[118] Besides shocks/events another source of path-dependence is asymmetries of power. Respectively, "when certain actors are in a position to impose rules on others, the employment of power may be self-reinforcing."[119]

Nevertheless, the general adherence to the idea of institutional 'stickiness' raises problems in explaining why in certain situations institutions indeed change. Therefore, HI acknowledges that some events -either internal or external- can be significant enough to change the policy path. Such an institutional change has been called a '*critical juncture*' or '*branching point'* since it triggers the move from a historical development onto a new path.[120]A critical juncture requires certain criteria to be met such as particular timing, sequencing, small events and critical moments that produce distinct legacies.[121] In regard to the latter, early institutionalists mainly refer to crucial events such as economic crisis or military conflict while others do not have a well-defined response.[122] In regard to European integration, critical junctures can be intergovernmental conferences and summits as well as crises such as the current refugee crisis or the British referendum on Brexit. In regard to privacy and data protection in the public security context, the Snowden revelations or the terror attacks on 9/11 could be considered to be critical junctures in the form of events. In addition, the Lisbon Treaty as constitutional reform can be considered to be a critical juncture.

More recently, HI scholars have also argued that not only external events can trigger change of institutional paths. Instead 'institution-internal' characteristics or parameters might also create the pre-conditions for institutional change. For example, when institutions are the outcome of compromises or when contested -yet durable- arrangements are based on specific coalitional dynamics, they are inherently

[118] Pierson, P. (2000) Increasing Returns, Path Dependence and the Study of Politics. *The American Political Science Review*, vol. 94 (2), p. 252.
[119] Ibid., p. 259.
[120] Gourevitch, P. (1986) *Politics In Hard Times*. Cornell University Press; Collier, D. and Collier, R (1991). *Shaping the Political Arena*. University Press; Krasner, S. (1984) Approaches to the State: Alternative Conceptions and Historical Dynamics. *Comparative Politics*, vol. 16 (2), pp. 223–46.
[121] Pierson, P. (2000) Increasing Returns, Path Dependence and the Study of Politics. *The American Political Science Review*, 94 (2), pp. 251-67.
[122] For an early analysis, see: Skocpol, T. (1979) *States and Social Revolutions*. Cambridge University Press.

vulnerable to shifts.[123] Furthermore, in other instances institutions also grant a certain amount of flexibility in the interpretation of particular rules or in the way the rules are instantiated in practice.[124] This leeway provides room for institutional change.

2.3 Rational-Choice Institutionalism (RCI)

In contrast to HI, RCI mainly focuses on scrutinising the interaction between institutions and the actors operating within the institutions. Originally, RCI emerged from the study of US congressional behaviour, where RCI claims that congressional outcomes are stable because congressional institutions control and structure the policy options.[125] Subsequently, RCI has been increasingly applied to assess policy outcomes in the EU.[126] The strength/popularity of RCI can be explained with its ability to show the important role that information flows play for power relations and policy outcomes.[127] Furthermore, it shows how actors' strategic behaviours determine policy outcomes. This is an important development vis-à-vis behaviouralism since they only highlighted structural variables (i.e. socioeconomic development or material discontent) to explain policy outcomes.[128]

RCI is marked by three characteristics which are relevant for this thesis. First of all, RCI employs a set of behavioural assumptions, including that relevant actors (i) have a stable set of preferences or tastes, (ii) behave instrumentally in order to achieve their preferences and (iii) behave strategically presupposing a high level of calculation.[129] In regard to point (i) it has been argued that preferences are formed via a 'two-level game' where Member States define their national policy preferences that are subsequently translated into strategies on an international level.[130] However, these strategies are not exclusively based on national preferences but factor in lack of

[123] Mahoney, J. & Thelen, K. (2010) A Theory of Gradual Institutional Change. In: Mahoney, J. & Thelen, K. (eds.) *Explaining Institutional Change: Ambiguity, Agency, and Power*. Cambridge University Press, p. 8.
[124] Ibid, p. 11.
[125] See for instance: Weingast, B. and Marshall, W. (1988) The Industrial Organization of Congress, *Journal of Political Economy*, vol. 96 (1), pp. 132–163.
[126] For early literature, see for instance: Tsebelis G. (1994) The power of the European Parliament as a conditional agenda setter. *American Political Science Review*, vol. 88, pp. 129–42; or: Tsebelis et al. (2001) Legislative procedures in the European Union: An empirical analysis. *British Journal of Political Science*, vol. 31, pp. 573–99.
[127] Hall, P. A. & Taylor, R. (1996), op. cit., p. 18
[128] ibid.
[129] Hall, P. A. & Taylor, R. (1996), op. cit., p. 12. See also: Shepsle, K. &Weingast, B. (1987) The Institutional Foundations of Committee Power, *American Political Science Review,* vol. 81 pp. 85–104.
[130] Wolff, S. (2012), op. cit., p. 29.

information about other actors as well as other considerations such as political feasibility.[131] An example illustrating this point is the behaviour of the British Presidency during the DRD negotiations. While preferring a framework decision as the legal instrument it agreed to a Directive in order to avoid a legal challenge triggered by the European Commission.[132]

Second, RCI regards politics as a 'series of collective action dilemmas'. More specifically, since actors strive to attain their own preferences, policy outcomes are mostly collectively suboptimal (i.e. another outcome could have been achieved that would have at least made one actor better off without making any of the others worse off). What usually prevents actors from agreeing on collectively-superior outcomes is the lack of institutional arrangements that ensures complementary behaviour of others. Often used examples of this situation are the 'prisoner's dilemma' or the 'tragedy of the commons'.[133] Examples for sub-optimal outcomes are the early versions of the SWIFT and PNR agreements. In both cases, the agreements reflect the difficulty of the parties to find a compromise leading to texts which do not provide sufficient legal certainty. In this way, the agreements did not satisfy the needs of either party.[134]

Third, RCI stresses the strategic interaction in the determination of political outcomes. This involves the belief that actor's behaviour is driven by strategic calculus and that this calculus factors in assumptions of how other actors behave. Respectively, institutions structure this strategic interaction between actors "(…) by affecting the range and sequence of alternatives on the choice agenda or by providing information and enforcement mechanisms that reduce uncertainty about the corresponding behaviour of others and allow 'gains from exchange', thereby leading actors towards particular calculations and potentially better social outcomes."[135] An example of strategic behaviour is the EP's decision to not agree to the SWIFT Agreement which has widely been regarded as turning point revealing the importance and power of the EP.

---

[131] ibid.
[132] See Chapter 4, section 2 of this thesis.
[133] Hall, P. A. & Taylor, R. (1996), op. cit., p. 12. See also: Ostrom, E. (1990). *Governing the Commons*. Cambridge University Press.
[134] For example, in the early version of the PNR Agreement it was not clear how the review of the Agreement has to be carried out leading to uncertainties in regard to the review procedures.
[135] Hall, P. A. & Taylor, R. (1996), op. cit.,p. 12.

2.4 Sociological Institutionalism (SI)

Similarly to RCI, Sociological Institutionalism (SI) is mainly concerned with assessing the relations between actors and between actors and institutions. It developed as a subfield of organisation theory and as a response to the Weber-based idea that institutions are the product of the aspiration to establish efficient structures that perform tasks associated with modern society. In contrast to the latter idea, SI seeks to explain institutions via culture. SI is marked by two main characteristics. First, SI theory tends to define institutions in a broader way than RCI or HI blurring the boundary between institution and culture. Accordingly, institutions include formal rules, procedures as well as 'symbol systems, cognitive scripts, and moral templates' providing the 'frames of meaning' that guide human action.[136] Second, SI has a distinct view on the relationship between institutions and actors. An older approach regarded the institutional impact on actors by applying the normative lens. Respectively, institutions are seen as 'roles' enshrining 'norms of behaviour' while the actors who are socialised into those roles internalise the enshrined norms of behaviour. A more recent approach interprets the interaction between institutions and actors through the cognitive lens. The latter approach claims that institutions influence behaviour by providing 'cognitive scripts, categories and models' which are necessary to interpret the policy context and the behaviour of other actors.[137] Ultimately, self-images and identities of social actors are based on templates provided by institutions. According to SI, this cultural approach does not mean that actors are not able to act rationally. However, the action that the actor perceives to be rational is in itself socially constituted.[138] It is difficult to gather evidence for SI and it is often used in circumstances where RCI fails to explain an actor's behaviour. For example, when the EP challenged the PNR Agreement in front of the CJEU it argued that the Agreement was wrongly based on a first pillar basis. Since the Court accepted this argument, the EP effectively excluded itself from the subsequent policy-making

[136] Hall, P. A. & Taylor, R. (1996), op. cit.,p. 14. See also: Campbell, J. (1995) *Institutional Analysis and the Role of Ideas in Political Economy.* Paper at Harvard University; Scott, W. R. (1994) Institutions and Organizations: Towards a Theoretical Synthesis. In: Scott, W.R. & Meyer, J. et al. (1994) *Institutional Environments and Organizations: Structural Complexity and Individualism*, Sage, pp. 55–80.
[137] Hall, P. A. & Taylor, R. (1996), op. cit.,p. 15.
[138] p. 16.

procedure. It has been argued that the moral aspirations of the EP trumped its strategic preferences.[139]

2.5 Limitations of New Institutionalism and the need for a holistic approach

While providing interesting views on institutions, actors and ultimately policy outcomes, institutionalism is subject to certain limitations. In regard to all three branches the most prominent limitation refers to its conceptualisation of institutional formation and change. Respectively, it has been argued that "[t]he need to appeal to two kinds of explanation, one for continuity and another for change, violates a rule of theoretical parsimony."[140] As a result, most efforts of institutionalist theorists were devoted to the analysis of change and persistence of institutions. This main challenge also triggered the suggestion to add a new form of institutionalism - discursive institutionalism- which focuses on the role of ideas and discourse in politics and in this way seems to provide a more dynamic approach to institutional change than the older three new institutionalisms.[141] Turning to the limitations of the individual branches of institutionalism several comments can be made. First of all, by predominately focusing on institutions themselves HI does not sufficiently emphasise the relationship between institutions and actors. More specifically, HI has devoted less time to determine a precise causal chain through which the institutions affect the actor's behaviour.[142] In contrast, RCI provides a precise conception of the interaction between institutional actors and behaviour as well as a general set of concepts. Nevertheless, it has been argued that RCI conveys a rather simplistic image of human motivation that misses important dimensions that have been relevant to inform preference formation.[143] Furthermore, RCI's purely functionalist view of institutions does not explain the inefficiencies that often occur in institutions. Ultimately, SI can be regarded as filling the gap of RCI whenever a situation cannot purely be explained by rationale and strategy. The validity of this overarching SI argument has been exemplified with the instance where humans would stop at a red traffic light even if

[139] For an assessment of this argument, see Chapter 6 (section 2.2) of this thesis.
[140] Reyners, J (2015), op. cit.
[141] For more details, see for example: Schmidt, V. A. (2008) op. cit.
[142] Hall, P. A. & Taylor, R. (1996), op. cit., p. 17.
[143] See for instance: Cook, K. S. and Levi, M. (1990). *The Limits of Rationality*. University of Chicago Press. See also: Mansbridge, J. (1990). *Beyond Self-Interest*. University of Chicago Press.

there were no car in sight.[144] However, SI can be criticised for not having a satisfactory explanation for why certain norms emerge in the first place and why they prevail over others. Furthermore, also from a methodological perspective, it is difficult to prove that actors' behaviour are norm-driven especially since SI stresses subconscious norm-internalisation.

A way to mitigate the limitations of each branch of institutionalism is to acknowledge their complementarity instead of regarding them as mutually exclusive. Respectively, there is a need for the interaction between the three branches since "(…) each of these literatures seems to reveal different and genuine dimensions of human behavior and of the effects institutions can have on behavior. None of these literatures appears to be wrong-headed or substantially untrue. More often, each seems to be providing a partial account of the forces at work in a given situation or capturing different dimensions of the human action and institutional impact present there."[145] Thus, the different branches of institutionalism are not mutually exclusive. Applied to this thesis, HI helps to gain a 'macro-level' understanding of all three cases studies by assessing how the institutional framework entraps all three regimes. In contrast, SI and RCI are used to assess the 'micro-level' by assessing how actors deal with the transformative institutional framework.[146] While the behaviours of actors often reflect RCI assumptions, normative aspirations should not be completely ruled out. Adopting a holistic approach to the analysis by acknowledging the vivid interplay of all three branches helps to overcome the drawbacks of each single approach and thus makes the analysis more solid.

2.6 Hypotheses

Having explained the background of NI, in the following three hypotheses will be presented which seek to answer the overarching research question of how the EU institutional framework shapes data protection and privacy in regard to data retention and access measures for public security purposes. Taken together the three hypotheses reflect that particularly HI and RCI assumptions of institutionalism are prevalent.

---

[144] Hall, P. A. & Taylor, R. (1996), op. cit., p. 18.
[145] Ibid., p. 22
[146] Accordingly, Katznelson & Weingeist have argued that HI supports 'macroanalysis' while RCI supports the 'microanalysis'. See: Katznelson, P. & Weingeist , B. (2005) *Preferences and Situations. Points of Intersection Between Historical and Rational Choice Institutionalism*. Russell Sage Foundation.

2.6.1 Hypothesis 1: 'Privacy and Data Protection in AFSJ' is an institutional framework in transition implying that both established as well as new institutional features co-exist and commonly determine how data protection and privacy is shaped in relation to public security.

Hypothesis 1 argues that 'Privacy and Data Protection in AFSJ' is an institutional framework in transition implying that old and new features coexist. This transitional nature can be ascribed both to external factors such as terror events and technological developments as well as internal factors mainly the changes through Lisbon and the adoption of CFREU. On the one hand, major changes to privacy and data protection in AFSJ are: the only recent constitutionalisation[147] of data protection, the increasing role of the CJEU due to the adoption of CFREU, the recent adoption of the new data protection package and the adoption of more 'privacy-friendly' international agreements with the US. On the other hand, features of old paths can still be detected. For example, although CFREU includes a right to data protection, this has not yet been fully acknowledged due to CJEU's path-dependence to ECtHR jurisprudence. Furthermore, although new EU data protection legislation emerged 'old features' still live on.

HI theorists have explained that the development of AFSJ in general has been a cumbersome process whereas policies evolved gradually through a pluralistic and highly conflictual process into a 'normalised' policy area.[148] While there were initial struggles and relapses, the overall trend to harmonisation reveals an incremental movement towards a new path.[149] In the case of the research at hand, certain events like terror attacks, technological development, the Snowden revelations and the Lisbon Treaty have led to critical junctures leading to incremental policy change whereas stickiness to pre-defined habits prevents the move onto a new path. Accordingly, HI helps to understand the overall institutional context in which all three data retention and access regimes emerged. Furthermore, it also allows making

[147] In the following, the term 'constitutionalisation' is primarily understood as the formal inclusion of data protection in CFREU. However, in the long term this also has broader implications in a sense that all governmental action in respect to data protection will be determined by the structures, processes and values of 'a constitution'. See: Loughlin, M. (2010). What is Constitutionalisation? In: Dobner, P. and Loughlin. M. (eds.) *The Twilight of Constitutionalism?* Oxford University Press, pp. 47-72.
[148] Hayes, M. (2001). *The Limits of Policy Change: Incrementalism, World View and the Rule of Law*. Washington, Georgetown University Press.
[149] Wolff, S. (2012), op. cit., p. 32. See also: Lindblom, C. (1959). The Science of Muddling Through. *Public Administration Review*, vol. 19 (2), pp. 79-88.

predictions about a potentially more stable setting in the future where standards on data protection and privacy are more clear in respect to the competences, applicable regimes and the nature and extent of relevant safeguards.

2.6.2 Hypothesis 2: The EU institutional framework enables EU legislative actors to pursue strategic preferences in the legislation-making process and thereby influences the way privacy and data protection is shaped in the public security context.

When data retention and access regimes emerged in the pre-Lisbon Treaty, the pillar structure led to a two-tier system of legislative competences where both Council and EP shared legislative powers under the first pillar and where EP influence was limited under the third pillar. At the same time however, the boundary between the pillars was not always clear-cut offering policy-makers the opportunity to advocate for the legal basis granting them more influence. The concept of cross-pillarisation has been discussed in the Justice and Home Affairs field[150] and refers to the complexity of AFSJ measures and the corresponding questions it raises about what constitutes an appropriate legal basis and what are the adequate decision-making procedures. It indicates the blurriness of the EU pillar structure since policies, actors and processes transcend the artificial borders between the pillars. This blurriness is evident in the behaviour of policy actors as well as CJEU rulings. In regard to the former, evaluations of annual policy statistics within the AFSJ field revealed that instead of systematically preferring intergovernmental non-binding instruments in the third pillar, national delegations in the Council are willing to disregard the pillar boundaries and adopt binding instruments according to their appropriateness.[151] In regard to the CJEU, there are certain cases where the Court explicitly upholds the pillar structure,

[150] See for instance: Bendiek, A. (2006). Cross-pillar security regime building in the European Union: Effects of the European Security Strategy of December 2003. *European Integration Online Papers*; Cremona, M. (2006). External relations of the EU and the member states: Competence, mixed agreements, international responsibility, and effects of international law. *EUI Working Papers Law No. 2006/22*; Stetter, S. (2004). Cross-pillar politics: functional unity and institutional fragmentation of EU foreign policies. *Journal of European Public Policy,* vo.11 (4), pp. 720–39; Trauner, F. (2005). *External aspects of internal security: A research agenda*. EU-Consent Project.

[151] Monar, J. (2010a). The Institutional Dimension of the AFSJ. In: Monar, J. (ed.). *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice*. College of Europe Studies, Peter Lang. See also: Monar, J. (2006). Specific factors, typology and development trends of modes of governance in the EU Justice and Home Affairs domain. *NEWGOV Working Paper*, *No. 1/D17*, European University Institute, Florence, 2006, pp. 17-18.

indirectly advanced the destruction of the artificial boundary, or locates policy areas within the pillar structure.[152]

According to Hypothesis 2, pre-Lisbon policy actors framed the policy objectives of data retention and access regimes to match their strategic preferences. While pursuing strategic preferences –mainly in regard to the legal basis- legislators influenced the way privacy and data protection is shaped in the public security context. For instance, the legal basis determines not only the competences of different actors in the legislation-making procedure but also which data protection framework applies in the context of the measure. Notably before 2008 no legal measure on data protection in the third pillar existed which had an impact on the level of protection granted to data subjects.

After Lisbon the ordinary legislation-making procedure became the relevant venue to influence policy outcomes since the abolition of the pillar structure implied that competences of different actors are distributed evenly across all policy fields. In the first instance the ordinary legislation-making procedure is a positive development since the EP has significant new powers and its views, which were originally often different from the Council, are now directly relevant in the legislation-making procedure. Thus, the Council deliberations should right from the beginning be marked by the need to come to an agreement with the Parliament. Thus, the main aspirations of the EP -traditionally the promotion of fundamental rights- can no longer be ignored by the Council.[153] According to Hypothesis 2, however, it can be observed that after becoming a co-legislator, the European Parliament is increasingly willing to compromise in order to reach an agreement during the first reading. If an agreement is reached already during the first reading a 'fast track' procedure was chosen.[154] Statistics reveal that first reading agreements were reached in a majority of AFSJ acts.[155] In the case studies scrutinised in this thesis, it can be observed that the EP has reached earlier conclusions and compromised its stance significantly in comparison to its previously strong views on data protection and privacy. This can for example be linked to the notion of 'sensitivity of failure' where a compromised policy outcome is

[152] See Hypothesis 3 below.
[153] De Capitani, E. (2010) The Evolving Role of the European Parliament in AFSJ. In: Monar, J. (ed.). *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice*. College of Europe Studies, Peter Lang.
[154] The 'fast-track' procedure is explained in greater detail in: Shackleton, M. (2000). The Politics of Co-decision. *Journal of Common Market Studies*, vol. 38, pp. 325-432.
[155] ibid, p. 540.

preferred over no policy outcome due to among others the integrationist preference of the EP. This explains why post-Lisbon expectations in respect to more solid safeguards on data protection and privacy were not always met.

2.6.3 Hypothesis 3: The transitional nature of the EU institutional framework contributed to the CJEU's evolution from a 'legal basis arbiter' to a political actor in its own right that increasingly determines substantial aspects relating to privacy and data protection in the public security context.

For many years, scholars have been debating the role and influence of the CJEU and its jurisprudence beyond its direct impact on a law under scrutiny in a specific case.[156] More specifically it has been analysed how and under which circumstances judgments influence political outcomes in more general terms and whether one can thus regard the CJEU partially as political actor.[157] In this thesis, the terms 'political actorness' or 'political actor' are thus not used to imply that judgments are politically motivated. Instead they are used to assess the CJEU's influence on policy outputs beyond the influence on the specific case at hand. In other words, political actorness assesses the extent and the conditions under which CJEU-generated principles, reasoning and interpretations impact the range of policy options, political agendas, and policy outputs.[158] It has to be noted that this analysis is value-neutral since it will not be assessed whether this influence is intentional and whether it is positive or negative. Instead political actorness is regarded from the point of view of the CJEU as an institutional actor where institutional parameters (such as the competences granted to the court) as well as the overall strife for legitimacy and rule of law drive the degree of influence. The debate on the extent of political actorness has developed between 'dynamic' and 'constrained' views of the judiciary. While the former camp claims that courts are powerful political actors in many contemporary democracies, the latter

[156] See for instance: Epp, C.R. (1998) *The Rights Revolution: Lawyers, Activists, and Supreme Courts in Comparative Perspective*. University of Chicago Press; McCann, M. (1994) *Rights at Work: Pay Equity, Reform and the Politics of Legal Mobilization*, University of Chicago Press; Rosenberg, G.N. (2008) *The Hollow Hope: Can Courts Bring About Social Change?* University of Chicago Press; Stone Sweet, A. (2000) *Governing with Judges: Constitutional Politics in Europe*, Oxford University Press.
[157] Dawson, M., De Witte, B. and Muir, E. (2013) *Judicial Activism at the European Court of Justice*. Edward Elgar.
[158] See: Martinsen, D. (2015) *An Ever More Powerful Court? The Political Constraints of Legal Integration in the European Union*, Oxford Scholarship Online, p. 7-8.

camp argues that the societal impact of courts is limited and dependent on a large set of institutional, political, and cultural factors.[159]

In regard to the constraint view, it has been argued that proponents of a high degree of political actorness of the CJEU often overlook the fact that on many occasions the CJEU has been ignored or constrained by both political and administrative counteractions.[160] For example, adherents to the restrained view do not unconditionally regard the CJEU as motor of EU integration. Instead it is argued that the CJEU is aware that its decisions do not automatically lead to compliance by EU Member States. It can be assumed that the CJEU wants to avoid non-compliance since it encroaches on its own authority. Therefore, CJEU decisions are influenced by the risk of non-compliance of the litigant government.[161] By turning the focus towards the way politics shapes court decisions instead of vice versa, adherents to the constraint view thus argue that the CJEU cannot uncritically be regarded as actor influencing policy outcomes. It is misleading and overlooks the highly complex interplay of law and politics.[162]

More commonly scholars do however acknowledge a certain degree of political actorness of the CJEU. According to the dynamic view, the CJEU has often been regarded as a 'master of integration' due to its capacity to strengthen integration at EU level - occasionally even against the willingness of the Member States.[163] In

[159] For a more detailed overview and relevant literature, see: Martinsen, D. (2015) op. cit., chapters 1 and 2.
[160] See for instance: Conant, L.J. (2002). *Justice Contained, Law and Politics in the European Union*, Cornell University Press. Larsson, O. and Naurin, D. (2016). Judicial independence and political uncertainty: How the risk of override impacts on the Court of Justice of the EU. *International Organization*, vol. 70 (2), pp. 377-408; Nowak, T. (2010). Of garbage cans and rulings: judgments of the European Court of Justice in the EU legislative process, *West European Politics*, vol. 33(4), pp. 753-69; Rasmussen, M. (2013) Rewriting the history of European public law: the new contribution of historians. *American University International Law Review*, vol. 28 (5), pp. 1187-223.
[161] See: Carruba, C. J., Gabel, M. and Hankla, C. (2008). Judicial behavior under political constraints: evidence from the European Court of Justice. *The American Political Science Review,* vol. 102 (04), pp. 435-54. See also: Carruba, C. J., Gabel, M. and Hankla, C. (2012). Understanding the Role of the European Court of Justice in European Integration. *The American Political Science Review*, vol. 106 (1), pp. 214-223.
[162] See for instance: Armstrong, K.A. (1998) Legal Integration: theorizing the legal dimension of European Integration, *Journal of Common Market Studies*, vol. 36 (2), pp. 155-74.
[163] See, for example: Alter, K. (1998) Who are the 'Masters of the Treaty'? European governments and the European Court of Justice. *International Organization*, vol. 52 (1), pp. 121-47; Alter, K. (2001) *Establishing the Supremacy of European Law: The Making of an International Rule of Law in Europe.* Oxford University Press; Alter, K. (2009) The European Court's political power across time and space, *Revue Francaise de Science Politique*, vol. 59, pp. 1-24. Burley, A.M. and Mattli, W. (1993) Europe before the Court: a political theory of legal integration. *International Organization*, vol. 47 (1), pp. 41-76. Höpner, M. and Schäfer, A. (2012) Embeddedness and regional integration: waiting for Polanyi in a Hayekian setting, *International Organization*, vol. 66 (3), pp. 429-55; Pollack, M.A. (2003) *The Engines of European Integration, Delegation, Agency and Agenda Setting in the EU*. Oxford

more specific terms, the CJEU has often been 'accused' of political actorness in regard to fundamental rights for two reasons. On the one hand, the CJEU created the pre-conditions for enhancing its political reach in regard to fundamental rights in the founding years of the EU. While initially the ECSC or EEC Treaties did not stipulate the need for Community institutions to respect fundamental rights, the CJEU incrementally started to stress the constitutional importance of fundamental rights in the EU legal order against the original will of the Treaty makers.[164] More specifically, the CJEU established the principle of supremacy in 1960 implying that Community acts prevail over national law, including national constitutional law. A logical conclusion of this CJEU principle is that judicial review can only be based on Community law itself.[165] In this way, the Court shaped its institutional profile by confirming its position as a guardian of the 'constitutionality' of EU acts. Furthermore, the Court not only positioned itself within the EU legal order, it also asserted its centrality in a legal order marked by interactions with Member States, Third States and International Organizations."[166] This became evident with two CJEU opinions rejecting the EU's accession to the ECHR.[167] On the other hand, three more recent institutional developments facilitated political actorness of the CJEU in regard to fundamental rights: (i) A stronger 'constitutional' mandate was granted to the CJEU with the entry into force of Lisbon; (ii) the adoption of CFREU and thus the codification of the rights to be protected provided more coherence when adjudicating on fundamental rights; and (iii) a general trend of politicization of fundamental rights at EU level led to increased discussions on fundamental rights among legislators and thus put CJEU jurisprudence in the centre of political debates.[168]

Under Hypothesis 3 a dynamic view of the CJEU is expected where the CJEU exhibits features of political actorness whilst shaping privacy and data protection in the public security context. However the type of 'political actorness' changed over

---

University Press; Stone Sweet, A. and Brunell, T. (2012). The European Court of Justice, state non-compliance, and the politics of override. *American Political Science Review,* vol. 106 (1), pp. 204-13; Weiler, J. (1991) The Transformation of Europe, *Yale Law Journal*, 100, pp. 2403-83.

[164] De Burca, G. (2011a) The Evolution of EU Human Rights Law. In Craig, P. and De Burca, G. (eds) *The Evolution of EU Law*. OUP. See also: Alston, P. & Weiler, J.H.H. (1998) An Even Closer Union in Need of a Human Rights Policy, *European Journal of International Law*, vol. 9, pp. 658- 723.

[165] De Witte, B. (1999) The Past and Future Role of the European Court of Justice in the Protection of Human Rights' in Alston, P. (ed) *The EU and Human Rights*. OUP.

[166] Muir, E. (2013). The Court of Justice: a fundamental rights institution among others. In: Dawson, M., De Witte, B. and Muir, E. (eds.) *Judicial Activism at the European Court of Justice*. Edward Elgar

[167] See Chapter 3 of this thesis.

[168] ibid.

time. Traditionally, the CJEU has played a significant role in determining the relationship between the pillars. There are some cases where the Court explicitly upholds the pillar structure. For instance, in the *Kadi* case the Court claimed that the Union and the Community co-exist as integrated but separate legal orders.[169] In other cases the Court indirectly advanced the destruction of the artificial boundary. In the famous *Pupino* case[170] the Court used first pillar Community law principles for a third pillar framework decision resulting in the erosion of the pillar structure.[171] Besides these two extremes, the Court rulings usually place policy areas within the pillar structure when the legal basis of a legal instrument is contested.[172] As explained later in this thesis, these Court clarifications are not always uncontroversial. For instance while the Court argued that the PNR Agreement should be a third pillar measure[173] in the similar case *Ireland v. Parliament and Council*[174] the Court ruled exactly the opposite. Consequently, criticism was expressed in the academic community about the judgment as such and on the lack of the Court's consistency.[175] The cases mentioned above arguably[176] reveal the lack of consistency and the weak and artificial boundary between the pillars.[177] However, above all this shows that the pillar structure was an important institutional feature for the CJEU to play an active role in determining the nature of legislative instruments and the allocation of powers between the EP, the Commission and the Council.

Post-Lisbon the pillar structure was abolished implying that the CJEU's role as 'legal basis arbiter' ceased to exist. However, this did not diminish the importance

[169] Case T-315/01 *Yassin Abdullah Kadi v Council of the European Union and European Commission* of 21 September 2005, para. 120.
[170] Case C-105/03 *Pupino* of 16 June 2005.
[171] Monar, J. (2010a). op. cit.
[172] See for example: Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission* of 30 May 2006; C-440/05 *Commission v Council* of 23 October 2007; Joined cases C-187/01 and C-385/01 *Gözütok and Brügge* of 11 February 2003; Case C-176/03 *Commission v Council* of 13 September 2005; Case T-228/02 *Modjahedines* of 12 December 2006. For an analysis of the relevant case law see: Hatzopoulos, V. (2008). With or without you...Judging politically in the area of freedom, security and justice", *European Law Review*, vol. 33 (1), pp. 44-65.
[173] Joined Cases C-317/04 and C-318/04, *European Parliament v Council and Commission* of 30 May 2006.
[174] Case C-301/06, *Ireland v. Parliament and Council*, judgment of 10 February 2006, para. 83.
[175] Simitis, S. (2009) Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung. *Neue Juristische Wochenzeitschrift 25*, pp. 1782-1786; Hijmans, H. & Scirocco, A. (2009) Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help? *Common Market Law Review*, vol. 46 (5), pp. 1485–1525.
[176] Other academics claim that the interpretation is not inconsistent (e.g. Böhm, F. (2011). *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*. Springer, p. 112-113).
[177] On the matter of consistency between the pillars, see Chapter 4 (section 2.2.2) of in this thesis.

of the CJEU. Instead, the simultaneous adoption of the Charter provided the CJEU with the means to adjudicate on substantial instead of procedural matters in relation to privacy and data protection and thereby to increasingly exhibit features of 'political actorness'. Recently the CJEU has delivered judgments that have two effects. On the one hand, they have implications for the legality of a particular data retention and access regime. On the other hand, they directly shape future legislative initiatives since legislators will factor in existing case law and anticipate future CJEU rulings. To analyse the CJEU's political actorness, the thesis will first analyse the legality of the three regimes in the case study chapters in light of the framework established in Chapter 3.[178] Subsequently it will be assessed whether and to which extent the CJEU reveals political actorness in respect to each regime.

Conclusion

The aim of this chapter was to provide an overview of the theoretical framework applied to assess the factors that influence how privacy and data protection is shaped in the public security context. The first part of the chapter provided an overview of 'European Integration Theory' which is an umbrella term combining different approaches to analyse EU policy. Several approaches have been presented (i.e. intergovernmentalism, neofunctionalism, the governance approach, policy networks analysis and constructivism). It has been illustrated that in regard to all of these approaches there are some reservations regarding their use to assess policy outcomes and thus to analyse how privacy and data protection is shaped in the public security context. While intergovernmentalism and neofunctionalism is mainly concerned with assessing Member States' interests regarding European integration, all the other approaches focus mainly on governance processes instead of concentrating on policy outcomes. It has thus been claimed that NI is better suited than the afore-mentioned approaches to assess data retention and access regimes since it offers tools to understand what mechanisms drive certain modes of governance as well as policy outcomes.

Subsequently, the chapter provided an overview of the main features of NI and how it is relevant for the thesis. First, it has been shown that NI emerged as a reaction to behaviouralism which argues that social forces and individual decisions are the

[178] Chapter 3 (section 3) in this thesis.

only factors determining policy outcomes. Second, key notions of NI have been explained. More specifically, it has been explained that 'actors' are the EU legislators namely the Council, the Commission and the EP and the CJEU. Further, the terms 'institution' or 'institutional framework' are considered to be the 'operating framework' for any actions taken by institutional actors. Since there is not one widely accepted definition of 'institution', the thesis adopts its own version by focusing on the 'formal' institutional aspects. In practical terms it thus refers to the constitutional and legal framework that structures legislation-making when privacy and data protection for public security purposes is at stake. Additionally, the notion of preference has been clarified by mentioning that the thesis focuses on strategic rather than fundamental preferences.

Third, the chapter provided an overview of the different branches of institutionalism. It has been shown that HI mainly emphasises the role of institutions and how they evolve over time. The main aim of HI is to assess why institutions persist over time and what triggers institutional change. Subsequently, RCI was presented as a branch of NI which focuses on scrutinising the interaction between institutions and the actors operating within these institutions. According to RCI, actors' strategic behaviours determine policy outcomes. Ultimately, SI assesses the relation between actors and institutions but focuses on cultural aspects and norms which drive the behaviour of actors.

In the last part of the chapter, three hypotheses -reflecting RCI and HI approaches- were presented as key factors shaping privacy and data protection in the public security context: (i) privacy and data protection in AFSJ' is an institution in transition; (ii) EU legislative actors pursue strategic preferences in the legislation-making process; (iii) CJEU evolved from a 'legal basis arbiter' to a political actor in its own right. This chapter is important because the three core hypotheses that intend to answer the core research question are based on NI notions. More specifically, Hypothesis 1 is based on HI elaborations of institutional persistency and change. Furthermore, Hypotheses 2 and 3 represent notions of RCI and HI where the strategic preference to maximise influence on policy outcomes as well as the empowerment through institutional change determines the actions of institutional actors. Thus, the analysis in the subsequent chapters will be based on NI accounts.

CHAPTER 3 – PRIVACY AND DATA PROTECTION IN THE 'AREA OF FREEDOM SECURITY AND JUSTICE': AN INSTITUTIONAL FRAMEWORK IN TRANSITION

Introduction

The relevant institutional framework for the purposes of this thesis is the legal and constitutional framework regulating privacy and data protection in the EU 'Area of Freedom, Security and Justice' (AFSJ). This is because all three case studies analysed in this thesis are concerned with the fight against terrorism and serious crime in order to safeguard public security while minding privacy and data protection. The purpose of this chapter is to assess this institutional framework in light of Hypothesis 1 from a historical institutionalist perspective.[179] It is claimed that the institutional framework is an example of *incremental transformation* where both constitutional and policy levels exhibit features of 'old paths' while at the same time new paradigms evolve. Turning points or so-called '*critical junctures'* and institution-internal uncertainty have led to the dynamic nature of the institutional framework. Most prominently the Lisbon Treaty and the adoption of CFREU have triggered the transformation. In addition, also events such as major terror attacks and the Snowden revelations as well as subtle processes such as the increasing use of technology for public security purposes lead to the flexibility of the institutional framework. Acknowledging the dynamic nature of privacy and data protection in AFSJ is important for the case study chapters as it determines the behaviours of institutional actors and thus the way privacy and data protection is shaped in the public security context. This chapter also provides a framework guiding the legal analysis of the DRD, the PNR and SWIFT Agreements.

First, an overview of the concepts of privacy and data protection as fundamental rights in the EU legal order and their correlation is provided. Privacy and data protection are complex fundamental rights which are not easy to define and to

[179] For a holistic analysis of AFSJ, see for example for pre-Lisbon accounts: Walker, N. (2004) *Europe's Area of Freedom, Security and Justice*. Oxford University Press; Mitsilegas, V. (2008) *EU Criminal Law.* Hart Publishing. For a post-Lisbon analysis, see: Eckes, C. & Konstadinides, T. (eds.) (2011) *Crime within the Area of Freedom, Security and Justice*. Cambridge University Press; Wolff, S., Goudappel, F. and De Zwaan, J. W. (2011) *Freedom, Security and Justice After Lisbon and Stockholm*. T.M.C. Asser Press; Mitsilegas, V. (2016) *EU Criminal Law after Lisbon. Rights, Trust and The Transformation of Justice in Europe*. Hart Publishing.

apply. Furthermore, the correlation of the two rights and the added value of data protection are marked by intricacies. This analysis is followed by an assessment of CJEU and ECtHR case law on data protection and privacy in the public security context. This provides a framework to analyse to what extent case law is applicable to the DRD, PNR and SWIFT Agreements.

Second, the emergence and current state of privacy and data protection in AFSJ as laid down by the Treaties and secondary legislation is presented. AFSJ is a complex policy field since it covers a broad array of sensitive topics ranging from subjects such as migration to criminal law and policing. Respectively, it has been argued that "unlike many major domains in European law (…) subject matters assembled under AFSJ do not form a "natural" unity in terms of a clearly defined overall project."[180] Instead it seems to be rather a 'network of articulated policies'[181] or a 'policy universe'.[182] This lack of unity implies that also privacy and data protection are not addressed in a uniform manner across AFSJ. On a procedural level many inconsistencies existed pre-Lisbon. Since AFSJ matters are at the 'heart of national sovereignty'[183] Member States traditionally aim to reduce the influence of EU institutional actors which has however become unavoidable throughout the years. This dichotomy led to complex legislation-making rules marked by exceptions and non-transparency. The latter assessment helps to contextualise the emergence of the DRD, the PNR and SWIFT Agreements and is important to understand the behaviours of institutional actors when the three regimes were formed.

Third, the external dimension of AFSJ is assessed. It is shown that external relations before Lisbon were –similarly to internal AFSJ arrangements- complex and marked by inconsistencies. This partially changed after the Lisbon Treaty where three main aspects contributed to the emergence of the EU as a stronger negotiator in EU-US relations. This analysis is mainly relevant for the PNR and SWIFT regimes elaborated in chapters 5 and 6 by providing an understanding about external relations procedures and competences.

---

[180] Walker, N. (2011) In Search of the Area of Freedom, Security and Justice: A Constitutional Odyssey. In: Walker, N. (ed.) *Europe's Area of Freedom Security and Justice*. Academy of European Law/European University Institute, p. 5.
[181] Trauner, F. & Carrapico, H. (2012) The External Dimension of EU Justice and Home Affairs after the Lisbon Treaty: Analysing the Dynamics of Expansion and Diversification'. *European Foreign Affairs Review*, vol.17, pp. 1–18.
[182] Smith, K. (2009) The Justice and Home Affairs Policy Universe: Some Directions for Further Research, *Journal of European Integration,* vol. 31 (1), pp. 1–7.
[183] Peers, S. (2012) *EU Justice and Home Affairs Law*, Oxford University Press, p. vii.

1. The rights to privacy and data protection as fundamental rights

1.1 The right to private life

The right to private life is recognised as a human right in universal, regional and national fundamental rights legislation.[184] In Europe, privacy is enshrined in Article 8 of the European Convention of Human Rights (ECHR):[185]

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Privacy is not an absolute right and interference is permissible if necessary in a democratic society for interests such as national security or for the prevention of disorder or crime. The generic notion of safeguarding 'public security' through prevention of disorder or crime is not only a legitimate ground to limit Article 8 (1) ECHR but it is also arguably stipulated as a fundamental right in the ECHR. Respectively, Article 5 ECHR stipulates that "[e]veryone has the right to liberty and security of person."[186] However, in this thesis 'public security' is treated as an exception of Article 8 (2) ECHR instead of its function under Article 5 ECHR.[187]

While the ECHR is the oldest European initiative stipulating the right to privacy, the Charter of Fundamental Rights of the European Union (CFREU) replicates Article 8 (1) ECHR in Article 7 CFREU which became legally binding with the entry into force of the Lisbon Treaty in 2009. Interestingly, CFREU differentiates between privacy in Article 7 ("Everyone has the right to respect for his or her private and family life, home and communications") and data protection in Article 8. The rationale behind the differentiation and the relation between privacy and data protection will be elaborated in detail in subsequent sections of this chapter. Both Article 7 and Article 8 CFREU do not directly entail any limitations, as it is the case with the ECHR. Instead Article 52 (1) CFREU mentions that

[184] For instance: Article 7, CFREU; Article 8, ECHR; Article 17, International Covenant on Civil and Political Rights (1966); Article 11, American Convention on Human Rights (1969); African Charter on Human and Peoples' Rights (1981), only indirectly included.
[185] Article 8 ECHR.
[186] Article 5 (1) ECHR.
[187] As explained in Chapter 1 of this thesis.

> "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of *general interest* recognised by the Union or the *need to protect the rights and freedoms of others*."[188]

While 'public security' is not explicitly mentioned as a ground justifying the interference with the right to privacy, the CJEU has acknowledged that the fight against terrorism in order to maintain international security constitutes an objective of general interest.[189] Furthermore, the CJEU also stipulated that the fight against serious crime in order to ensure public security constitutes a matter of general interest.[190] In addition, the fact that Article 52 (1) CFREU mentions that rights can be limited to protect the rights of others includes the option that the right to privacy can be limited to safeguard the right to security of person (i.e. public security) stipulated under Article 6 CFREU. However, both the CJEU as well as the thesis at hand regard 'public security' as legitimate ground that limits privacy instead of its function of Article 6 CFREU.

While privacy was originally seen as the 'right to be left alone'[191], subsequently scholars developed multiple conceptualisations leading to the conclusion that privacy is large and unwieldy and "(…) has become as nebulous a concept as 'happiness' or 'security'."[192] This is also reflected in case law since neither CJEU nor ECtHR provide an exhaustive definition of privacy. Instead the ECtHR developed the reach of privacy in a piecemeal fashion by adding certain aspects through case law. In *P G and J H v United Kingdom* the ECtHR expresses itself in the following way:

> Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name and sexual orientation and sexual life are important elements of the personal sphere protected by Article 8 (…). Article 8 also protects a right to identity and personal development, and the right

[188] Article 52 (1) CFREU. Emphasis added by author.
[189] Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission* of 3 September 2008, para. 363, and Cases C-539/10 P and C-550/10 P *Al Aqsa* v *Council* of 15th November 2012, para. 130.
[190] See for instance: C-145/09 *Land Baden-Württemberg v Panagiotis Tsakouridis* of 23 November 2010.
[191] Warren, S. & Brandeis, L, (1890). The Right to Privacy, *Harvard Law Review,* vol. 4(5).
[192] Wacks, R. (2000). *Law, Morality, and the Private Domain*. Hong Kong University Press, p. 222. See also other literature on the conceptualisation of privacy: Bennett, C. (1992) Regulating Privacy: Data Protection and Public Policy in Europe and the United States. *Cornell University Press*; Whitman, J. (2002). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal*, vol. 113; Delany, H. & Carolan, E. (2008) *The Right to Privacy – A Doctrinal and Comparative Analysis*. Thomson Round Hall; Bennett, C. & Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective.* MIT Press.

> to establish and develop relationships with other human beings and the outside world (…). It may include activities of a professional or business nature (…). There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life". [193]

The ECtHR added that the concept of private life expands to a person's picture;[194] and that privacy of individuals also exists in public spaces when videos of events occurring in public are permanently stored. [195] In addition to that, the ECtHR also stressed that privacy includes a person's physical and psychological integrity by ensuring "(…) the development, without outside interference, of the personality of each individual in his relations with other human beings."[196] The ECtHR prefers a broad definition due to the difficulty of defining a one-size-fits-all approach to privacy acknowledging that an adequate definition and level of protection depends on the context and case facts.[197]

When defining privacy, the CJEU either directly refers to ECtHR case law or at least comes to the same conclusions as the ECtHR. The CJEU mentioned on several occasions that Article 7 CFREU "[…] contains rights which correspond to those guaranteed by Article 8(1) of the ECHR and that, in accordance with Article 52(3) of the Charter, Article 7 thereof is thus to be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights."[198] This shows that particularly in regard to conceptual clarifications of privacy, CJEU jurisprudence follows the path laid down by the ECtHR. On other occasions, CJEU case law discusses more specific aspects of privacy by mentioning that a person's name[199], and a person's sexual orientation[200] are a "constituent element

---

[193] *P G and J H v United Kingdom*, Application No. 44787/98 of 25 September 2001, para. 56. See also: *Pretty v. United Kingdom*, Application No. 2346/02 of 29 April 2002, para. 61; *Evans v. United Kingdom*, Application No. 6339/05 of 10 April 2007, para. 71 and *Odièvre v. France* Application No. 42326/98 of 13 February 2003, para. 29.
[194] *Schüssel v. Austria*, Application No. 42409/98 of 21 February 2002, para. 2.
[195] *Peck v United Kingdom,* Application No 44647/98 of 28 January 2003, para. 58.
[196] *Von Hannover v Germany,* Application no. 59320/00 of 24 June 2004, para. 50. See also: Hatzis, N. (2005). Giving Privacy is Due: Private Activities of Public Figures in von Hannover v Germany. *The King's College Law Journal*, vol. 16 (1), pp. 143-157 See also: *P G and J H v United Kingdom*, Application No. 44787/98 of 25 September 2001.
[197] For this argument (however not in relation to privacy): McHarg, A. (1999). Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights. *The Modern Law Review*, vol. 62(5), pp. 671-696.
[198] See: Case C-419/14 *WebMindLicenses Kft* of 17 December 2015, para. 70. See also: C-400/10 *PPU J. McB. v L. E.* of 5 October 2010, para. 53; and C-256/11 *Murat Dereci and Others v Bundesministerium für Inneres* of 15 November 2011, para. 70.
[199] C-208/09 *Ilonka Sayn-Wittgenstein v Landeshauptmann von Wien* of 22 December 2010*,* para. 52. Reference to: *Burghartz v. Switzerland*, Series A No 280-B, p. 28, of 22 February 1994, para. 24; and *Stjerna v. Finland,* Series A No 299-B, p. 60, of 25 November 1994, para. 37.

of his private life" instead of engaging in a more fundamental discussion of privacy. In contrast to the ECtHR, the CJEU also discusses the essence of privacy on some occasions. For instance, in both *Digital Rights Ireland* and *Schrems* the CJEU argues that the knowledge of the content of the electronic communications forms the essence of privacy.[201] The concept of the 'essence of a right' –enshrined in Article 52 (1) CFREU- derives from older CJEU case law holding that the very substance of the rights should never be compromised.[202] The concept's usefulness is limited since the boundary between a right in general and its essence is not always clear-cut.[203] This is also reflected in the CJEU approach since the Court does not generally engage in a detailed discussion on the essence of rights.

The fact that ECtHR as well as CJEU refrain from defining privacy in a narrow way has both negative and positive implications. On the one hand, being a nebulous concept makes privacy vulnerable to criticism that it is merely a conglomerate of other rights. Furthermore, it can be claimed that a lack of a precise definition hinders legal certainty.[204] On the other hand, leaving privacy as a broad concept allows for flexibility. Flexibility of interpretation and scope is for example important to account for the dynamic nature of data-intrusive technology and practices. Moreover, flexibility of the concept helps to compensate for its large rhetorical counterclaims, namely freedom of inquiry, the right to know, freedom of expression and liberty of the press.[205]

1.2 The right to data protection

Article 8 CFREU stipulates that:

> "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.

---

[200] See for instance: Joined Cases C-148/13 to C-150/13 *A and Others v Staatssecretaris van Veiligheid en Justitie* of 2 December 2014, para. 64.
[201] *DRI*, para. 39 and C-362/14 *Maximillian Schrems v Data Protection Commissioner* of 6 October 2015, para. 94.
[202] For example: Case C-5/88 *Hubert Wachauf v Bundesamt für Ernährung und Forstwirtschaft* of 13 July 1989, para. 18; Case C-292/97 *Karlson and others* of 13 April 2000, para. 45.
[203] For instance in *DRI*, content data was regarded as "essence of the right" while traffic and location data was not considered to be the essence of the right. As shown in Chapter 4 (section 3) of this thesis in reality the boundary between traffic and location data is not always clear-cut.
[204] McCullagh, K. (2009). Protecting 'privacy' through control of 'personal' data processing: A flawed approach. *International Review of Law, Computers and Technology*, vol. 23 (1-2), p. 23.
[205] Bygrave, L.A. (2001). The Place of Privacy in Data Protection Law. *UNSW Law Journal*, vol. 24 (1), p. 278.

> 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."[206]

The multitude of aspects included in Article 8 CFREU shows that the right to data protection is a 'cluster right' in a sense that it entails a set of "fair information practices."[207] Its aim is to reconcile conflicting values such as business interests (free flow of information in the internal market), privacy rights (of individuals and businesses) and government interests (data processing for security or taxation purposes).

Data protection is a much more pragmatic and recent concept than privacy. In 1965 "Moore's law" predicted the continuous doubling of density of transistors on integrated circuits every 18-24 months.[208] This prediction was confirmed and within a short period computer power as well as storage capacity and disk information density increased tremendously. This development decreased costs of storing and processing of data and facilitated the growing flow of information.[209] Accordingly in the early 70s, concerns about data privacy emerged leading to the first data protection law being adopted in the German *Land* Hessen which was followed by the enactment of similar laws in other European countries.[210] While national legislation on transborder data exchange reveal the international dimension of data protection, international instruments were only adopted at a later stage.[211] On the EU level, the regulatory efforts intensified during the 1980s and 1990s and culminated in the adoption of the DPD, which has recently been replaced by the General Data Protection Regulation

---

[206] Article 8, CFREU.
[207] The DPD and the GDPR acknowledge at least eight different data protection principles: (1) Data has to be processed fairly and lawfully, (2) data shall be obtained only for specified and lawful purposes, (3) data shall be adequate, relevant and not excessive in relation to the purpose (4) data needs to be accurate and up-to-date, (5) data shall not be kept for longer than necessary, (6) data needs to be processed in accordance with rights of data subjects, (7) data access of unauthorized persons shall be prevented via adequate technical means and (8) when data is transferred outside the EU the third country needs to have adequate data protection standards.
[208] Moore, G. (1965) Cramming more components onto integrated circuits. *Electronics Magazine*, vol. 38 (8). In: Brown, I. (2010). Data protection: the new technical and political environment. *Computers & Law*, vol. 21 (1).
[209] Ibid. See also: Greenleaf, G. (2012). Global data privacy in a networked world. In: Brown, I. (ed) *Research Handbook on Governance of the Internet*. Cheltenham: Edward Elgar.
[210] Hessisches Datenschutzgesetz, 7 October 1970.
[211] Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980 and updated in 2013; Council of Europe (CoE), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981; United Nations (UN) *Guidelines Concerning Computerized Personal Data Files*.

2016/679.[212]

1.2.1 Data protection and the reversed hierarchy of norms

Data protection is an interesting example of a 'reversed hierarchy of norms' as it has been regulated via secondary legislation before it was granted the status of a fundamental right.

When the DPD was adopted in 1995 no constitutional right to data protection existed. Therefore, its legal basis was Article 100a TEC in conjunction with Article 189b TEC relating to the functioning of the internal market. In this way, the main purpose of the directive was to facilitate the free movement of goods, persons, services and capital through the free flow of personal data.[213] With the legal basis on the internal market, the Directive did however stress that the right to privacy as laid down by Article 8 ECHR shall be minded.[214] Even without a tailor-made legal basis further data protection legislation emerged amounting to four crucial instruments.[215] The constitutionalisation of data protection only followed in 2009 with the adoption of the Lisbon Treaty. Article 16 TFEU enshrines that "everyone has the right to the protection of their personal data". In this way data protection enjoys a constitutional status at EU level.[216] Furthermore, CFREU –which became binding in 2009- acknowledges data protection as a stand-alone right in Article 8 CFREU by distinguishing it from the right to private life.

The rationale as to why CFREU introduced retrospectively a separate right to data protection was not extensively discussed in the Charter's explanatory memorandum. [217] The memorandum merely states that Article 8 CFREU is based on Article 286 TEC, the DPD, Article 8 ECHR, and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to

[212] Directive 95/46/EC, op. cit., and Regulation (EU) 2016/679, op. cit.
[213] Recital 3, DPD.
[214] Recitals 3 and 10, DPD.
[215] DPD, Framework Decision 2008/977/JHA, e-privacy Directive, and Regulation (EC) No 45/2001.
[216] This article is not entirely new but based on Article 286 TEC (General and Final Provisions) which was introduced with the Treaty of Nice in 2001.
[217] Anderson, D. & Murphy, C. (2011) The Charter of Fundamental Rights: History and Prospects in Post-Lisbon Europe. *EUI Working Paper LAW 2011/08*, p. 7. Arguably, Article 8 (1) ECHR is divided into three different articles in CFREU, namely the integrity of the person (Article 3), private and family life (Article 7) and data protection (Article 8).

Automatic Processing of Personal Data.[218] Furthermore, the Article 29 WP argued that the constitutionalisation of data protection is a logical step to take since in some Member States the right to data protection is already constitutionalised or has gained this status through case law.[219] Thus, it seems that Article 8 CFREU was mainly a reaction to national and international data protection instruments that had evolved over time. There are three other reasons that could explain the introduction of Article 8 CFREU.

First, De Hert and Gutwirth argue that the aim of introducing Article 8 CFREU was to provide more legitimacy to the EU data protection framework by stressing the fundamental rights dimension of the DPD.[220] This interpretation is plausible because the legal basis of the DPD only accounts for the internal market dimension of the Directive[221] while case law rightly stresses the dual function of ensuring the functioning of the single market and the protection of fundamental rights.[222] By introducing Article 8 CFREU the previously prevailing free movement of data objective of the DPD became more diluted with privacy considerations. However, if the purpose of introducing Article 8 CFREU was indeed to infuse privacy considerations to data protection, it is not clear why the right to privacy was not sufficient to be the appropriate fundamental rights foundation. Furthermore, establishing a retroactive legitimacy for a legislative framework seems intuitively unsatisfactory.[223]

Second, Walden provides a more extensive two-fold explanation for the necessity of constitutionalising data protection. He argues that on the one hand, constitutionalising data protection was necessary from an institutional perspective since the EU was not able to accede to the CoE Regime including its Convention

[218] Draft Charter of Fundamental Rights of the European Union – Text of the explanations relating to the complete text of the Charter as set out in *CHARTE 4487/00 CONVENT 50, CHARTE 4473/00*, 11 October 2000.
[219] Recommendation 4/99 of the Article 29 WP on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights, *5143 /99/EN*, adopted on 7.09.1999.
[220] De Hert and Gutwirth, S. (2009) Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth, S. et al. (eds.) *Reinventing Data Protection?* Springer, p. 5.
[221] Note however that while the legal basis purely focuses on the internal market dimension, Article 1 (1) DPD mentions that its objective is to protect the right to privacy with respect to the processing of personal data.
[222] See: Case C-465/00 *Rechnungshof v Österreichischer Rundfunk and Others* of 20 May 2003.
[223] Lynsky, O. (2015) *The Foundations of EU Data Protection Law*. OUP, p. 92.

108.[224] On the other hand, constitutionalising data protection was necessary from a substantive perspective since the emergence of communication technologies exponentially increased the automatic processing of personal data from both the public and private sectors. Therefore, Article 8 CFREU adds value because: (i) the right is applicable to all data independent of it being of a private or public nature; (ii) the right establishes a general obligation on the person processing personal data. In contrast, traditional privacy law focuses mainly on cases where an individuals' private life is interfered with; (iii) the right to data protection lays down the obligation to establish an independent supervisory authority monitoring compliance with the rules. Particularly the latter two points legitimise data protection as an independent regulatory regime.[225]

Third, the aim of the introduction of Article 8 CFREU was arguably to achieve a spill-over effect. One the one hand, introducing Article 8 CFREU was considered to extend the main elements enshrined in the DPD to data processing under former pillars two and three.[226] Article 29 WP also mentioned that a right to data protection has the potential to trigger harmonised legislation on data protection in pillars two and three.[227] On the other hand, the introduction of Article 8 CFREU ensures the extended reach of EU data protection legislation in international relations. This is because secondary legislation is not binding when international agreements are concluded while the Charter is applicable. Nonetheless, after the abolition of the pillar structure there are still different standards in data protection regarding former pillar one and former pillars two and three.[228] Furthermore, standards of EU instruments differ from those of international agreements.

Since the rationale for constitutionalising data protection was neither clarified by the drafters themselves nor have academic explanations fully resolved the issue, it is not surprising that it was also subject to criticism. For instance, Cuijpers argues that

---

[224] In *Opinion 2/13* of 18 December 2014, the Court came to the same conclusions as in *Opinion 2/94* of 1996, by arguing that the EU could not accede to the ECHR.
[225] Walden, I. (2015) *The right to privacy and its future.* Retrieved 26.04.16 from: https://issuu.com/vpmarketing/docs/synergy_57_online_5e0911c1a89c2a
[226] Rouvoy, A. & Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth, S. et al. (eds.) *Reinventing Data Protection?* Springer, p.71.
[227] The Future of Privacy-Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, *WP168*, 01.12.2009, p. 7. This was restated by: Cannataci, J. & Mifsud-Bonnici, J. (2005). Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty. *Information and Communications Technology Law*, vol. 14 (5).
[228] Lynsky, O. (2015), op. cit., p. 93.

data protection infringements do not necessarily lead to a violation of privacy, hence less fundamental interests are at stake. Therefore, it is questionable "(…) whether it is necessary and even desirable to have mandatory rules of law governing the processing of personal data (…)".[229] This argument does however not account for the fact that protection is expanded to situations where privacy would not apply and in this way data protection effectively extends protection. The next section discusses in further detail the added value of data protection by discussing its relation to privacy.

2. Conceptualising the correlation between the rights to privacy and data protection

Having analysed potential reasons for introducing the right to data protection it is also relevant to assess the correlation of both rights. In the following four different approaches are presented: inherency approach, quasi-separatist approach, instrumentalist approach and assemblage approach.[230] Furthermore, by applying the concept of path-dependence it will be explained why the CJEU has to date settled on the first approach in its case law.

2.1 Inherency approach: data protection as an aspect of privacy

A common approach reflected in public opinion,[231] academic literature,[232] and case law[233] is to regard data protection as an *inherent* feature of privacy thus questioning the added-value of the constitutionalisation of data protection in CFREU. One proponent of the so-called 'inherency approach' is Daniel Solove. He suggests that privacy as such cannot be characterised with one notion and is rather a cluster of different concepts which are linked according to the notion of 'family

[229] Cuijpers, C. (2007). A Private Law Approach to Privacy; Mandatory Law Obliged? *SCRIPT-ed*, vol. 4 (4), pp. 304 – 318.
[230] Note that the terms for these approaches are not framed by the authors themselves but used in this thesis to categorise existing literature.
[231] In an interview with an EU official it was mentioned that privacy/data protection practitioners in the EU institutional bodies do not necessarily regard data protection and privacy as two distinct rights neither do they see a reason for having two distinct rights in the CFREU.
[232] For example, see: Solove, D. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York Press; Papakonstantinou, V. & De Hert, P. (2009) The PNR Agreement and Transatlantic Anti-terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic, *Common Market Law Review*, vol. 46, p. 885; Poullet, Y. (2009) Data Protection Legislation: What is at Stake for Our Society and for Democracy, *Computer Law and Society Review*, vol. 25, p. 211.
[233] As explained in section 3.1 in this Chapter.

resemblance'.[234] As such, data protection is the most recent addition to the right to privacy 'cluster'.[235] This means that before the emergence of the informational age, privacy was mainly regarded as 'seclusion' and the 'right to be let alone'. Nowadays, informational control had to be added to the notion of privacy due to the digitalisation and mass availability of information.[236] As such, privacy and data protection cannot be regarded as distinct rights but they rather serve the same purpose and are supported by the same values.

This conceptualisation is also based on the ECHR and related ECtHR case law. Since the ECHR does not grant data protection the status of an independent right, all aspects related to data protection obviously need to be grouped under privacy. More specifically the ECtHR brought multiple data protection principles/aspects under the scope of Article 8 ECHR including: (i) informational self-determination[237] such as claims to access personal files,[238] claims to delete personal information from public files,[239] and claims for data rectification;[240] (ii) independent supervisory bodies to prevent abuse of state power especially if secret surveillance is carried out;[241] (iii) the special status of sensitive data;[242] (iv) the basic idea of purpose limitation because personal data shall not be processed when it goes beyond foreseeable use;[243] (v), the principle of non-excessiveness since governmental authorities shall only collect data

[234] Solove makes use of the notion of Ludwig Wittgenstein, See: Wittgenstein, L. (1958). *Philosophical Investigations*, paras. 66-67. G.E.M. Anscombe trans
[235] Solove, D. (2004). op. cit., p.75.
[236] Ibid.
[237] De Hert, P. and Gutwirth, S. (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth, S. Poullet, Y,. De Hert, P. et al. (eds.). *Reinventing Data Protection*. Springer, p. 19.
[238] *Gaskin v. the United Kingdom*, Application no. 10454/83, judgment of 7 July 1989; *McMichael v. the United Kingdom*, Application no. 16424/90, judgment of 24 February 1995; *Guerra and others v. Italy*, Application no. 14967/89, judgment of 19 February 1998; *McGinley and Egan v. the United Kingdom*, Application nos. 21825/93 and 23414/94, judgment of 9 June 1998.
[239] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987; *Segerstedt-Wiberg and others v. Sweden*, Application no. 62332/00, judgment of 6 June 2006 ; *Rees v. the United Kingdom*, Application no. 9532/81, judgment of 17 October 1986.
[240] *Rees v. the United Kingdom*, Application no. 9532/81, judgment of 17 October 1986; *Cossey v. the United Kingdom*, Application no. 10843/84, judgment of 27 September 1990; *B. v. France*, Application no. 13343/87, judgment of 25 March 1992; *Christine Goodwin v. the United Kingdom*, Application no. 28957/95, judgment of 11 July 2002.
[241] *Klass v. Germany*, para. 55; *Leander v. Sweden*, paras. 65-67, *Rotaru v. Romania, Application no. 28341/954, judgment of 4 May 2000*, para. 59-60. Note that this only applies to state actors and not to private entities.
[242] *Gaskin v. the UK* and *Z. v. Finland*.
[243] De Hert, P. and Gutwirth, S. (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth, S. Poullet, Y,. De Hert, P. et al. (eds.). Reinventing Data Protection. Springer, p. 19. See also: *Peck v. UK*, para. 62; *Perry v. the United Kingdom,* Application no. 63737/00, judgment of 17 July 2002, para. 40; *P.G and J.H. v. the United Kingdom*, para. 59.

that is relevant and based on concrete suspicions;[244] (vi) financial compensation when data processing activities led to a breach of Article 8.[245] While acknowledging those data protection principles, the ECtHR still regards them as aspects of privacy.

While being a prominent model, the inherency approach raises multiple questions. For instance, in practice it is not entirely clear why data protection should follow exclusively the same purposes as privacy. Data protection tools do not only aim to ensure the right to privacy but also support the free flow of information in order to allow the smooth functioning of the internal market. Thus, it has an economic function which does not have any relevance for the right to privacy. In addition to that, some aspects that have been recognised as belonging to the right to private life, such as the sexual orientation and gender identification, do not necessarily have a data processing element. Therefore, regarding data protection merely as a facet of privacy is debatable. In fact, the notion of family resemblance as advocated by Solove can also be used to criticise the inherency approach as shown under 2.4 below in this chapter.

2.2 Quasi-separatist approach: privacy as an opacity tool and data protection as a transparency tool

According to Gutwirth and De Hert, privacy has an opacity function and data protection has a transparency function in the democratic constitutional state.[246] By guaranteeing non-interference in individual matters, privacy is an opacity tool.[247] The inviolability of the home is a good example of the latter since it illustrates the concern for respecting the boundary of the home. The fact that the sanctity of the home can only be upheld when the law is respected clearly shows that opacity tools always need to be balanced with considerations of the societal interest.[248] In addition to being an opacity tool, privacy can similarly be regarded as a negative (prohibitive) right that protects individuals against interference by governments and private actors.[249] Nevertheless, privacy has also a positive function in that it ensures individuals their

[244] *Segerstedt-Wiberg and others v. Sweden*, para. 79.
[245] *Rotaru v. Romania*, para. 79.
[246] De Hert, P. & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In Claes, E., Duff, A. & Gutwirth, S. (eds.) *Privacy and the criminal law*. Intersentia, pp. 61-104.
[247] ibid., p. 71.
[248] ibid., p. 68.
[249] The formulation as a negative right can be observed in Article 8 ECHR (no interference...unless...)

freedom of self-determination and their autonomy to make choices and to engage in relationships.[250] In sum, privacy can mostly be regarded as an opacity tool, however it still has a regulatory or transparency dimension.[251]

In contrast to opacity tools, transparency tools come into play after normative choices have been made in order to regulate the normatively accepted exercise of power.[252] Accordingly, data protection is a tool of transparency (or a permissive tool).[253] Assessing the formulation of data protection principles supports this categorisation. For instance, fairness, accountability, individual participation principles all rely on procedural justice instead of substantive or normative justice.[254] Furthermore, data protection is mostly not about prohibiting data processing but channelling and regulating it.[255] By doing so, data protection laws contain certain conditions to ensure transparency of the processing and accountability mechanisms of the data controller.[256] Besides being mainly a transparency tool, two characteristics of data protection regulation also reveal features of opacity. First, processing of data relating to ethic or racial origin or data revealing religious or philosophical beliefs (sensitive data) is in general prohibited. Second, decision-making exclusively on the basis of data profiles is also prohibited.[257]

By arguing that privacy is mainly an opacity tool while data protection is mostly a transparency tool, this approach provides an interesting account of the different functions of privacy and data protection as instruments of political control in democratic constitutional states.[258] Nevertheless, the approach can also regarded as too simplistic to describe the complex and multi-layered interaction between privacy and data protection. First of all, as already rightly pointed out by the authors themselves the distinction between opacity and transparency tools is not clear-cut since both rights also reveal some features of the respective other category. This shows that privacy and data protection are not completely distinct. Respectively, instead of

---

[250] Arendt, H. (1958). *The Human Condition*. University of Chicago Press, p. 70 and Habermas, J. (1989). *The structural transformation of the public sphere*. MIT Press, p. 26.
[251] De Hert, P. & Gutwirth, S. (2006). op. cit.
[252] De Hert, P. & Gutwirth, S. (2006), op. cit., p. 78.
[253] Ibid.
[254] Ibid.
[255] For example, the purpose limitation principle requires data to be necessary/proportionate for a specific purpose. In this way it regulates and channels processing rather than prohibiting it.
[256] Friedewald, M. et al. (2010). Privacy, data protection and emerging sciences and technologies: towards a common framework. *Innovation -The European Journal of Social Science Research,* vol. 23 (1), p. 163.
[257] Both the first and second aspect is mentioned in the DPD. See for instance: Article 8 (1), DPD.
[258] De Hert, P. & Gutwirth, S. (2006), op. cit.

pursuing two distinct objectives, data protection and privacy can be understood "(…) together as forming the evolving bundle of legal protections of the fundamental…value of the automatic capabilities of individuals in a free and democratic society."[259] A second shortcoming of this theory is that while acknowledging that inherent to both data protection and privacy are elements of opacity and transparency, the authors do not further develop the common overarching value of privacy and data protection. By regarding them as two separate instruments to limit control of the state, the authors disregard an important intermediate step - namely the analysis of values pursued by both rights- which leads to the assumption that both rights are separate.

2.3 Instrumentalist approach: data protection and privacy as instruments to protect the right to human dignity

Rouvroy and Poullet establish a two- step argument where data protection and privacy are perceived as sharing the same goal of supporting individual self-development and the autonomous capacities of individuals to act and interact which are essential elements of human dignity.[260] This approach has been described as a model where data protection and privacy are complementary tools.[261] However, the focus of the theory is not on how privacy and data protection have distinct or complementary functions. Instead both privacy and data protection are considered to be instruments to safeguard the more upstream right to human dignity.[262] Therefore, in this thesis this approach will be termed an 'instrumentalist' approach. One might wonder whether the instrumentalist approach is a sub-category of the inherency approach as both privacy and data protection are regarded as sharing the same overarching value. The reason for presenting it as independent approach is the rather 'agnostic' and incomplete view of the authors on the correlation of data protection and privacy. While the inherency approach actively tries to grasp the link between data protection and privacy in their own capacity, the instrumentalist approach regards this aspect as subordinate by primarily focusing on the ultimate goal that both rights pursue.

[259] Rouvoy, A. & Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In; Gutwirth, S. et al. (eds.) *Reinventing Data Protection?* Springer, p.76
[260] Rouvoy, A. & Poullet, Y. (2009), op. cit., p.47.
[261] Lynsky, O. (2015), op. cit., p. 94.
[262] The term 'instrumentalist approach' has also been used by: Tzanou M. (2013) Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, vol. 3(2), p. 94.

In essence, Rouvroy and Poullet argue that both privacy and data protection have an 'intermediate' rather than final value since they are instrumental to the achievement of a more fundamental value, namely the right to human dignity. As human dignity is a broad concept with blurred boundaries,[263] the authors point out that data protection and privacy are instrumental to the following two aspects of human dignity: informational self-determination and self-development of one's personality. In developing this claim the authors particularly have recourse to the German *Volkszählungsurteil* of 1983. In the judgment the German Constitutional Court establishes that a cluster of rights (which nowadays form part of data protection) stems from the individual's right to 'informational self-determination'. The latter is itself derived from 'the right to personality' which stems from the right to human dignity[264] and the right to free development of personality.[265] Based on that, the authors argue that privacy and data protection are tools that foster the autonomic capabilities of individuals that are crucial to sustain a vivid democracy.[266]

While being an important approach that is rooted in German jurisprudence, there are some objections to this theory. First, human dignity is a very broad concept with multiple different meanings in EU Member States. Consequently, generalising a German approach to EU law might be problematic.[267] Second, the EU Charter itself groups data protection and privacy under the heading 'freedoms' instead of grouping it together under the heading of 'dignity' (combining rights such as: right to live, right to integrity of person, prohibition of torture, etc.). While a draft version of the Charter did use a more dignity-based interpretation of data protection this was rejected in the final version - most likely because it did not represent the majority of national interpretations of the concept.[268] Third, human dignity has been used to express various different philosophical beliefs. In this respect one could argue that an underlying principle of dignity is giving data subjects the *choice* to waive their rights. If this were the case, all prohibitive aspects of data protection law would be a breach of human dignity.[269] Ultimately, another criticism is that human dignity is an

[263] See for instance: *Evans v United Kingdom*, para. 77. See also: Bognetti, G. (2003) The Concept of Human Dignity in European and US Constitutionalism. In: Nolte, G. (ed.) *EU and US Constitutionalism*. Cambridge University Press.
[264] Deutsches Grundgesetz, Article 1 (1)
[265] Deutsches Grundgesetz, Article 2 (1)
[266] Rouvoy, A. & Poullet, Y. (2009), op. cit., p.46.
[267] Lynsky, O. (2015), op. cit., p. 99.
[268] p. 100.
[269] Ibid.

inviolable right which excludes the possibility of limiting it due to other considerations. However, data protection also follows other objectives such as economic objectives (e.g. the free flow of information).

Besides the obvious focus on the link to human dignity and its orbiting values, Rouvoy and Poullet only marginally discuss the correlation of data protection and privacy. Thus, the authors miss the chance to elaborate more on the distinctiveness of privacy and data protection. Especially when regarding 'consent' as relevant aspect of informational self-determination differences between privacy and data protection could have been detected. Neither Article 8 ECHR nor Article 7 CFREU refer to the concept of consent as a legitimation for intrusion. Furthermore, in case law this point is often neglected when assessing the legality of Article 8 ECHR interferences.[270] Contrarily, the role of consent plays a significant role in the context of data protection. For instance, in the data protection directive consent is one of the grounds determining the legitimacy of data processing.[271] In this regard, consent can empower the data subject if it is freely given, informed and specific.[272]

2.4 Assemblage approach: data protection and privacy as part of the same conceptual network with intersecting and distinct nodes

The three above-mentioned approaches illustrate the complexity of conceptualising the correlation of privacy and data protection. While none of the approaches should be rejected, all three have been subject to some criticism. The inherency approach has been criticised for not sufficiently accounting for the different goals pursued by privacy and data protection while the quasi-separatist approach has not sufficiently elaborated on the shared values of privacy and data protection. Ultimately while the instrumentalist approach argues that both privacy and data protection are instrumental in safeguarding informational self-determination and self-development of one's

[270] See for instance: *Murray v. the United Kingdom,* Application no. 14310/88, judgment of 28 October 1994; *Z. v. Finland,* Application no. 22009/93, judgment of 25 February 1997; *M. S. v. Sweden,* Application no. 20837/92, judgment of 27 August 1997; *L. L. v France,* Application no. 7508/02, judgment of 10 October 2006. An exception to this general trend is *Peck v United Kingdom*, Application No 44647/98, judgment of 28 January 2003. The Court mentioned that an illegal privacy intrusion could have been prevented if the concerned individual would have been asked for consent (para. 80).
[271] Articles 7 and 8, DPD.
[272] Article 2 (h), DPD. It needs to be noted though that according to data protection law, 'consent' is not absolute. Article 7 (f) DPD permits data processing without consent if necessary "for the purposes of the legitimate interests pursued by the controller".

personality as aspects of human dignity, the correlation or added value of having two separate rights is not addressed.

In this context, what could an alternative approach look like? As argued by Lynsky[273] the notion of family resemblance used by Solove to underpin the inherency approach can at the same time be used to support an alternative model. Solove explains that privacy is a pluralistic concept that offers a set of protections against a related cluster of problems. By offering protection to different problems privacy shall not be regarded as 'one thing' but a cluster of many distinct yet related things.[274] To illustrate this, he makes use of Wittgenstein's family resemblance theory. Wittgenstein argues that "(…) certain concepts might not share one common characteristic; rather, they draw from a common pool of similar characteristics – 'a complicated network of similarities overlapping and criss-crossing: sometimes overall similarities and sometimes similarities of detail.'"[275] Wittgenstein calls this observation 'family resemblance' since the detected overlapping and criss-crossing characteristics also exist between family members such as "build, features, colour of eyes, gait, temperament, etc."[276] Following Solove's line of thought implies that data protection belongs to the conceptual cluster of privacy. Contrarily Lynsky argues that the family resemblance theory can also support the argument that data protection and privacy are distinct in the sense that data protection is a right that serves a number of purposes, including but not limited to privacy purposes. This is because "(…) data protection overlaps to a certain extent with other elements of privacy but also includes aspects which fall outside the scope of the right to privacy."[277]

While the substance of Lynsky's interpretation of the family resemblance approach is an attractive alternative model since it allows flexibility and accounts for different ways that privacy and data protection are related, the term 'family resemblance' may not be appropriate since 'family' implies derivative from one common origin. Logically 'family' also implies only one-directional causal links. In reality, there is not always the same causal relationship between the two concepts. For example, in some cases data protection is a tool to safeguard privacy while in other cases data protection is unrelated to protecting privacy. Furthermore, there is not one

[273] Lynsky, O. (2015), op. cit., p.102-103.
[274] Solove, D. (2008). *Understanding Privacy*. Harvard University Press, p. 40.
[275] Ibid., p. 42; (referring to: Wittgenstein, L. (1958), para. 66).
[276] Wittgenstein, L. (1958), op. cit., para. 67.
[277] Lynsky, O. (2015), op. cit., p. 103.

overarching origin of both concepts as "family" implies: While the overarching objective of privacy originated from the goal to protect the individual against state intrusion, data protection emerged with the technological revolution and related internal market considerations.[278] Taking this into account the neutral term "conceptual assemblage" to relate data protection and privacy seems more appropriate. Assemblage theory has been mainly developed to study the composition of the society. Nevertheless, the notion of "assemblage" can also provide useful insights when defining the correlation of privacy and data protection. An assemblage is a network of more or less heterogeneous components and their symbiotic relationship through which those single components are grouped into a co-functioning system.[279] The single components forming the assemblage do not form an overarching unity. Instead the single elements establish a degree of consistency which can be analysed as an assemblage without however converging it into an independent system.[280] While similar to the notion of family resemblance, this approach grants a slightly more independent status to both privacy and data protection. One can consider both privacy and data protection as elements of the same conceptual assemblage. Within the assemblage both elements are actively engaging with each other without loosing their status as an independent concept. In practice this means that while some aspects of privacy and data protection are intertwiningly linked others are inherently distinct from each other. Consequently a sphere exists where both concepts interact and diverge in a multi-layered, networked way.

Having explained the assemblage approach the question emerges what it can offer in contrast to the other three approaches. First and foremost, the theory accounts for the close connection between privacy and data protection while acknowledging that they are two separate rights as stipulated in the EU constitutional order. In addition acknowledging the clear distinction between data protection and privacy is also more respectful to different constitutional traditions in EU Member States, which are often used as benchmark by the CJEU in its jurisprudence.[281] For instance in Germany data protection law is based on human dignity while in France data protection is anchored to the notion of individual liberty and in Belgium data

[278] Data protection could even be regarded as counter-movement to privacy because different rules on how to protect privacy resulted in barriers to the free flow of information.
[279] On assemblage theory, see: DeLanda, M. (2006) *A New Philosophy of Society: Assemblage Theory and Social Complexity*. Continuum.
[280] Deleuze, G., & Parnet, C. (2007) *Dialogues II*. Columbia University Press, p. 69.
[281] Lynsky, O. (2015), op. cit., p. 104.

protection is rooted in privacy.[282]

2.5 The CJEU adopts the inherency approach: an example of path-dependence?

Having explained different approaches to the conceptual interdependence of data protection and privacy, the CJEU has adopted the inherency approach although the CFREU does acknowledge data protection as distinct fundamental right.[283] More specifically, the CJEU has two ways to correlate the two rights. First, the CJEU considers data protection –embodied by the Data Protection Directive- as an ancillary, procedural tool that safeguards the right to privacy.[284] Second, the CJEU also regards data protection merely as a facet of privacy.[285] While the CJEU is required to take ECtHR case law into account when ruling on fundamental rights[286] it is striking that the constitutional difference between CFREU and ECHR has not been acknowledged. Nevertheless, in the recent judgment *Tele2 Sverige* the CJEU for the first time explicitly mentions that "(…) Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR."[287] While this potentially signifies the move towards a different conceptualisation of the correlation of Articles 7 and 8 CFREU, in the substantial parts of *Tele2 Sverige* the CJEU does not distinguish between the two rights. This strong statement does thus not have any immediate effects on how the CJEU considers the correlation between Articles 7 and 8 CFREU. It is rather to be considered as attempt to stress the autonomy of EU fundamental rights vis-à-vis the ECHR. Nonetheless, the remarks on the clear distinction may be picked up and be subject to future case law.

The CJEU's adoption of the ECtHR approach can be explained by applying a conceptual and/or institutional reasoning. In regard to the former the CJEU arguably adopts the ECtHR approach since this is how the two concepts *de facto* interact or

---

[282] Brouwer, E. (2008) *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*. Martinus Nijhoff Publishers, p. 198.
[283] While the explanations accompanying the Charter mention that Article 8 CFREU is based on Article 8 ECHR, the Charter itself only requires the CJEU to provide equivalent protection as the ECHR 'in so far as this Charter contains rights which correspond to rights guaranteed by the Convention' (Article 52 (3) CFREU).
[284] Case C-465/00 *Rechnungshof v Österreichischer Rundfunk and Others*, judgment of 20 May *2003*, para. 70. See also the corresponding Opinion of AG Tizzano, para. 50.
[285] Case C-275/06, *Productores de Música de Espana Promusicae vs. Telefónica de Espana*, judgment of 29 January 2008, para. 63; Joined cases C-92/09 and C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen* , judgement of 9 November 2010, para. 52; *DRI*, para. 53.
[286] Article 52 (3), CFREU.
[287] *Tele2 Sverige*, para. 129.

ought to interact. This would correspond to the arguments presented under the inherency approach.[288] However, as pointed out earlier this conceptualisation can be challenged in multiple ways.

A second explanation as to why the CJEU adopts the inherency approach is based on an institutionalist assessment. More specifically, the concept of path-dependence[289] can help to explain why the CJEU follows the interpretation of the ECtHR. The cross-fertilisation between the two courts on the correlation of privacy and data protection is just one aspect of a special institutional relationship between the courts. On a purely formal level, the ECHR and the EU are unconnected since the EU did not accede to the ECHR.[290] Therefore, neither does EU legislation fall within the jurisdiction of the Strasbourg court nor does the ECHR or related jurisprudence create direct obligations for the EU. This has been stressed in *Tele2 Sverige* where the CJEU stated that "(…) the ECHR does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated in EU law."[291] Besides the separation between the two courts a strong relationship based on judicial dialogue evolved over the years.[292] Initially the CJEU did not deal with fundamental rights issues by understanding itself mainly as 'internal market' court. In the 1970s it then started to address fundamental rights by regarding it as general principle of Community law and by explicitly pointing to the ECHR.[293] While *Opinion 2/94*, putting EU accession to the ECHR to a halt, implied a short 'ice period' in the relationship between the courts, the relationship quickly normalised again with the CJEU citing frequently and in greater depth ECtHR jurisprudence.[294] Efforts were even made to rectify inconsistencies between CJEU and ECtHR judgments.[295] The

[288] Section 2.1 of this Chapter.
[289] As explained in Chapter 2.
[290] Note that the CJEU did not accede to the ECHR. In 1996, *Opinion 2/94* stipulated that the Treaties lacked an appropriate legal basis for accession. Post-Lisbon, *Opinion 2/13* still held that accession is not compatible with EU law. Nevertheless, there is some debate as to whether Article 6 (3) TEU and 52 (3) CFREU at least require the CJEU to account for ECtHR case law. For a more detailed analysis, see: Krommendijk, J. (2015). The use of ECtHR case law by the CJEU after Lisbon: The View of the Luxembourg insiders. *Maastricht Faculty of Law Working Paper 2015/6*, pp. 7-12.
[291] *Tele2 Sverige*, para. 127.
[292] Krisch, N. (2010) *Beyond Constitutionalism*. Oxford University Press, p.129
[293] See for instance: De Witte, B. (1991) Community Law and National Constitutional Values. *Legal Issues of European Integration*, vol. 18 (1), pp. 1-22. See also: Stone Sweet, A. (1998) Constitutional Dialogues in the European Community. In: Slaughter, A. Stone Sweet, A. & Weiler, J. (eds.) *European Courts and National Courts*. Hart Publishing.
[294] E.g. C-368/95 *Familiapress*, judgment of 26 June 1997, para. 24-6. See also: C-185/95 *Baustahlgewebe*, judgment of 17 December 1998.
[295] See for instance: C-94/00 *Roquette Frères*, judgement of 22 October 2002, departing explicitly from C-227/88 *Hoechst* judgment of 21 September 1989.

"friendly interplay between the courts mirrored political developments" when the ECHR was "granted a prominent place in the EU Charter of Fundamental Rights in 2000".[296] Nevertheless, *Opinion 2/13* again postulated the autonomy of the EU vis-à-vis the ECHR. This has also been reiterated in case law where the CJEU mentions that interpretation of EU law must be 'undertaken solely in light of the fundamental rights guaranteed by the Charter'[297] and that consistency between the ECHR and CFREU shall not adversely affect the autonomy of Union law and the CJEU.[298] All in all, one can conclude that over thirty years of interaction between the two courts is marked by the persistence of autonomy but extensive judicial dialogue and convergence in interpreting fundamental rights issues.[299] While originally the CJEU rationale of using ECtHR as 'source of inspiration' was at least to a certain extent to underpin its own authority,[300] the intertwined relationship continued even after CFREU was adopted.

The reason for being bound to earlier trajectories is related to both practical and abstract aspects. On the one hand, in relation to practical considerations the CJEU has an interest in preventing the emergence of two 'branches' of fundamental rights law which are too diverse in nature. Since EU Member States are bound by both regimes it would reduce legal certainty and ultimately undermine the CJEU's own legitimacy if Member States had to 'pick' which fundamental rights regime to follow in case that inconsistencies emerge.[301] Particularly deviation in terms of the conceptualisation of rights -such as the rights to data protection and privacy, and their correlation- could lead to variety and has the potential of substantial discrepancy to earlier paths. On the other hand, stickiness to established paths can also be explained in more abstract

[296] Krisch, N. (2010), op. cit., p.131.
[297] *Tele2 Sverige*, para. 128.
[298] *Tele2 Sverige*, para. 129. See also: C-601/15 *PPU*, para. 47.
[299] This was acknowledged by the President of the CJEU at the time (Judge Rodriguez Iglesias). See also: Costello, C. (2006) The *Bosphorus* Ruling of the European Court of Human Rights: Fundamental Rights and Blurred Boundaries in Europe. *Human Rights Law Review,* vol. 6 (1), p.114.
[300] From the 60s onwards the CJEU referred to ECtHR case law and argued that fundamental rights form an integral part of the general principles of law which the CJEU protects. The references to fundamental rights via ECtHR jurisprudence was an attempt of the CJEU to justify the CJEU's establishment of doctrines such as direct effect and supremacy. Member States have become concerned about the latter doctrines since the CJEU adjudication had far-reaching effects on Member States and their constitutions. See: Schimmelfennig, F. (2007). Competition and Community: Constitutional Courts, Rethorical Action, and the Institutionalization of Human Rights in the European Union. In: Rittberger, B. & Schimmelfennig, F. (eds.). *The Constitutionalisation of the European Union*. Routledge.
[301] See: Rosas, A. (2007) The European Court of Justice in Context: Forms and Patterns of Judicial Dialogue. *European Journal of Legal Studies*, vol. 1, p. 9 -10. See also: Krommendijk, J. (2015), op. cit., p. 18 -19.

ways. Firstly, sticking to previous paths is a result of a naturally limited 'room for action' created by legal frameworks which judges need to adhere to. Thus, adoption of similar interpretations like in previous rulings is more likely. Secondly, previous cases create an 'argumentation framework' which help judges to make analogies and frame topics in a certain way. 'Argumentation frameworks' not only help judges to apply certain problem-solving frameworks but also shape the way claimants pose their request to the court. Ultimately, sticking to previously developed paths leads to more legal certainty and provides more legitimacy to courts as they are considered to be less arbitrary and inspired by judicial instead of political considerations. While acknowledging that path-dependence is important to understand how the CJEU correlates privacy and data protection in some circumstance deviation from previous paths can take place as shown in the next section.

3. CJEU and ECtHR jurisprudence on privacy and data protection in the public security context: the incremental move onto a new path?

As mentioned in the previous section, the CJEU traditionally referred to ECtHR jurisprudence when adjudicating on fundamental rights rendering the ECtHR a standard-setter for the EU legal order. ECtHR case law not only played an important role in shaping fundamental rights in general terms but also in setting standards when assessing whether an interference with the right to private life on grounds of public security was proportionate. Various ECtHR cases concern the legality of measures that allow the collection, retention or access to personal data for the purposes of safeguarding national security and/or of preventing disorder and crime.

Most ECtHR cases refer to surveillance measures governing the targeted access to individual communication. At the same time, in recent years an increasing blurriness between targeted and 'wide-ranging' retention and access regimes can be detected. The shift to wide-ranging measures can be explained by technological advancement. Due to big data analysis and the use of algorithms it has become increasingly necessary to 'accumulate the haystack to find the needle.'[302] In the context of the shifting nature of public security measures, existing standards as laid down by the ECtHR continue to play an important role for the assessment of their

[302] Former NSA Director Keith Alexander Keith Alexander quoted in: Rosenbach, M. and Stark, H. (2015). *Der NSA Komplex. Edward Snowden und der Weg in die totale Überwachung*. Spiegel Verlag.

legality. The ECtHR made this clear by stating that "(…) there is [not] any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other."[303]

In parallel to the ECtHR's continuous role, one can however observe that the CJEU is gaining importance in setting standards in respect to wide-ranging data retention and access regimes. This increasing role is evidenced by the ECtHR's recent references to Luxembourg judgements in the context of data access regimes.[304] The intertwined relationship and relevance of both ECtHR and CJEU case law is outlined in 3.1 below. It is shown that both courts give a similar weight to privacy and data protection in the public security context. Section 3.2 will then show that due to institutional aspects a more prominent role for the CJEU can be detected in the post-Lisbon context.[305] The subsequent framework will serve as a model for the legal assessment in the case study chapters.

3.1 The judicial dialogue between the ECtHR and CJEU in relation to data retention and access regimes

3.1.1 Processing of data should be based on 'accessible, foreseeable and precise rules' and respect the essence of the right

Any legislative measure must be in accordance with law meaning that it must be foreseeable (i.e. as to its effects for the individual) and accessible (i.e. public).[306] On many occasions the ECtHR held that foreseeability in the context of public security measures cannot be the same as in other fields. More specifically, if a suspect was notified ex-ante about interception or if he/she was able to predict surveillance, he or

[303] *Liberty and others v UK*, para. 63.
[304] In *Zakharov v. Russia,* the ECtHR quoted the findings from *Digital Rights Ireland* under the section "Relevant International and European Instruments" (para. 147). In *Szabó and Vissy v. Hungary* the ECtHR refers to *Digital Rights Ireland* in the section "Other relevant international texts" (para. 23) and in the legal assessment (para. 68, 70).
[305] Storgaard, L. H. (2015). Composing Europe's Fundamental Rights Area: A Case for Discursive Pluralism. *Cambridge Yearbook of European Legal Studies*, vol. 17, pp. 222 -223. Storgaard argues that the dialouge and/or potential tensions between the CJEU and ECtHR can be linked to three categories: (i) interpretive competition caused by the overlapping substantive and jurisdictional powers of both courts, (ii) contest on the weight or priority to be given to fundamental rights when they collide with other legitimate interests, (iii) controversy about who holds the ultimate authority on fundamental rights. When arguing that the CJEU has a more prominent role, reference is made to point (i) of the three categories.
[306] *Malone v. United Kingdom*, paras. 65, 66 and 70.

she could adapt the behaviour accordingly.[307] Therefore, in the public security context, foreseeability means that laws must be sufficiently clear as to circumstances and conditions on which national authorities might engage in interception.[308] In addition to the accordance with law requirement, laws must also be sufficiently precise by providing detailed provisions as further explained below.[309]

In contrast to the ECtHR, the CJEU requires not only that the interference is 'provided for by law' but also that any interference respects the essence of privacy and data protection. For instance, in both *Digital Rights Ireland* and *Schrems* the CJEU argues that the content of electronic communications forms the essence of privacy.[310] At the same time, the CJEU argues that certain principles of data security constitute the essence of Article 8 CFREU such as data quality, appropriate technical and organisational protection against data loss, mandatory destruction of data at the end of the retention period, etc.[311] The concept of the 'essence of a right' derives from older CJEU case law holding that the very substance of the rights should never be compromised.[312] The concept is not always clear since especially in the context of data protection and privacy the boundary between the periphery of a right and its essence is not always clear-cut.[313] Furthermore, the CJEU does not usually discuss the essence of a right in detail. One reason may be that this would immediately lead to a breach of the Charter and thus the Court could not engage in a discussion of the various interests at stake.[314]

In sum, ECtHR jurisprudence provides a detailed framework to establish whether a measure is in accordance with the law or in CFREU terms 'provided by law'. Instead the CJEU discusses these aspects often under the proportionality assessment and focuses on assessing whether the essence of the right to privacy and data protection has been infringed. In practice the discussion on the essence does not often go into depth and does not take the complexities of privacy and data protection

[307] *Zakharov* v. *Russia*, para. 229
[308] ibid.
[309] Section 3.1.2 of this Chapter.
[310] *DRI*, para. 39 and *Schrems*, para. 94.
[311] *DRI*, para. 40.
[312] E.g. Case C-5/88 *Wachauf* of 13 July 1989, para. 18 or Case C-292/97 *Karlson and others* of 13 April 2000, para. 45.
[313] For instance, in *Digital Rights Ireland*, content data was regarded as "essence of the right" while traffic and location data was considered beyond the essence of the right. As shown in Chapter 4 in reality the boundary between traffic and location data is not always clear-cut.
[314] Hijmans, H. (2016). *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU*. Springer

into account.[315] Therefore, the CJEU does not often consider the essence of a right.[316]

3.1.2 Proportionality in terms of necessity with regard to the legitimate objectives pursued

There is no doubt that data retention and access regimes for public security purposes trigger an interference with the right to privacy and data protection.[317] Since this interference is particularly serious[318] it can only be considered to be legal if it is 'strictly necessary in a democratic society'[319] and proportionate in relation to a legitimate objective. Proportionality in terms of necessity is however difficult to assess. It opens a debate on which values prevail in a democratic society and about what kind of society we wish to live in.[320] In this value-driven discussion, it is necessary to discuss advantages and disadvantages of wide-ranging data retention and access measures for public security. On the positive side, in contrast to targeted surveillance, wide-ranging data retention and access measures allow law enforcement authorities to access past communications effected by persons before they have been identified.[321] On a practical level, the usefulness of these regimes lies for example in preventing the recent phenomenon of 'foreign fighters' or in investigating terror attacks such as the 2015 terror attacks in France.[322] This contributes to the overarching aim of maintaining public security by preventing and detecting crime and to the enforcement of the law by facilitating the investigation and prosecution of crime.

On the negative side, "(…) by contrast with targeted surveillance measures, a general data retention obligation is liable to *facilitate considerably mass interference*, that is to say interference affecting a substantial proportion or even all the relevant population."[323] A practical example of mass interference is where data retention measures could allow a person to easily extrapolate a list of persons who suffer from a

[315] Limiting the essence of privacy to content data and the essence of data protection to data security is too simplistic. It does not take the constitutional value of data protection into account and does not acknowledge the implications of non-content related data on the right to privacy.
[316] Therefore, the CJEU's claim in *Schrems* that the essence of Article 7 CFREU was infringed reflects a deviation from usual practices and shows the increasing significance the CJEU ascribes to privacy.
[317] *DRI*, para. 36.
[318] Ibid.
[319] *Klass and Others v. Germany*, para. 42 and 48; *Malone v. United Kingdom*, para. 81; *DRI*, para. 52; Case C-473/12 *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others* of 7 November 2013, para. 39.
[320] AG Opinion in *Tele2 Sverige*, paras. 248.
[321] AG Opinion in *Tele2 Sverige*, paras 178-183.
[322] Ibid. Emphasis added by author.
[323] AG Opinion in *Tele2 Sverige*, para. 256; emphasis added by author.

psychological disorder or of persons that oppose the incumbent government.[324] It was mentioned that there is 'nothing theoretical' about abuse or illegal access given the extremely high numbers of requests for data.[325] Another risk of wide ranging data retention and access regimes is that it "(…) is likely to generate in the minds of the persons concerned the *feeling* that their private lives are the subject of *constant surveillance*."[326] This is particularly concerning as it could inhibit the development of individual personalities and the establishment of relationships.[327]

In general, case law does not go into great depth on the parameter on whether a measure is 'necessary' in regard to the legitimate objectives pursued. For instance, in *DRI* the CJEU differentiates between appropriateness of the DRD and 'strict necessity'[328]. While the DRD was deemed appropriate due to its ability to shed light on serious crime, the 'strict necessity' criterion is intrinsically linked to the assessment of the existence of safeguards against abuse of powers.[329] Thus, the CJEU's elaborations focus more extensively on analysing the provisions of the respective measure instead of elaborating on the measure's necessity in more abstract terms.[330] Ultimately, assessing the strict necessity of data retention and access regimes is highly context dependent and is often based on hypothetical risks on both sides.[331] Therefore, a wide margin for courts to conduct the proportionality assessment is required.[332]

3.1.3 Proportionality in terms of existence of safeguards against 'abuse of power'

Both CJEU and the ECtHR have developed several safeguards to mitigate risks of 'abuse of power' and which ought to be included in any data retention and access

[324] Ibid., paras. 257-258.
[325] Ibid., para. 260.
[326] *DRI*, para. 37; emphasis added by author.
[327] This is particularly true in the digital age where a large amount of personal interaction and personality building happens in the online space, generating vast amounts of personal data.
[328] *DRI*, paras. 46 - 52.
[329] *DRI*, paras. 52 - 55.
[330] In regard to the likelihood of abuse it has been mentioned that "the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system." (*Klass and Others v Germany*, para. 59.). Thus 'safeguards against abuse' can only be understood in a sense of diminishing the 'risks of abuse'.
[331] The relevance of data to fight threats to public security is in this case as hypothetical as the risk of mass interference of the rights of individuals.
[332] *Tele2 Sverige*, para. 124.

legislation in the public security context.[333] This is necessary 'especially as the technology available for use is continually becoming more sophisticated'.[334] In the following several safeguards on access, oversight of access, remedies, retention period, data security and onward transfer will be discussed.

(i) Scope of application

According to both ECtHR and CJEU case law the target group liable to interception needs to be defined by law and both courts express concerns in regard to measures facilitating mass surveillance.[335] For example, in *Szabó and Vissy*, the ECtHR expressed its concerns with the legislation in question because "(…) it might include indeed any person and be interpreted as paving the way for unlimited surveillance of a large number of citizens."[336] The ECtHR further criticises that there is no need for authorities to demonstrate the actual or presumed relation between the persons concerned and the prevention of a terrorist threat.[337] Similarly, in *DRI* the CJEU criticised the unlimited and indiscriminate scope of the DRD.[338] It held that the scope of data retention measures must not be beyond a point where a connection between the data to be retained and the objective of fighting serious crime is evident.[339] While this statement implies that indiscriminate data retention is illegal, the Court subsequently specifies that the link has to be 'at least an indirect one'.[340] Since this is just one example and the fact that 'an indirect link' is possible, the judgement as well as ECtHR judgments leave a margin to Member States in deciding the precise scope of retention and access regimes.

(ii) Grounds for access

The courts put an emphasis on substantive and procedural conditions relating to access of competent authorities to data and their subsequent use.[341] Four different aspects are worth pointing out in this respect: First, access to data should be strictly

[333] *Klass v. Germany*, para. 50; *Weber and Saravia v. Germany*, para. 95; *Liberty v. UK*, para. 62; *Zakharov v. Russia*, para. 231 and *Szabó and Vissy v. Hungary*, para. 56; *DRI*, para. 54.; *Schrems*, para. 91.
[334] *Weber and Saravia v. Germany*, para. 93.
[335] See: *Liberty and others v. UK*, para. 64 or *Szabó and Vissy v. Hungary*, para. 66 -67; *DRI*, para. 56 to 59; *Tele2 Sverige*, para. 97 to 106
[336] *Szabó and Vissy v. Hungary*, para. 67.
[337] Ibid.
[338] *DRI*, para. 56 - 59.
[339] *Tele2 Sverige*, para. 110.
[340] *Tele2 Sverige*, para.111.
[341] *DRI*, para. 60.

limited to the purpose of preventing and detecting defined criminal offences.[342] The CJEU mentions that in regard to data retention measures, access can only be granted if it is assumed that an individual is either himself suspected of having committed or planning a serious crime or if the individual can contribute to provide evidence on it.[343] Furthermore, the CJEU also mentions that serious crimes need to be precisely defined.[344] It has been suggested that this could be best achieved by providing a list of the offences that qualify as 'serious crime'.[345] An alternative approach has been adopted by other EU legislation where not only a list of serious crimes is considered as sufficiently precise but also the requirement that an offence leads to a minimum term of imprisonment of three years.[346] The CJEU also held that access to data shall not only be limited to serious offences but also to a small number of authorised persons.[347]

The ECtHR also argues that the crimes giving rise to surveillance need to be defined for the sake of foreseeability of the scope of the law. In *Zakharov v. Russia* the ECtHR criticises that a minor offence such as pickpocketing is sufficient to give raise to interception.[348] At the same time however, the ECtHR seems to be more lenient since it mentions that conditions of foreseeability do not require states to set out exhaustively, by name, the specific offences which give rise to interception.[349] Furthermore, crimes of medium severity and serious offences seem to be sufficient for the ECtHR to justify surveillance measures.[350] It has thus been argued that CJEU goes beyond the protection as established by the ECHR and ECtHR case law.[351] However, shortly afterwards the ECtHR took the particular character of 'cutting-edge surveillance technologies' and its effects on privacy into account and argued that secret surveillance can only be regarded as compliant with the Convention if two conditions are met. First, it has to be strictly necessary for safeguarding democratic

[342] ibid., *Tele2 Sverige*, para. 111, *Kennedy v. UK*, para. 159, *Zakharov v. Russia*, para. 244.
[343] *Tele2 Sverige*, para. 119.
[344] *DRI*, para. 60.
[345] AG Mengozzi on *Opinion 1/15*, para. 235.
[346] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States, *OJ 2002 L 190/1*, Article 2 (2) of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters, *OJ 2014 L 130*, Article 11 (1) (g) and Annex D.
[347] *DRI*, para. 62
[348] *Zakharov v. Russia*, para. 244.
[349] Ibid; *Kennedy v. United Kingdom*, para. 159.
[350] Ibid.
[351] See: *Secretary of State for the Home Department v. David Davis and others*, [2015] EWCA Civ 1185, para. 112.

institutions and, second, it has to be inevitable for intelligence in an individual operation.[352] The ECtHR refered to the CJEU's *DRI* judgment showing the reciprocal character of judicial dialogue between the two courts.

(iii) Oversight on access

An independent oversight mechanism should exist to monitor the access of public authorities to the data. In the ECtHR landmark ruling *Klass v. Germany* it was held that interference with Article 8 ECHR should be subject to oversight either by a judge or by another independent body.[353] The CJEU shared this view when it ruled in *DRI* that the access by the competent national authority to the data retained should be dependent on ex-ante review carried out by a court or independent administrative authorities "(…) whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions."[354] This was reiterated in *Tele2 Sverige* where it was held that "(…) it is essential that access of competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to prior review carried out either by a court or by an independent administrative body.[355]

The ECtHR expressed a preference for a judge or court as the best way to carry out the oversight since impartiality can be best guaranteed.[356] The AG in *Tele2 Sverige* makes an interesting observation regarding the reason for the importance of having independent oversight mechanisms in place. First, it facilitates the filtering of sensitive information (i.e. data subject to professional privilege) which can be technically difficult to filter out in advance. Second, because all other parties involved have either an own interest in the data overriding impartiality (i.e. law enforcement authorities) or are ignorant of important information underlying the investigation (i.e. service providers).[357]

---

[352] *Szábo and Vissy v. Hungary*, para. 73.
[353] *Klass v. Germany*, para. 55 and 56.
[354] *DRI*, para. 62.
[355] *Tele2 Sverige*, para. 120.
[356] *Zakharov v. Russia*, para. 233. Note that later in the judgment the ECtHR concedes that also another body can exercise the review function "as long as it is sufficiently independent from the executive", (para. 258).
[357] See: AG Opinion in *Tele2 Sverige*, para. 235 and 236.

Both the ECtHR and the CJEU acknowledge that there are instances where ex-ante review needs to be replaced with ex-post review.[358] For example, the ECtHR mentions that ex-ante authorisation "(…) is not an absolute requirement *per se*, because where there is extensive *post factum* judicial oversight, this may counterbalance the shortcomings of the authorisation".[359] While this seems to suggest that ex-post and ex-ante authorisations are interchangeable, the ECtHR has ruled on different occasions that in some cases ex-ante notification is necessary. For example, regarding surveillance of media, the ECtHR has emphasised the need for prior authorisation by an independent body, since *ex post facto* review cannot re-establish confidentiality.[360] Furthermore, in case of wide-ranging secret surveillance measures ex-ante review is also essential.[361] The CJEU mentions that ex-ante review should be the rule but that in case of urgency ex-post review can replace ex-ante review.[362]

Both courts also lay down several principles to analyse whether the oversight body qualifies as independent: (i) when adequate procedures of appointment are in place and independence of the members of the oversight committee can be guaranteed;[363] (ii) no external influence exists even if the members are functionally independent;[364] (iii) the level of access to all (including restricted) documents is ensured;[365] and (iv) public scrutiny is in place.[366]

(iv) Remedies

Both courts stress that remedies shall be available to all individuals that are under the remit of any public security measure and who believe their rights have been infringed. It needs to be acknowledged that the system of remedies is a multi-layered one consisting of administrative and judicial remedies.[367] According to CFREU independent supervisory authorities are tasked with reviewing whether personal data

[358] However, regarding surveillance of media, the ECtHR has emphasised the need for prior authorisation by an independent body, since *ex post facto* review cannot re-establish the confidentiality: see *Szabó and Vissy v. Hungary*, para. 77.
[359] *Szabó and Vissy v. Hungary*, para. 77. See also: *Kennedy v United Kingdom*, para. 167.
[360] *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, para. 101.
[361] *Szabó and Vissy v. Hungary*, para. 73.
[362] *Tele2 Sverige*, para. 120.
[363] *Zakharov v. Russia*, para. 278 and *Ekimdzhiev v. Bulgaria*, para. 85 and 87. See also: C-288/12 *Commission v. Hungary* of 8 April 2014, para. 51 including cited jurisprudence.
[364] C-614/10 *Commission v. Austria* of 16 October 2012, para. 42
[365] *Zakharov v. Russia*, para. 281.
[366] Ibid., para. 283.
[367] In relation to the EDPS, see: Hijmans, H. (2006) The European data protection supervisor: The institutions of the EC controlled by an independent authority. *Common Market Law Review*, vol. 43, pp. 1313-1343.

has been processed in accordance with the law.[368] Under this broad mandate, data subjects can lodge claims to the responsible DPA requesting access to data which has been collected concerning him or her, or to have it rectified.[369] The importance of DPAs as a provider of administrative remedies has been acknowledged in recent case law. Most prominently, in *Schrems* the applicant asked the Irish DPA to exercise its statutory powers by prohibit Facebook from transferring his data to the US. The DPA refused his request arguing that it was unfounded and that processing was lawful under the Safe Harbour Agreement. The CJEU held that a Commission Decision (such as the Safe Harbour Decision) cannot prevent persons from lodging a claim with a DPA. Furthermore, it can neither eliminate nor reduce powers expressly accorded to DPAs under Article 8 (3) CFREU to examine related claims.[370] If a DPA finds that a Commission Decision violates the rights to privacy or data protection of data subjects it must be able to engage in legal proceedings with the aim that the Commission Decision will be annulled.[371] The ultimate power to annul any measure remains with the CJEU.[372] The *Schrems* case stresses DPA powers to deal with claims lodged by data subjects and thus acknowledges their important role in offering effective remedies to individuals.

The CJEU also held that data shall be retained in the EU because "(…) the control, explicitly required by Article 8 (3) of the Charter, by an independent authority of compliance with the requirements of protection and security (…) is not fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data."[373] This idea was reiterated in *Tele2 Sverige* where it was held that national data retention regimes shall ensure storage within their territories to facilitate that national supervisory authorities can review that rights of individuals are adequately protected.[374] These examples show that DPAs are crucial for providing an appropriate

[368] Article 8 (2) and 8 (3) CFREU.
[369] Ibid.
[370] *Schrems*, para. 53.
[371] *Schrems*, para. 65.
[372] *Schrems*, para. 61.
[373] *DRI*, para. 68 and *Tele2 Sverige*, para. 123. See also: Case C-614/10 *Commission v Austria*, para. 37.
[374] *Tele2 Sverige*, para. 122.

remedy[375] provided that they have effective powers, especially access, and enjoy sufficient independence in the fulfilment of their duties.[376] The CJEU's emphasis on storage location also provides an interesting account of the Court's EU-centric approach since some companies may need to re-locate data to the EU.

If administrative remedies have been exhausted, a data subject should in light of Article 47 CFREU be able to access judicial remedies enabling him/her to challenge an adverse decision before national courts.[377] In respect to Articles 7 and 8 CFREU, the CJEU held that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."[378] ECtHR jurisprudence on targeted surveillance mentions that ex-post notification is important to assess whether effective judicial remedies are available since the secrecy of the measure makes it difficult for an individual to understand whether his/her rights were breached.[379] However, the ECtHR conceded that ex-post notification might not be necessary if "(…) any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications."[380] The CJEU has also expressed the view that those authorities that access data of an individual shall notify the person affected. However, the CJEU also mentioned that notification shall take place once it does not put the investigation at risk anymore.[381]

Neither CFREU nor ECHR explicitly require that a court needs to review data subject's claims.[382] However, "in a field where abuse is potentially so easy in

---

[375] Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, p.4

[376] The CJEU evaluated on several occasions on whether DPAs are sufficiently independent, see: C-518/07, *Commission v. Germany*, judgment of 9 March 2010; Case C-614/10 *Commission v Austria* of 16 October 2012 and Case C-288/12 *Commission v Hungary* of 8 April 2014.

[377] *Schrems*, para. 64.

[378] *Schrems*, para. 95.

[379] For instance, *Klass and Others v. Germany*, para. 57, and *Weber and Saravia v. Germany*, para. 135

[380] *Zakharov v. Russia*, para. 234.

[381] *Tele2 Sverige*, para. 121.

[382] Article 47 CFREU refers to 'tribunals' instead of 'courts'. However, in *Schrems* the Court seems to interpret 'tribunals' as equivalent to 'courts' (i.e. para. 64.). Article 13 ECHR refers to 'national authorities'. In *Klass and Others v. Germany*, the ECtHR clarified that the 'national authority' does not have to be a judicial authority as long as "the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy before it is effective" (para. 67).

individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.[383] In the case that claims are dealt with by a non-judicial authority, the ECtHR has high expectations. A body is deemed to offer sufficient remedies if it is: (i) an independent and impartial body with internal rules of procedure and consisting of experienced lawyers; (ii) it has access to relevant information including restricted documents; and (iii) it has the power to remedy non-compliance.[384]

(v) Data retention period

Data retention periods shall be strictly limited according to the usefulness of the data for the purposes pursued. The CJEU held that the retention period of data retention and access measures should differentiate between the different categories of data or between the persons concerned and their respective usefulness for the purposes of the objective pursued.[385] The CJEU also held that any data retention period "(…) must be based on objective criteria in order to ensure that it is limited to what is strictly necessary."[386] Ultimately, the CJEU mentions that irreversible destruction of the data at the end of the prescribed data retention period shall be ensured.[387] The ECtHR also laid down that the duration of interception shall be limited. For example, laws allowing for a 90 days retention period with the possibility of renewal need to lay down how often the period can be renewed otherwise this provision is an 'element prone to abuse'.[388] On another occasion, a six months retention period was considered proportionate but the law has to establish that the data has to be destroyed immediately as soon as it is not relevant anymore to the purpose for which it have been obtained.[389] In *Tele2 Sverige*, the AG refers to the ECtHR ruling in *Zakharov v. Russia* mentioning that any data shall be destroyed once it is no longer strictly necessary in the fight against serious crime.[390] Furthermore, immediate deletion of

[383] *Klass and Others v. Germany*, para. 56.
[384] *Kennedy v. United Kingdom*, para.167
[385] *DRI*, para. 63; AG Opinion in *Tele 2 Sverige*, para. 242.
[386] *DRI*, para. 64; AG Opinion in *Tele 2 Sverige*, para. 242.
[387] *DRI*, para. 67.
[388] *Szabó and Vissy v. Hungary*, para. 74.
[389] *Zakharov v. Russia*, para. 255. See also: *Klass and Others v. Germany*, para. 52; or *Kennedy v. United Kingdom*, para 162.
[390] AG Opinion in *Tele 2 Sverige*, para. 243.

unnecessary data ought to apply both to data retained by service providers and data that has been accessed by state authorities.[391]

(vi) Data security

To ensure effective security of data several aspects have been identified by the CJEU. An adequate data security strategy needs to account for: (i) the vast quantity of data whose retention is required; (ii) the sensitivity of the data; (iii) the risk of unlawful access to data requiring data integrity and confidentiality.[392] Furthermore, economic considerations shall not play a role when companies determine the level of security standards. This reasoning is derived from Article 4 (1) of the e-privacy Directive. It stipulates that when establishing data security standards, electronic communications service providers must take into account the state of the art and the *cost* of implementation. The level of security of adopted measures shall be appropriate to the risk presented.[393] Since the CJEU evaluated the risk as extremely high, that costs shall not only be sub-ordinate but play no role at all. This reasoning can however be criticised. As argued earlier in this thesis, the objective of data protection is not solely to guard the privacy of individuals but also to ensure economic prosperity in the internal market. Furthermore, Directive 95/46/EC stipulates that "[h]aving regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.[394] In addition Article 52 (1) CFREU also argues that limitations to a right are possible if it is proportionate and meets a general interest. Respectively, Article 3 (3) TEU lists a highly competitive social market economy as a general interest within the EU and as such it seems logical to regard data security considerations in the context of economic feasibility.

(vii) Onward transfer

Without more detailed elaborations, the ECtHR held that precautions have to be taken when data is transferred to third parties. This safeguard stems from the *Kruslin* and *Huvig v. France* cases where French law was deemed to not provide sufficient

[391] Ibid.
[392] *DRI*, para. 66. See also also: *Tele2 Sverige*, para. 122.
[393] Article 4 (1) e-privacy Directive; *Tele2 Sverige*, para. 122.
[394] Article 17, DPD.

safeguards against abuse of power when court material was sent to other parties.[395] While this finding refers to situations where data was communicated for purposes of court proceedings, in other cases this doctrine was phrased more generally. For instance, in *Weber and Saravia v. Germany* the ECtHR held that surveillance measures need to include precautions when data is transferred to third parties.[396] The latter does then also apply when data is for instance shared between different law enforcement or intelligence agencies. More recently, the ECtHR also held that due to governments' widespread practices of transferring and sharing intelligence, remedial measures and external supervision gained importance.[397]

3.2 The increasing role of the CJEU due to institutional reasons

As shown in 3.1, CJEU and ECtHR jurisprudence lays down similar criteria to assess the legality of data retention and access regimes for public security purposes. The interaction between the two courts is marked by judicial dialogue and mutual agreement on which safeguards need to be in place.

Apart from the fairly congruent level of protection granted to privacy and data protection, the CJEU seems to have become increasingly important from an institutional perspective. The CJEU's emancipation on fundamental rights matters -as evidenced in particular in *Digital Rights Ireland, Tele2 Sverige* and *Schrems* – can be directly linked to the fact that the Charter of Fundamental Rights acquired *valeur juridique*[398] and thus provides the CJEU with a formal reference point when adjudicating on privacy and data protection.[399] In an empirical study involving interviews with CJEU staff it was confirmed that the starting point of any legal assessment is now commonly the CFREU since it is the "most up-to-date fundamental rights catalogue."[400] Furthermore, it has also been confirmed that post-Lisbon formal

[395] *Huvig v. France*, para. 34; *Kruslin v France*, para. 35.
[396] *Weber and Saravia v. Germany*, para. 95.
[397] *Szábo and Vissy v. Hungrary*, para. 78.
[398] Douglas-Scott, S. (2011). The European Union and Human Rights After the Treaty of Lisbon. *Human Rights Law Review*, vol. 11, p. 645.
[399] It has been argued that CFREU provides a 'clear reference text for the hermeneutical activity of the EU courts', see: Fabbrini, F. (2015) The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court, *iCourts Working Paper Series*, no. 15, p. 9.
[400] At the same time relevant ECtHR case law is also considered but less extensively. See: Krommendijk, J. (2015), op. cit., p. 15.

references to ECtHR jurisprudence decreased.[401] However, a decrease in formal references does not mean that the CJEU is not informally inspired by ECtHR jurisprudence. The adoption of CFREU and the resulting fundamental rights mandate of CJEU increased CJEU's role vis-à-vis the ECtHR in several ways.

First, the CJEU became a more attractive venue to raise fundamental rights concerns. This is related to the fact that judgements will be delivered much quicker than it is usually the case in regard to the ECtHR. The reason for the inertia of the ECtHR is its extreme case overload resulting from the way the ECtHR operates as well as the vast number of applications it receives.[402] While being more efficient, the CJEU's level of scrutiny in respect to data protection and privacy, is equivalent if not higher compared to the ECtHR. In earlier days this would not have been conceivable as the CJEU was mainly an 'economic court' where fundamental rights played a subordinate role.[403]

Second, the EU institutional framework provides more opportunities for the CJEU to adjudicate, namely via requests from EU institutional actors. In this way, it will potentially have more chances to rule on fundamental rights issues. For example, as shown in the case study chapters especially the strategic use of the CJEU by EU institutional actors triggers an increased relevance of the CJEU in respect to data retention and access measures in the public security context.[404]

Third, another factor relates to the different focus of CJEU rulings. While ECtHR cases exclusively focus on ensuring the protection of individual rights in regard to very specific national legislation, the CJEU takes a more holistic approach as its main aim is to ensure uniformity, primacy and effectiveness of EU law. Hence,

---

[401] See: De Búrca, G. (2013). After the EU Charter of Fundamental Rights: The Court of Justice as a human rights adjudicator. *Maastricht Journal of European and Comparative Law*, vol. 20 (2), pp. 168-184.

[402] For instance, in 2011 around 47000 applications have been deemed inadmissible while 1500 cases were decided by the Court and 54000 cases are still pending. See: Bradley, A. (2013) Introduction: The need for both national and international protection of human rights – the European challenge. In: Flogaitis, S; Zwart, T; and Fraser, J. (eds), *The European Court of Human Rights and its Discontents*. Edward Elgar, p.4.

[403] See for example: Coppel, J. and O'Neill (1992) The European Court of Justice: Taking Rights Seriously? *Common Market Law Review*, vol. 29, p. 669. For an assessment of the early failed attempts of infusing a fundamental rights dimension into the rationale of the EU, see: De Burca, G. (2011b). The Road not taken: The European Union as a Global Human Rights Actor, *American Journal of International Law*, vol. 105, p. 649.

[404] In this thesis: Chapter 4 (section 2.2.2); Chapter 5 (section 2.2); and Chapter 6 (section 2.2).

it has a broader reach and its assessments are more general by scrutinising fundamental rights in the context of economic considerations.[405]

A fourth institutional aspect favouring the increasing CJEU role relates to the spill-over effect of judgments. While recent judgments have had a substantial impact on the level of protection granted to privacy and data protection the CJEU often failed to provide an in-depth explanation on how and why certain conclusions have been reached.[406] This in turn leads to uncertainty on the implications of judgments and thus to follow-up requests.[407] One explanation for the CJEU's tendency to deliver vague judgments relates to the set-up of the Court not allowing for dissenting opinions. The need to reconcile diverging opinions can thus negatively affect the quality and depth of the rulings.[408]

Last, the increasing role of the CJEU vis-à-vis the ECtHR is related to a tendency of European integration in respect to public security measures. If more national measures result from the transposition of EU law, the influence of the ECtHR will shrink - at least until the EU accedes to the ECHR. The ECtHR has conditionally accepted the prevalence of the CJEU when fundamental rights concerns arise from national laws transposing EU law. In *Bosphorus v. Ireland* the ECtHR acknowledged the self-sufficiency of the EU legal system as long as the level of protection is at least equivalent to that of the Convention.[409] While leaving the backdoor open for ruling on national laws transposing EU law, the ECtHR essentially accepted the CJEU's exclusive role in adjudicating on fundamental rights within the EU context.[410] Taken together, the institutionalisation of privacy and data protection through CFREU in conjunction with the structural set-up of the two courts potentially grants the CJEU more opportunities to pave the way in respect to fundamental rights in respect to privacy and data protection.

---

[405] Costa, J.P. (2011) On the legitimacy of the European Court of Human Rights' judgments. *European Constitutional Law Review*, vol. 7, pp. 173-182.
[406] See Chapters 4, 5 and 6 of this thesis.
[407] E.g. *Tele2 Sverige* can be considered a follow-up of *DRI*.
[408] This was pointed out in a lecture of a CJEU judge at the Annual Lecture of the Queen Mary University of London Criminal Justice Centre held in London, 24th of February 2017.
[409] *Bosphorus v Ireland*, Application no 45036/98 of 30 June 2005, para. 155. See also: Lavranos, N. (2008). Towards a Solange-Method between International Courts and Tribunals? In: Broude, T. & Shany, Y. (eds.) *The shifting Allocation of Authority in International Law: Considering Souvereignty, Supremacy and Substiarity*. Hart Publishing.
[410] Note however that on an earlier occasion the ECtHR ascribed itself more competences in respect to EU law. In *Matthews v UK* Application No. 24833/94 of 18 February 1999, the ECtHR felt that it cannot rule on EC acts directly. However, if Member State responsibility derives from EU law the Convention applies.

Turning to the causes for further EU integration in regard to public security measures, it is worth pointing out that the abolition of the pillar structure post-Lisbon as well as recent terror activities on EU soil facilitated the adoption of public security measures at EU level. As elaborated further in the case study chapters the ordinary legislation-making procedure applicable to AFSJ led to increased consensus between the different EU institutional actors which enables swift adoption of relevant measures.[411] The CJEU can also be seen as a catalyst of EU integration.[412] For example, in *Tele2 Sverige* the CJEU argued that not only retention of data for public security purposes but also access to this data falls under Article 15 (1) of the e-privacy Directive.[413] The CJEU admitted that there is a fine line between measures falling beyond and within the scope of EU law. However, since data retention is explicitly mentioned in Article 15 (1) of the e-privacy Directive it is inevitable that data retention falls within the scope of EU law. Consequently any further national or EU-wide regulation of data retention and access will be under the remit of EU law and thus within the CJEU's jurisdiction. This is a good example of the CJEU's attempt to close legal loopholes in the protection of individuals, which may arise from the national security exception and Member States' attempts to make recourse to it.[414] It also shows the CJEU's impact on enhancing EU integration and thus grants less importance to Member States' sovereignty concerns. In *DRI*, AG Cruz Villalón justified the integration bias by mentioning that if EU legislation has a 'creating effect' in the sense that it imposes obligations constituting serious interference with fundamental rights, it cannot be left entirely to the Member States to define the guarantees capable of justifying that interference.[415] Consequently, by ruling on the reach of EU law and by making more detailed safeguards at EU level a precondition for legality of data retention, any future regulatory efforts on EU level imply increased harmonisation among Member States. Applied more generally, this tendency of EU integration implies that the remit of the CJEU is increasing while the

[411] See in this thesis: Chapter 4 (section 2); Chapter 5 (section 2); Chapter 6 (section 2).
[412] See for example: Stone Sweet, A. (2003) European Integration and the Legal System. In: Börzel, T. and Cichowski, R.A. (eds.) *The State of the European Union: Law, Politics, and Society*. Oxford University Press, chapter 2.
[413] *Tele2 Sverige,* paras. 72 and 73. In paras. 78 and 79 the CJEU held that 'access' and 'retention' are intrinsically linked implying that the former also falls within Article 15 (1) of the e-privacy Directive.
[414] It also shows that while the introduction of Article 15 (1) in 2006 was an attempt of Member States to legitimise EU-wide data retention (see more details in Chapter 4) it paradoxically enabled the CJEU to rule several years later on its illegality both on EU and national levels. This illustrates how strategic preferences of some actors can inadvertently translate into strategic preferences of another.
[415] AG Opinion in *DRI*, para. 120.

ECtHR is still not able to rule on EU legislation. This situation will obviously change if/when the EU accedes to the ECHR.[416]

3.3 Summary

As shown the ECtHR and the CJEU share to a large extent the same views on how to protect privacy and data protection in the public security context. Standards and procedural safeguards mentioned by both courts largely coincide and direct and indirect judicial dialogue is taking place. It is interesting to note that initially the ECtHR was the trendsetter by introducing general principles and safeguards. While these standards still play an important role on a substantial level, CJEU jurisprudence is becoming more relevant due to institutional reasons. As has been shown the adoption of the CFREU and the resulting emancipation of the CJEU on fundamental rights triggers a shifting focus on CJEU jurisprudence in several ways. On the one hand the architecture of the CJEU leads to more efficiency in dealing with fundamental rights. On the other hand, the communitarisation of AFSJ post-Lisbon shifts a substantial part of relevant national activities under the remit of EU law and thus the CJEU. The prevalence of the CJEU triggered by the communitarisation of AFSJ might become less relevant once the EU accedes to the ECHR because the ECtHR will then be able to rule on EU legislation. Nonetheless, the more agile architecture of the CJEU would then still support a continuous prominent role for the CJEU vis-à-vis the ECtHR.

4. The institutionalisation of privacy and data protection in AFSJ - A case of incremental EU integration?

4.1 EU competences in AFSJ: An example of incremental EU integration

Since the early days of EU integration, the idea behind coordinating AFSJ on the EU level has been to react to the increased threat of cross-border criminal activities due to the facilitation of free movement. Despite of the need to harmonise AFSJ, European integration in those matters has been slow and non-linear.

[416] Note that at political and academic levels, it has been suggested that new accession negotiations are not likely to happen in the near future. See: Fabbrini, F. & Larik, J. (2016). The Past, Present, and Future of the Relation between the European Court of Human Rights. *Yearbook of European Law,* pp. 1-35. For an assessment on a possible route to accession, see: Krenn, C. (2015) Autonomy and Effectiveness as Common Concerns: A Path to ECHR Accession After Opinion 2/13, *German Law Journal*, vol. 16, p. 147.

The disjointedness is a result of contradictory forces marked by disagreement on the fundamental question as to whether legislation should be adopted on an 'intergovernmental basis' where all powers are reserved for national governments or on a 'supranational basis' where power is assumed by EU institutional actors. The persistence of intergovernmental considerations can be explained with the perception that security and criminal justice are at the 'heartland of Member State authority'.[417] The occasional trump of supranational considerations can be ascribed to pragmatic considerations on the efficiency and effectiveness of centralised efforts. For example, after 9/11 and the London and Madrid bombings authorities became increasingly aware of the benefits of cooperation. Thus, these instances can be considered to be '*critical junctures*' which enable the institutional framework to incrementally move from previous intergovernmental practices to more supranational practices.

While there have been informal cooperation mechanisms on AFSJ matters since the early years of EU integration[418] this was only formalised with the Maastricht Treaty. Interestingly, Title VI 'Provisions on Cooperation in the Fields of Justice and Home Affairs' did not mention that the purpose of cooperation is maintaining and safeguarding security in the EU. Instead it is stipulated that "[f]or the purposes of achieving the objectives of the Union, in particular the free movement of persons, and without prejudice to the powers of the European Community, Member States shall regard the following areas as matters of common interest."[419] The article goes then on by determining that issues such as criminal judicial cooperation and police cooperation fall under JHA and thus under the third pillar.[420] There are four main aspects that differentiate policies adopted under the first and the third pillar. First, the power constellation between the EU institutional actors differs in terms of right of initiative and the applicable legislation-making procedure.[421] Second, the legal instruments differ from the first to the third pillar.[422] Third, while first pillar measures had direct effect implying that they could be directly invoked in front of a national

[417] Anderson, D. & Eeckhout, P. (2011) Series Editors' Foreword. In: Peers, S. (2011). *Justice and Home Affairs Law*, OUP, pp.vii-viii.
[418] For example in the 1970s the TREVI Group was a network of law enforcement officials who discussed on an informal basis counter-terror issues. See: Mitsilegas, V. (2009) *EU Criminal Law*. Hart Publishing, p. 6.
[419] Article K.1 TEU, Maastricht Treaty.
[420] Note that all JHA issues are grouped under Title VI apart from certain visa related issued.
[421] This is explained in more detail in Chapters 4, 5 and 6 of this thesis.
[422] The first pillar is regulated via Directives, Regulations and Decisions, (former Article 249 EC) while third pillar topics are regulated via Framework Decisions, Common Positions, Conventions (former Article 34 TEU).

court, third pillar measures do not have this same effect.[423] Fourth, the Court of Justice has the competence to adjudicate on first pillar matters while its jurisdiction is limited in respect to the third pillar.[424] As explained further in the case study chapters, the categorisation of a subject matter under one of the pillars was not always clear-cut. An example is the increasing importance of data held by the private sector for AFSJ purposes which blurs the boundary between internal market (first pillar) and security (third pillar) concerns. Besides the differences between the first and third pillar it is also necessary to point out that another important field that partially overlaps with AFSJ falls -since the early days of EU integration up until today- beyond the scope of EU action. Article K2 (2) of the TEU mentions that all provisions on cooperation in AFSJ "(…) shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."[425]

The Treaty of Amsterdam introduced the policy field of the Area of Freedom Security and Justice and replaced earlier references to Justice and Home Affairs.[426] By adhering to the pillar tradition of the Maastricht Treaty, the Amsterdam Treaty aimed to clarify the objectives and legal effects of AFSJ cooperation. Furthermore, by re-phrasing JHA into AFSJ the security dimension was more clearly expressed in contrast to the Maastricht Treaty. Still caught in the old intergovernmental/supranational debate, Member States reached a complex agreement where on the one hand the Schengen acquis was adopted by allowing opt-outs to the UK, Ireland and Denmark while on the other hand issues related to migration were shifted from the third to the first pillar.[427] Besides that, other relevant changes include that the EP had to be consulted before the Council could adopt a third pillar measure.[428] Furthermore, Conventions ceased to exist under the Amsterdam Treaty meaning that Framework Decisions,[429] Decisions,[430] and Common Positions[431] were

[423] Peers, S. (2011). *EU Justice and Home Affairs Law*, OUP, p. 8.
[424] Ibid.
[425] Post-Lisbon this is regulated via Article 4 (2) TEU and Article 72 TFEU stipulating that responsibility for internal security remains for Member States. According to the AG Opinion in C-145/09 *Land of Baden-Württemberg v Panagiotis Tsakouridis*, judgment of 23 November 2010, the terms 'internal security' and 'national security' can be used interchangeably and they cover both external and internal security of a state.
[426] Note, however, that the thesis always refers to AFSJ for the sake of consistency.
[427] See Articles 61-69 TEC.
[428] Article 39 TEU.
[429] Article 34 (2) (b) TEU.
[430] Article 34 (2) (c) TEU.

the three legislative measures to be adopted in the third pillar. It is also worth pointing out that the jurisdiction of CJEU was expanded post-Amsterdam by allowing the Court jurisdiction over the validity and interpretation of decisions and framework decisions.[432] In addition to the formal Treaty amendments, the European Council started to adopt action plans and policy programmes as follow up to its regular meetings to set out broad objectives related to specific JHA matters.[433] In addition, the European Commission decided to found a Directorate General for Justice and Home Affairs (DG JHA) in 2000. This means that although formally Member States were still in full control, the codification of political objectives via formal programmes and the foundation of DG JHA created new 'supranational spaces' which contributes to incremental EU integration.

The Lisbon Treaty was a major supranational push for AFSJ cooperation mainly due to the abolition of the pillar structure. First of all, the abolition of the pillar structure led to the consolidation of all AFSJ matters under on single title (Title V) of the TFEU.[434] There are various different protocols on AFSJ matters attached to the TFEU mainly relating to internal border controls and Schengen, and to opt-outs regarding UK, Ireland and Denmark. These protocols are remnants from the Treaty of Amsterdam but almost all of them have been substantially amended with the Lisbon Treaty.[435] Other protocols relate to the CJEU's jurisdiction over AFSJ measures.[436]

Second, the legislation-making procedure changed significantly. While previously many AFSJ matters were still subject to unanimity voting, post-Lisbon most AFSJ subjects –such as most aspects of criminal law and police cooperation[437] are decided under the ordinary legislative procedure.[438] In some cases QMV is applied but the Parliament is only consulted, such as the adoption of measures on

---

[431] Article 34 TEU.
[432] Article 35 TEU. It needs to be noted that not all Member States opted in on granting the CJEU third pillar jurisdiction.
[433] Multiple action plans have been adopted since the entry into force of the Amsterdam Treaty and are usually named after the place in which they were concluded: Vienna Action Plan (1998), Tampere programme (1999), Laeken conclusions (2001), Hague programme (2004), Stockholm programme (2010).
[434] Title V, TFEU.
[435] Peers, S. (2011) Mission Accomplished? EU Justice And Home Affairs Law after the Treaty of Lisbon. *Common Market Law Review* vol. 48, pp. 661–693.
[436] Protocol on transitional provisions annexed to the Treaty of Lisbon, Articles 9 and 10.
[437] Articles 79, 82–85, 87 and 88 TFEU.
[438] Article 294 TFEU.

administrative cooperation in the fields of policing and criminal law.[439] In few cases a 'special legislative procedure' instead of the ordinary legislative procedure is applied where unanimity still applies and the Parliament is only consulted. Among other fields this is used when sensitive issues on policing and criminal law are at stake.[440] The general shift to QMV can be assessed as a positive development as it leads to more accountability and transparency. Furthermore, it provides more clarity in cases where AFSJ matters cannot sharply be distinguished from internal market aspects (as is the case in all three case study regimes). Nevertheless, the EU competence has also been limited more narrowly to certain crimes and types of criminal procedure that have a cross-border element.[441] In other words, the ambitious goal mentioned in Article 3 (2) TEU[442] is limited by Article 67 TFEU and subsequently also by different specific provisions.[443] Furthermore, exceptions to the ordinary legislative procedure and the introduction of so-called 'emergency brakes' show that intergovernmental elements persisted and may lead to obstacles in harmonisation efforts.[444]

Third, the CJEU's competences were extended by the removal of restrictions in relation to migration, asylum and in regard to the former third pillar. There is only one exception in regard to policing and criminal law where the Court cannot "review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."[445] In addition, there are some transitional rules as regards pre-Lisbon Third Pillar measures.[446]

The above-mentioned changes introduced with the Lisbon Treaty tackled the lack of accountability and transparency and thus the approach to AFSJ can be

[439] Article 74 TFEU.
[440] Articles 87 (3) and 89 TFEU.
[441] Peers, S. (2011).
[442] Article 3 (2) TEU: "The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which free movement of person is ensured in conjunction with appropriate measures with respect to (…) the prevention and combatting of crime".
[443] Wessel, R., Marin, L. & Matera, C. (2011). The External Dimension of the EU's Area of Freedom, Security and Justice. In: Eckes, C & Konstadinidis, T. (eds.) (2011) *Crime within the Area of Freedom, Security and Justice*. Cambridge University Press, p. 275.
[444] Articles 82(3) and 83(3) TFEU.
[445] Article 276 TFEU.
[446] See: TFEU Protocol on transitional provisions.

regarded as more rights-based, open and participatory.[447] Due to these positive developments, the Lisbon Treaty provided the pre-conditions for a new paradigm of European criminal justice where fundamental rights instead of security is at its core.[448] At the same time it has to be noted that: (i) some intergovernmental features remain post-Lisbon; (ii) there is still a legacy of instruments that have been adopted under older Treaty provisions where 'old standards' live on in the post-Lisbon era; (iii) the effectiveness of a more 'rights-based' AFSJ framework is also determined by policy priorities and political realities.[449] While a 'rights-based AFSJ' has often been stressed[450] this has been put under pressure by several terror attacks on European soil as well as the refugee crisis.[451] In this context, political realities might trump the fundamental rights discourse as exemplified by the adoption of the PNR Directive.[452]

Taken together it has been shown that AFSJ moved incrementally towards a 'normalised' policy field. The incremental nature of these changes was both event-driven and based on pragmatic considerations. Furthermore, the abolition of the pillar structure – an inherent pre-Lisbon feature- was a key driver for change.[453] Nonetheless, some institutional intricacies persist showing the co-existence of old and new paths.

4.2 Regulatory framework of data protection and privacy in AFSJ: Persisting fragmentation?

The main data protection instruments that evolved in the EU in the late 90s explicitly excluded privacy and data protection in AFSJ matters from its remit.[454] Only after 9/11 was the importance of regulating data protection in this field acknowledged. The result was a patchwork of data protection rules enshrined in multiple different

[447] Konstakopoulou, D. (2010) An Open and Secure Europe? Fixity and Fissures in the Area of Freedom, Security and Justice After Lisbon and Stockholm, *European Security*, vol. 19 (2), pp. 151-167.
[448] See: Mitsilegas, V. (2016) *EU Criminal Law after Lisbon. Rights, Trust and The Transformation of Justice in Europe*. Hart Publishing.
[449] Konstakopoulou, D. (2010) op. cit.
[450] The Stockholm Programme, p. 18 and European Council Conclusions from the meeting on 26/27 of June 2014. *EUCO 79/14*, 27 June 2014, Brussels.
[451] Attacks have been carried out in France, Belgium and more recently Germany.
[452] Further debated in Chapter 6 of this thesis.
[453] As aligned with the theoretical reasons for institutional change as mentioned in Chapter 2, see: Mahoney, J. & Thelen, K. (2010) A Theory of Gradual Institutional Change. In: Mahoney, J. & Thelen, K. (eds.) *Explaining Institutional Change: Ambiguity, Agency, and Power*. Cambridge University Press
[454] See: Article 3 (2) DPD, and Article 1 (3) of the e-privacy Directive.

regulatory instruments of varying legal status and binding power.[455] For instance, distinct data protection regimes were established in the Europol, Schengen and Eurojust, Prüm, PNR and SWIFT Agreements.[456] These instruments are only partially inspired by basic data protection principles and thus this means in each case the setting-up of separate regimes.[457] Furthermore, due to the blurred boundary between the first and third pillar the DPD was occasionally applicable when processing was carried out by companies.[458] Only in 2008 a first attempt to overcome this mosaic approach was made by adopting the 2008 Framework Decision.[459] While aiming to replicate the provisions of the DPD for the AFSJ sector, it only had limited effect. For instance, it did not affect any of the separate data protection regimes mentioned earlier and its provisions were vague and allowed numerous exceptions. Furthermore, it exclusively applied to trans-border data flows between Member States and thus did not establish EU-wide standards.[460]

The Lisbon Treaty and the abolition of the pillar structure provided the means for a new attempt to establish an AFSJ data protection regime. The rationale for amending the pre-Lisbon data protection regime was not only to strengthen its relevance for AFSJ but also to account for technological developments.[461] The Data Protection Directive for police and criminal justice authorities was adopted in 2016 after several years of negotiations.[462] The Directive applies to:

"[t]he processing of personal data by competent authorities for the purposes of the

---

[455] O'Neill, M. (2010) The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar, *Journal of Contemporary European Research*, vol. 6 (2), pp. 211 – 235.
[456] Council Decision of 6 April 2009 establishing the European Police Office, *OJ 2009, L-121/37*; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of second generation Schengen Information System, *OJ 2007, L-205/63*; Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, *OJ 2002, L-63/1*; Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime *OJ 2008 L 210* (Prüm Decision), PNR and SWIFT Agreements.
[457] Böhm, F. (2012), op. cit.
[458] See for instance in the case of the Data Retention Directive.
[459] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ 2008 L350/60*.
[460] De Hert, P. and Papakonstantinou, V. (2015) Data Protection: The EU Institutions' Battle over Data Processing vs. Individual Rights'. In: Trauner, F. and Ripoll Servent, A. (eds) *Policy Change in the Area of Freedom, Security and Justice: How EU Institutions Matter*. Routledge, p. 181.
[461] See for instance: Articles 4 (5), 9 (1) and 20 GDPR.
[462] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. *OJ 2016 L 119.*

> prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, [and it] should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction."[463]

The Directive applies to all data processing in the law enforcement context. Therefore, the main achievement of the Directive in contrast to the Framework Decision is that it is also applicable if processing happens at national level and not only if data is transferred across borders. Unchanged is however that it does not apply to: aspects that fall outside the scope of EU law;[464] data processing carried out by Union bodies and agencies;[465] and data processing which is subject to specific regimes.[466] On the latter point it needs to be mentioned that the Directive does require that data processing with third countries is based on an adequacy finding.[467] However, agreements that already exist on exchange of data in the law enforcement field are unaffected by the Directive.[468] In terms of substance, the Directive follows a similar structure as the GDPR and includes the same data protection principles. Nevertheless, the Directive accounts for the special nature of data processing in the criminal law context and challenges brought about by new technological developments which infuses more flexibility.[469] For example, the right to information and access cannot be applied as strictly as under the GDPR since this would render targeted surveillance meaningless. Accordingly, the provisions on access and information are subject to certain limitations and flexibility.[470] Furthermore, strict requirements on data quality may not be realistic since data in the law enforcement context is not only derived from facts but in some cases from unconfirmed intelligence. Respectively, Article 7 points out that the latter two categories of data need to be distinguished and treated differently.[471]

As mentioned earlier, also the DPD was subject to major revisions in 2016 leading to the adoption of the GDPR. Similarly to the DPD, the Regulation does not

[463] Ibid., Recital 34.
[464] Ibid., Article 2 (3) (a).
[465] Ibid., Article 2 (3) (b).
[466] Ibid., Article 60.
[467] Ibid., Chapter V.
[468] Ibid., Article 60.
[469] Ibid., Recitals 1 and 10.
[470] Ibid., Chapter III.
[471] Ibid., Article 7.

apply to AFSJ processing.[472] However, this exemption is not always clear-cut where processing is initially executed by private companies. For instance, in the annulled data retention directive it was stipulated that the DPD is 'fully applicable' to the data retained in accordance with the data retention directive since access to data was not subject to the Directive.[473] Furthermore, also in the recently adopted PNR Directive it is mentioned that "this Directive is without prejudice to the applicability of Directive 95/46/EC of the European Parliament and of the Council to the processing of personal data by air carriers (…)."[474] However, as soon as data is transferred to the competent authorities (i.e. PIU), the processing "should be subject to a standard of protection of personal data under national law in line with Council Framework Decision 2008/977/JHA"[475] These examples show that the provisions of the GDPR may still partially apply to data processing operations for public security purposes as long as the processing is executed by private entities.

Taken together, there have been attempts to elevate data protection and privacy in AFSJ to a less fragmented or more 'normalised' policy area. However, due to the only recent changes resulting in the GDPR and the Police and Criminal Justice Data Protection Directive it is difficult to conclude whether 'normalisation' has indeed happened. The new data protection package has the potential to create a more uniform framework while some initial uncertainties are still likely to persist, particularly since various autonomous regimes continue to exist.

5. The institutionalisation of EU-US relations on privacy and data protection in AFSJ

5.1 Rationale and EU competence in the external dimension of AFSJ

While AFSJ cooperation with third states or international organisations has been possible since the Treaty of Amsterdam, no indication on the specific external objectives in AFSJ were stated.[476] Only during the 2000 Feira Council meeting it was

[472] Article 2 (2) (d), GDPR.
[473] Recital 15, DRD.
[474] Article 13 (3), PNR Directive.
[475] Recital 27, PNR Directive.
[476] Gilmore, W, Fletcher, M., & Lööf, R. (2008). *EU Criminal Law and Justice.* Elgar European Law. Edward Elgar Publishing.

mentioned that the primary purpose of the external dimension of EU criminal matters is the contribution to internal AFSJ matters and not an objective in itself.[477] Some scholars have called this reasoning the 'internal-external security nexus'.[478] This concept implies that in a globalised world, security on EU territory cannot be regarded in isolation from external threats and thus requires measures beyond the EU level. While this realisation did not mark the beginning of a comprehensive 'global AFSJ strategy', it provided a rationale for acting externally.

Before the adoption of the Lisbon Treaty, it was debatable whether the EU was at all able to conclude international agreements since no treaty provision expressly conferred legal personality on the EU. In addition, no treaty provisions provided the EU competences to cooperate with third states on AFSJ matters either.[479] However, this was relaxed with the ratification of the Amsterdam Treaty in 1999.

Article 24 TEU within the CFSP Title stipulated that if necessary international agreements can be concluded with third states or international organisations. Respectively, the Council may authorise the Presidency, assisted by the Commission as appropriate. Article 24 TEU could be read in conjunction with Article 38 TEU of the AFSJ Title stating that "[a]greements referred to in Article 24 may cover matters falling under this title."[480] The combination of these two articles was frequently used as the legal basis for agreements involving the third pillar.[481] However, Article 24 (5) TEU stipulates that "[n]o agreement shall be binding on a Member State whose representative in the Council states that it has to comply with the requirements of its own constitutional procedure; the other members of the Council may agree that the agreement shall nevertheless apply provisionally."[482] This provision was in many cases invoked by Member States leading to complications and delays in the entry into

[477] European Union Priorities and Objectives for External Relations in the Field of Justice and Home Affairs. Report of the Council submitted to the European Council. *Council Doc. 7653/00*, 6 June 2000.
[478] Smith, K. (2003). *European Union foreign policy in a changing world*. Cambridge: Polity Press; Wolff, N. & Mounier, G. (2009) The External Dimension of Justice and Home Affairs: A Different Security Agenda for the EU? *Journal of European Integration*, vol. 31 (1), pp. 9-23; Eriksson, J. & Rhinard, M. (2009) The Internal External Security Nexus: Notes on an Emerging Research Agenda *Cooperation and Conflict*, vol. 44 (3) pp. 243–267.
[479] Note that the only international aspect of AFSJ was that Common Positions within international organisations and at international conferences are defended (see Article K.5.).
[480] Article 38 TEU. Note that under the Amsterdam Treaty, AFSJ matters were labelled: "police and judicial cooperation in criminal matters".
[481] For example: Wessel, R. A. (2010) Cross-Pillar Mixity: Combining Competences in the Conclusion of EU International Agreements. In: Hillion, C. and Koutrakos, P. (eds.) *Mixed Agreements in EU Law Revisited*. Hart Publishing.
[482] Article 24 (5) TEU.

force of agreements.[483] When the Lisbon Treaty entered into force several third pillar Agreements were still provisional due to Article 24 (5) TEU. Since new rules apply immediately to ongoing legislative measures if not otherwise specified, all provisional Agreements had to be re-negotiated under post-Lisbon procedures.[484] As shown in Chapters 5 and 6, this was the case for the PNR and SWIFT Agreements.

Another pre-Lisbon complexity refers to situations where the legal basis of a measure cannot be clearly assigned to one of the three pillars. This resulted in situations where it was not clear which negotiation procedure should be applied. In those cases the CJEU was able to play a significant role in AFSJ external relations. A prominent case on cross-pillarisation in external AFSJ matters concerned the PNR case where the CJEU held that the Agreement was based wrongly on a first pillar legal basis instead of a third pillar basis.[485] A more detailed elaboration of this case follows later in the thesis.[486]

Post-Lisbon, the pillar structure was abolished leading to the unification of former Title IV TEC and former Title VI TEU under the heading 'Title V AFSJ'. The result was that international agreements in AFSJ have the same legal basis and are concluded under the same procedures as other policy fields. While no explicit reference is made to a Union competence in external AFSJ matters, a declaration attached to the TFEU details that treaty-making competence of the EU on AFSJ matters is possible in areas covered by chapters 3, 4 and 5 of Title V as long as such agreements comply with Union law.[487]

The Lisbon Treaty also brought several other advantages when international agreements are concluded in the AFSJ area. First of all, the consolidation of the AFSJ policy field leads to increased consistency in regard to its external dimension. Furthermore, since Article 216 (2) TFEU stipulates that agreements need to be binding on institutions and Member States, 'vertical' consistency among different

[483] For example, in regard to the EU-US PNR Agreement: Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) – Declarations made in accordance with Article 24(5) TEU - State of Play, *Council doc 5311/1/09*, 19 March 2009.
[484] See: Peers, S. (2011), op. cit., p. 133.
[485] Joined Cases C-317/04 and C-318/04 *European Parliament v Council*, judgment of 30 May 2006. More details, see: Cremona, M. (2008) EU External Action in the JHA Domain: A Legal Perspective. *EUI Working Papers, LAW No. 2008/24*, p. 17.
[486] Chapter 6 of this thesis.
[487] Declaration on Article 218 of the Treaty on the Functioning of the European Union concerning the negotiation and conclusion of international agreements by Member States relating to the area of freedom, security and justice.

levels of government is achieved.[488] Moreover, the procedure laid down in Articles 218 (2) and (3) TFEU in conjunction with the end of the division between the EC and EU will facilitate the negotiations of agreements. This does however not mean that competence struggles are completely eradicated. On the one hand, there might still be situations where it is not clear whether the EU has a competence to act. On the other hand, Article 218 (3) TFEU foresees that the negotiator will be appointed by the Council depending on the subject matter. On subject matters with ambiguous objectives, turf battles between different actors might still arise. Furthermore, it is not clear whether a consistent approach in determining a specific lead negotiator on all external AFSJ matters is favourable to maintaining consistency across the different AFSJ internal policies.[489]

In sum, particularly before Lisbon the AFSJ external dimension was fraught with complexities and uncertainties as to whether and how the EU has a competence to act and if so in which areas. Post-Lisbon the unification of pillars led to more certainty but competence struggles may still occur.

5.2 The nature and evolution of EU-US relations on privacy and data protection in ASFJ

The purpose of this section is to explain the origins and nature of EU-US relations on AFSJ matters. It will be shown that similarly to EU-internal AFSJ, the relationship between the EU and the US on AFSJ matters also underwent changes due to the transformative nature of the EU institutional framework. It is important to bear in mind the overarching dynamics of EU-US AFSJ cooperation when the three case studies in the next part of the thesis are presented.

EU–US cooperation on AFSJ matters started in the 1970s via the informal Trevi Group. In 1995 the New Transatlantic Agenda was a further stepping-stone regarding this cooperation.[490] The agenda was an attempt to strengthen cooperation between the EU and US in general. However, one of its goals was to respond to global challenges including 'active, practical cooperation between the U.S' in the 'common battle' against crime, drug trafficking and terrorism.[491] Only since the terror

[488] Wessel, R., Marin, L. & Matera, C. (2011). The External Dimension of the EU's Area of Freedom, Security and Justice. In: Eckes, C & Konstadinidis, T. (eds.) *Crime within the Area of Freedom, Security and Justice*. Cambridge University Press, p. 298.
[489] Ibid.
[490] New Transatlantic Agenda signed at EU-US summit in Madrid on 3 December 1995.
[491] ibid.

attacks of 9/11, did EU-US cooperation on public security become more institutionalised[492] and start to address privacy and data protection issues.

5.2.1 Five different cooperation mechanisms

EU-US AFSJ cooperation can be regarded as a "multi-layered and extensive framework"[493] containing different safeguard mechanisms for data protection and privacy. Within this framework, cooperation can be categorised according to five different instruments: (i) traditional agreements, (ii) agreements with AFSJ agencies, (iii) 'executive' or 'operational' agreements, (iv) informal cooperation, and (v) framework agreements.

First, 'traditional agreements'[494] on criminal justice matters are the extradition and mutual legal assistance agreements between the US and the EU.[495] Both agreements are noteworthy as they were among the first major steps in the EU-US relationship on AFSJ matters as well as the first international agreements that were negotiated under the third pillar.[496] The second category of agreements consists of agreements with EU agencies that work on AFSJ matters. Worth mentioning is a cooperation agreement with Eurojust[497] since it aims to facilitate the exchange of data between the EU agency Eurojust and US authorities. There are also agreements between the US and Europol and Frontex but these treaties only legitimise the exchange of strategic and technical information and not personal data.[498]

The third category refers to 'executive' or 'operational' agreements, which are "(...) agreements that have been concluded as a response to US unilateral emergency security measures adopted post-9/11".[499] This includes the PNR and SWIFT

[492] As stressed in: Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001, *SN 140/01*. See: Gilmore, B. (2003). The Twin Towers and the Third Pillar: Some Security Agenda Developments. *EUI Working Paper LAW No. 2003/7*.
[493] Mitsilegas, V. (2014). Transatlantic counterterrorism cooperation and European Values. The elusive quest for coherence. In: Curtin, D. & Fahey, E. (eds.). *A Transatlantic Community of Law Legal Perspectives on the Relationship between the EU and US Legal Orders*. Cambridge University Press, p. 291.
[494] Mitsilegas, V. (2014), op. cit., p. 291.
[495] Agreement on extradition between the European Union and the United States of America, *OJ 2003 L181*, p. 27; Agreement on mutual legal assistance between the European Union and the United States of America, *OJ 2003 L 181*, p. 34. Note that only the latter Agreement includes privacy safeguards.
[496] See: Mitsilegas, V. (2003) The New EU-US Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data. *European Foreign Affairs Review*, vol. 8, pp. 151-36.
[497] Agreement between the United States of America and Eurojust of 6 November 2006.
[498] Cooperation Agreement between Europol and the USA of 6 December 2001. Article 10 states that the exchange of personal data shall be considered in future negotiations.
[499] Mitsilegas, V. (2014), op. cit., p. 292.

Agreements which concern the cooperation regarding aviation security and anti-terrorist financing. As elaborated further in the case study chapters, both agreements establish a tailor-made data protection regime that was amended multiple times since the existence of the agreements.[500] The fourth category consists of informal cooperation mechanisms aiming at the establishment of a forum to discuss practical issues related to AFSJ. For instance the 'Transatlantic Legislators' Dialogue' aims to facilitate the dialogue between European and American legislators, the EP and the American Congress. Furthermore, the so-called 'EU-US High Level Contact Groups' have been formed as informal transatlantic high-level advisory groups to discuss specific issues arising from AFSJ cooperation. Examples are the EU-US High Level Contact Group on data protection and data sharing (HLCG) formed in 2006[501] and the High Level Political Dialogue on Border and Transportation Security.[502]

Finally, framework agreements are cooperation mechanisms which attracted attention especially in the post-Snowden era by addressing the legal differences between the EU and the US regarding the balance between security and fundamental rights. These agreements set out general rules for AFSJ cooperation. In this category the 'Agreement on data protection relating to the prevention, investigation, detection, and prosecution of criminal offenses' (Umbrella Agreement)[503] is the most relevant. The Privacy Shield[504] can also be categorised as a cooperation agreement between the EU and the US since it establishes common legal grounds to facilitate data flows between the EU and the US. While not primarily designed for AFSJ matters, the shield is nonetheless relevant for this thesis since parts of it deal with LEA access to data held by private companies. Both framework agreements are discussed under 5.2.3 below since they are of a systemic nature illustrating the transformative nature of EU-US relations. Furthermore, they may be relevant for any future EU-US AFSJ initiative.

---

[500] See Chapters 5 and 6 of this thesis.
[501] See EU-US Summit, 12 June 2008 - Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection of 12 June 2008, *Council Document 9831/08*.
[502] Further details in: Pawlak, P. (2009b) Network Politics in Transatlantic Homeland Security Cooperation, *Perspectives on European Politics and Society*, vol. 10 (4), pp. 560-581.
[503] Proposal for a Council Decision on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, *COM/2016/0237 final.*
[504] Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, *C (2016) 4176 final*.

5.2.2 The changing nature of EU-US cooperation: A shift from a US monologue towards a EU-US dialogue?

In the period after 9/11 it has often been argued the US was setting the tone of EU-US relations whereas the EU had a rather reactionary role.[505] However in subsequent years, the EU developed incrementally into an equal actor due to mainly three aspects: (i) the entry into force of the Lisbon Treaty led to more consistency of the EU as international actor. Furthermore, the Treaty in conjunction with strategic EU policy objectives emphasised the fundamental rights dimension of AFSJ; (ii) the Snowden revelations led to an increased opposition of EU actors to unconditionally accepting security practices, and (iii) the CJEU started to play a more prominent role in stressing compliance with EU fundamental rights standards in international relations.

(i) The role of the Lisbon Treaty

The PNR and SWIFT Agreements were both examples of an US unilateral policy initiative that had extraterritorial effects on the EU.[506] Thus, the EU was naturally in a reactionary position when the agreements were negotiated. In addition, the pillar structure led to confusion on which procedure to apply and the rather insignificant role of the EP implied that the participation of a strong fundamental rights advocate to the negotiations was missing. As a result the first versions of the PNR and SWIFT Agreements constituted the result of negotiations among 'securocrats' which was reflected in the nature of the agreements.[507]

With the entry into force of the Lisbon Treaty a "democratisation of foreign policy" took place since the EP was granted full co-legislative powers through the abolition of former second and third pillars.[508] This had two main implications for EU-US relations. First, it led to more coherence in foreign relations in general since no ambiguity on the right legal basis or turf battles between the institutional actors

[505] Wessel, R., Marin, L. & Matera, C. (2011), p. 283. See also: Argomaniz, J. (2009) When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms. *Journal of European Integration*, vol. 31 (1), pp. 119-136.
[506] See Chapters 5 and 6 of this thesis.
[507] Pawlak, P. (2009a) *Made in the USA? The Influence of the US on the EU's Data Protection Regime.* Centre of European Policy Studies, Liberty and Security in Europe, Justice and Home Affairs section.
[508] Kuijper, P. J. (2014). The Case Law of the Court of Justice of the EU and the Allocation of External Relations Powers. Whither the Traditional Role of the Executive in EU Foreign Relations? In: Cremona, M. & Thies, A. (eds.). *The European Court of Justice and External Relations Law. Constitutional Challenges*, Hart Publishing, p. 99.

obscured the negotiations.[509] Thus, by decreasing the opportunities for power struggles between institutional actors the Lisbon Treaty contributed to more coherence and actorness of the EU in foreign relations.[510] Second, mainly before but also right after the adoption of the Lisbon Treaty the EP presented itself as strong defender of fundamental rights. Accordingly, the Lisbon Treaty enabled the EP to advocate more effectively for the introduction of higher privacy and data protection safeguards in the PNR and SWIFT agreements. As will be shown in the case study chapters, there are still some concerns with both agreements. Nevertheless, a significant improvement has taken place which can be ascribed to post-Lisbon changes to the procedure on concluding external agreements.

(ii) The NSA scandal as a turning point

In 2013 the NSA scandal provided EU actors with a justification for a more uncompromising stance in EU-US negotiations. This becomes clear in several policy documents adopted in the aftermath of the Snowden revelations. For instance, the EP argues that the US adherence to principles of mutual trust and cooperation as well as fundamental rights and the rule of law can be doubted after the 2013 revelations.[511] As a consequence, the EP suggested suspending the SWIFT Agreement.[512] The Commission also expressed concerns on EU-US AFSJ cooperation but focused on elaborating ways to restore trust.[513] In this context the Commission stressed the importance of the Umbrella Agreement. Negotiations on the Agreement had started already in 2010 and were still ongoing in 2013.[514] The purpose of the Umbrella

[509] The Lisbon Treaty also aimed to increase consistency in regard to external relations in general and in the CFSP policy field, see: Cremona, M. (2011a). Coherence in European Union Foreign Relations law. In Koutrakos, P. (ed.). *European Foreign Policy: Legal and Political Perspectives*. Edward Elgar.
[510] For an elaboration of the detrimental effect of pre-Lisbon structures on foreign relations, see: De Witte, B. (2008). Too Much Constitutional Law in the European Union's Foreign Relations? In: Cremona, M. and De Witte, B. (eds.) *EU Foreign Relations Law*. Hart Publishing, p.11. It has to be noted though that not all inconsistencies ceased to exist post-Lisbon. For an overview, see: Van Elsuwege, P. (2014). The Potential for Inter-Institutional Conflicts before the Court of Justice: Impact of the Lisbon Treaty. In: Cremona, M. & Thies, A. (eds.). *The European Court of Justice and External Relations Law*. Hart Publishing, pp. 114 -136.
[511] European Parliament Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy, *2013/2682(RSP)*.
[512] European Parliament Resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance; *2013/2831(RSP)*.
[513] Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows, *COM(2013) 846 final*.
[514] Note that the Agreement was signed by the negotiating parties in June 2016, approved by the EP in December 2016 and entered into force on 1st of February 2017.

Agreement was to enable even closer cooperation regarding the fight against crime and terrorism while affording a high level of privacy and data protection to EU and US citizens.[515] Due to the Snowden revelations arguably more US concessions were achieved. For instance, two critical provisions in the negotiations concerned redress mechanisms and direct access of LEA to privately held data.[516] On judicial redress, the EU-US negotiations triggered the adoption of the US Judicial Redress Act.[517] In regard to LEA access to privately held data, the privacy shield also led to some improvements.[518]

(iii) The role of the CJEU

Apart from constitutional and political developments the case law of the CJEU also contributed to the shifting nature of AFSJ cooperation in mainly two ways: (i) by ruling on the legal basis of AFSJ instruments before the adoption of the Lisbon Treaty and (ii) by ruling on the legality of AFSJ instruments in light of fundamental rights compliance. In regard to the first point, the annulment of the PNR Agreement led to the re-negotiation of the agreement. As further elaborated in Chapter 6 the case concerned the CJEU's assessment as to whether the first pillar was the correct legal basis for the PNR Agreement. The Court concluded that PNR data transfer to the US "(…) constitutes processing operations concerning public security and the activities of the State in areas of criminal law".[519] As a consequence the agreement did not fall within the scope of the DPD and had to be re-negotiated under third-pillar procedures.[520] The latter procedures implied a different power constellation among EU institutional actors impacting on the nature of the agreement.[521] It has often been argued that the deliberations in the PNR case contradict the judgment on the legal basis of the DRD.[522] Thus, the Court did not seem to have a special preference for democratic legitimisation of external policies when ruling on the legal basis in the

[515] Article 1 (1), Umbrella Agreement.
[516] Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows, *COM(2013) 846 final*.
[517] H.R.1428 - *Judicial Redress Act of 2015*, 114th Congress (2015-2016).
[518] See section 5.2.3 in this Chapter on the Privacy Shield and Umbrella Agreement.
[519] Joined Cases C-317/04 and C-318/04 *European Parliament v Council*, para. 56.
[520] Ibid., paras. 59 and 61.
[521] See Chapter 6 of this thesis.
[522] Ibid.

PNR case.[523] By arguing in favour of a third pillar basis it deprived the EP of its co-legislative power and its own competence to rule on the agreement in the future.[524] In this way, the case led to a less democratic decision-making process. This approach contradicts the CJEU's recent strong stance on privacy and data protection. The reason for the Court's changed approach in the post-Lisbon context is related to the adoption of CFREU providing greater legitimacy to a stricter assessment of fundamental rights compliance.[525]

The second way in which the Court exercised influence on EU-US relations refers to the Court's analysis of substantial aspects. For example, in *DRI* it was criticised that the DRD does not require data to be stored in the EU with the result that it cannot be held that the control -required by Article 8(3) CFREU- by an independent authority of compliance with the requirements of protection and security is complied with.[526] Given that commercial data exchange at that time was still based on Safe Harbour certifying adequate standards, the mistrust of the CJEU towards the US was clearly visible and arguably was a result of the Snowden revelations. Apart from this, the significance of CJEU case law in shaping EU-US relations reached its height with the *Schrems* case in 2014 where the CJEU annulled the Safe Harbour Agreement since it did neither adequately protect individuals' rights to data protection and privacy nor did it provide adequate redress mechanisms.[527] The CJEU's decision to invalidate the Safe Harbour Agreement with immediate effect can be criticised since not allowing for a transitional period had a negative effect on legal certainty although the role of the CJEU is to maintain the legal order.[528] However, the fact that the CJEU took such drastic action is arguably related to the CJEU's attempt to set a sign for "better law-making."[529] While a replacement for the Safe Harbour Agreement has been established in the meantime (EU-US Privacy Shield), the Article 29 WP has already criticised its provisions for being insufficient.[530]

[523] In other fields such a bias can be detected. For example in environmental protection cases as argued by: Kuijper, P. J. (2014), op. cit., p. 111.
[524] Ibid., p. 112
[525] Interview with former EP official.
[526] *DRI*, para. 68.
[527] *Schrems,* para. 94 and 95.
[528] European Parliament Debate with Jan-Philip Albrecht and Max Schrems of 21 October 2015.
[529] ibid.
[530] Article 29 WP, Opinion 01/2016.

In sum, it has been shown the CJEU plays a significant role in shaping AFSJ cooperation between the EU and the US.[531] While pre-Lisbon its influence was limited to determining the legal basis of agreements, post-Lisbon the Court's rulings on the substance have had a direct effect by increasingly postulating EU fundamental rights in EU-US relations.

5.2.3 The Umbrella Agreement and the Privacy Shield: A more EU centric EU-US dialogue?

The Privacy Shield and Umbrella Agreement can be regarded as an example of the increasing impact of the EU in US-EU relations since both were initiated by the EU. In the following it will be assessed in how far these two framework agreements in fact reflect EU standards in terms of increased transparency and fundamental rights compliance. It is shown that both agreements lead to a more rights-based approach in EU-US relation on AFSJ matters supporting the first hypothesis on the transitional character of the AFSJ institutional framework. However, there are still some concerns in regard to the extent to which those measures will in practice comply with CFREU.

(i) Privacy Shield

The Privacy Shield was adopted after the *Schrems* case annulled the Safe Harbour Agreement.[532] Due to the immediate annulment, EU and US authorities were under pressure to swiftly adopt a new agreement which complied with Articles 7, 8 and 47 CFREU and which assured that US data protection safeguards were *essentially equivalent*[533] to EU standards. Against this background, the Privacy Shield is an ambitious attempt to establish a more rights based transatlantic data transfer framework in respect to data processing for commercial purposes. At the same time the Shield also has some implications on data processing for public security purposes.

First of all, any measure regulating access to data for public security purposes should be based on 'accessible, foreseeable and precise rules'. In contrast to Safe

[531] Also in other circumstances CJEU jurisdiction had extraterritorial implications on the US. In Case C-131/12 *Google Spain SL, Google, Inc. v Agencia Española de Protección de Datos, Mario Costeja González* of 13th May 2014 the CJEU established the 'right to be forgotten' with respect to search results of the US-based search engine Google. The judgment sparked wide-ranging discussions on the geographical reach of CJEU jurisprudence. See for instance: Van Alsenoy B. and Koekkoek M. (2015) Extra-Territorial Reach of the EU's Right to Be Forgotten. *ICRI Research Paper 20.*
[532] *Schrems,* para. 107.
[533] *Schrems*, paras. 73-74.

Harbour, the Privacy Shield includes key definitions such as 'personal data', 'processing' and 'controller' and thus provides more legal certainty and clarity.[534] However, specifically in respect to law enforcement access to data for public security purposes the Privacy Shield seems to be less precise. Annex VII lists several paragraphs of different measures such as statutes, guidelines and policies all providing legitimisation for law enforcement agencies to access data. Furthermore, it also lists other laws that are relevant in this context without describing them further. The legal basis to any given data request might thus be different depending on the "(…) nature of the data sought, the nature of the company, the nature of the legal procedures (criminal, administrative, related to other public interest) and the nature of the entity requesting access."[535] While fragmentation of laws does not necessarily mean that they are not 'accessible, clear and precise', the existence of a multitude of different laws can lead to ambiguities depending on which law serves as the legal basis.

Second, safeguards to 'avoid abuse of power' need to exist in regard to access, oversight of access, remedies, retention period, data security and onward transfer.[536] It was mentioned in *Schrems* that any measure needs to include rules limiting the access of the public authorities to the data, and its subsequent use.[537] While the Safe Harbour Agreement did not contain any information on the existence of US rules limiting interference[538] the Privacy Shield explains the different tools available for law enforcement authorities to access data such as Grand Jury or Trial Subpoenas, and Administrative Subpoenas.[539] On the positive side, most tools described in Annex VII require a court decision before data can be accessed. Examples are: court orders for Pen Register and Trap and Traces, court orders for surveillance pursuant to the Federal Wiretap Law, and search warrants. In other situations an administrative subpoena may be sufficient but in those cases there is the possibility for the recipient of a subpoena to challenge the latter in Court "by presenting evidence that the agency

[534] Privacy Shield, op. cit., Annex II, para. 8.
[535] Article 29 Data Protection Working Party Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision of 13 April 2016, p. 53.
[536] *Schrems*, para. 91; *DRI*, para. 54; *Klass and Others v. Germany*, para. 50; *Weber and Saravia v. Germany*, para. 95; *Liberty v. UK*, para. 62; *Zakharov v. Russia*, para. 231 and *Szabó and Vissy v. Hungary*, para. 56.
[537] *Schrems,* para. 93.
[538] *Schrems*, paras. 87-88.
[539] Privacy Shield, Annex VII.

has not acted in accordance with basic standards of reasonableness".[540] These safeguards seem to be fairly robust as independent oversight mechanism regulating access.[541] However, it is unclear whether other laws could also provide a justification for access since the Privacy Shield only refers to 'primary investigative tools'[542] implying that there are also others available not listed in the Shield. Another concern refers to the provisions of the US Presidential Policy Directive 28 (PPD-28) quoted in the Shield providing that signals intelligence collected in bulk can be used for six specific purposes including the detection and countering of certain activities of foreign powers and combating transnational criminal threats. Neither the precise meaning of 'signal intelligence' nor the previously mentioned purposes are clear.[543] Further PPD-28 specifies that bulk collection is temporarily possible if it facilitates targeted collection.[544] Particularly the latter point leaves room for mass surveillance which was the very reason for replacing Safe Harbour with the Privacy Shield.

Another safeguard against abuse of power is the availability of effective remedies when public authorities access data. In the first place, the Privacy Shield establishes an Ombudsperson which can be approached by individuals to request information of whether data has been used by US state authorities. This is a step forward in terms of offering individuals administrative redress, but its effectiveness can be doubted. In Annex A point 4 (e) it is stated that the Ombudsperson only reacts to requests by mentioning that complaints have been properly investigated and by informing the individual whether potential non-compliance has been remedied. Thus, individuals will never be informed whether he or she has been subject to surveillance and if it was the case which remedial actions have been taken (not even when this does not harm the investigation at stake).[545] The Privacy Shield also mentions several laws that are available to all individuals when seeking judicial redress independent of their nationality.[546] These are the Administrative Procedure Act, the Freedom of Information Act and the Electronic Communications Privacy Act. Furthermore, the Judicial Redress Act entered into force in 2015 granting non-US citizens rights to judicial redress. These rights are however focused on a limited amount of actions such

[540] Ibid., Annex VII, p. 103.
[541] Article 29 WP Opinion 01/2016, p. 55.
[542] Privacy Shield, Annex VII, p. 100.
[543] Ibid., Annex VI, p. 80.
[544] US Presidential Policy Directive 28 (PPD-28) of 17 January 2017, sec. 2, fn.5.
[545] Privacy Shield, Annex A, point 4 (3), p. 55.
[546] Ibid., recital 130 to 134.

as the right to access and correction of data and the right to obtain civil remedies in cases of disclosures of data "intentionally or wilfully made.[547] It is also unclear whether EU citizens could in fact challenge access under the Fourth Amendment as it only applies to US citizens.[548] Even if EU citizens could benefit from it, the fact that laws apply in the first place to companies holding data, individuals seem not to be in a position to challenge access to their data.[549] In sum, more laws and mechanisms offering remedies are available to individuals than under the Safe Harbour Agreement but their effectiveness is questionable.

(ii) Umbrella Agreement

The purpose of the Umbrella Agreement is to enable even closer cooperation regarding the fight against crime and terrorism while affording a high level of privacy and data protection to EU and US citizens.[550] The ultimate goal is to facilitate the adoption of subsequent EU-US Agreements on AFSJ matters. While being of a similar nature as the Privacy Shield, the Umbrella Agreement is not an adequacy decision but an international agreement that applies when data is processed by or among law enforcement authorities.[551] In the following an analysis of the Agreement is provided.

First of all, from the EU point of view it is positive that concepts such as 'personal information', 'processing of personal information' and 'competent authority' are defined in a similar way as in the Police and Criminal Justice Data Protection Directive.[552] This common terminology will facilitate negotiations on any future initiative and establish legal certainty. Furthermore, the agreement requires both parties to inform each other –if possible in advance- of any measure adopted that affects the Agreement.[553] This is particularly an improvement considering that for instance SWIFT was first executed in secret and PNR was initiated without immediately informing the EU in advance. The requirement to keep an open dialogue will facilitate negotiations on both sides.

[547] Judicial Redress Act of 2015, H.R. 1428.
[548] Privacy Shield, para. 127.
[549] Ibid.
[550] Article 1 (1), Umbrella Agreement.
[551] Article 5 (3) of the Umbrella Agreement shows that the effect of the Agreement resembles that of an adequacy decision.
[552] Article 2, Umbrella Agreement and Article 3 of Directive 2016/680.
[553] Article 24, Umbrella Agreement.

Second, in regard to 'access' to data, the agreement provides some minimum safeguards. Article 6 lays down that the transfer of personal data shall be "(…) for specific purposes authorised by the legal basis for the transfer as set forth in Article 1."[554] Furthermore, any further processing of data shall not be incompatible with the purposes for which it was originally transferred. While this limitation is an important safeguard the article further stipulates that 'compatible processing' includes processing according to any international agreement or written international framework that is concerned with the prevention, detection, investigation or prosecution of serious crime.[555] In this way, further processing will not be limited to the purpose of a specific agreement but will remain broad. In regard to onward transfer the Agreement specifically sets out that the competent authority which originally transferred data has to consent to the transfer.[556] However, entrusting a judicial or independent administrative authority with a review of onward transfer would have been a more solid safeguard.

Third, the Umbrella Agreement mentions that retention periods shall be no longer than necessary and appropriate. Furthermore, retention periods shall account for "(…) the purposes of the processing, the nature of the data and the authority processing it, the impact on relevant rights and interests and other applicable legal considerations."[557] Furthermore, retention periods shall be specified in operational agreements and periodic review shall be carried out to assess whether the period is still appropriate.[558] By laying down that retention periods shall depend on several criteria and that it should be regularly reviewed, arbitrarily long retention periods shall be avoided. It is also positive that retention periods shall not depend on technical feasibility of deletion, as is the case under SWIFT. However it is regrettable that it is not explicitly specified that retention periods shall take the *usefulness* of retention in light of the objectives pursued into account.[559] Instead only the purposes of processing shall be accounted for without explicitly referring to the added value of this purpose.

Fourth, the Agreement mentions that individuals shall have the right to access and obtain rectification of their data[560] and that individuals of both parties are entitled

[554] Ibid., Article 6
[555] Ibid., Article 6 (2).
[556] Ibid., Article 7 (1).
[557] Ibid., Article 12 (1).
[558] Ibid., Article 12 (2) and 12 (3).
[559] *DRI*, para. 63.
[560] Article 16 and 17, Umbrella Agreement.

to seek administrative and judicial redress.[561] Article 21 lays down that oversight authorities shall exercise independent oversight and shall have the right to act upon complaints of individuals. It can however be criticised that it is not explicitly mentioned that in the US this authority has to be always independent of the authority processing the data or of authorities that can benefit from data processing.[562] The broad formulation of the article might lead to a less effective oversight mechanism.

One major concern of the Agreement refers to the scope of redress mechanisms. Article 19 (1) of the Umbrella Agreement stipulates that "(…) subject to any requirements that administrative redress first be exhausted, *any citizen of a Party* is entitled to seek judicial review (…)."[563] To ensure the effectiveness of this provision, the Judicial Redress Act was adopted in the US. While the adoption of the Redress Act is a noticeable achievement providing more legal certainty for EU citizens, a problem is that Article 19 precludes any non-EU citizen from seeking redress even though this person might be subject to Union law. The TFEU and CFREU stipulate that "*Everyone* has the right to the protection of personal data concerning them"[564] implying that both citizens and non-citizens located in the EU territory are covered by this provision. The fact that non-EU citizens are not covered creates a loophole in legal protection and its legality is questionable in light of *Schrems* where it was held that "legislation not providing any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."[565]

In sum, the Umbrella Agreement provides a solid foundation for any future agreements to be concluded between the EU and the US in the public security context. While there are still some critical aspects especially in relation to the accessibility of redress mechanisms, it is clear that EU fundamental rights standards are increasingly playing a role in EU-US relations. This confirms the first hypothesis, namely that privacy and data protection are shaped by the transformative character of the AFSJ

[561] Ibid., Article 18 and 19.
[562] Ibid., Article 21 (3).
[563] Ibid., Article 19 (1). Emphasis added by author.
[564] Article 16 (1) TFEU and Article 8 (1) CFREU. Emphasis added by author.
[565] *Schrems*, para. 95.

institutional framework. This holds true also when considering the external dimension of AFSJ in general and the AFSJ cooperation with the US.

Conclusion

The purpose of this chapter was to examine the institutional framework on privacy and data protection in AFSJ from a historical institutionalist perspective. The findings confirm Hypothesis 1 stating that '*the institutional framework of privacy and data protection in AFSJ is an institutional framework in transition implying that both established as well as new institutional features co-exist and commonly determine how data protection and privacy is shaped in relation to public security.*' Turning points or so-called 'critical junctures*'* as well as institution-internal uncertainties have contributed to the transitional character of the institution while simultaneously path-dependence has led to the stickiness to former institutional habits. The two key 'critical junctures' are the entry into force of the Lisbon Treaty and the adoption of the CFREU. However, also the role of events and subtle processes in triggering institutional change are relevant. For example, the attacks on 9/11 and the Snowden revelations had an underlying impact on determining the paths of EU-US relations. In addition, technological change is considered to be an underlying process that led to change on constitutional and legislative levels.

As stated above some features are locked into 'old paths' while others are moving 'onto a new path'. On the constitutional level, a major change was the introduction of Article 8 CFREU. It was illustrated that by entering into judicial dialogue with the ECtHR, the CJEU adheres to the ECtHR conceptualisation of the correlation of privacy and data protection and reiterates many safeguards that were laid down by the ECtHR when reconciling public security with the right to privacy. However, it has been shown that recent CJEU jurisprudence seems to be the new trendsetter mainly due to its more efficient *modus operandi*, more venues for actors to file cases and due to EU integrationist tendencies of public security measures.

On the legislative level, a major change was brought about by the destruction of the pillar structure. It has been shown that pre-Lisbon the institutional framework for AFSJ was unduly complex and had a convoluted relationship with other areas of EU law.[566] In this environment data protection and privacy were mainly regulated in a

[566] Peers, S. (2011), op. cit., p. 135.

piece-meal fashion where single policies established autonomous data protection regimes. Post-Lisbon many regimes regulating privacy and data protection in AFSJ are still subject to autonomous rules on data protection and privacy. Nevertheless, particularly the GDPR and the Police and Criminal Justice Directive are promising tools to eradicate at least some fragmentation by providing a more solid foundation for more harmonised solutions.

On the international legislative level particularly EU-US relations are relevant. In terms of institutional change, it has been shown that due to mainly three reasons (i.e. (i) more coherence in EU external relations through Lisbon; (ii) the Snowden revelations; (iii) and the increasing role of the CJEU) the EU became more emancipated in negotiations on data protection and privacy in the AFSJ context turning a US monologue incrementally into a dialogue. In terms of path- dependence, the two most recent agreements between the EU and the US addressing privacy and data protection in AFSJ (the Umbrella Agreement and the Privacy Shield) do still not completely live up to the strict EU standards.

Acknowledging the transitional nature of 'privacy and data protection in AFSJ' on constitutional and legislative levels is important for the case study chapters. On the one hand, this chapter is important to set the strategic behaviours of policy actors into the context of the changing institutional framework (Hypothesis 2). On the other hand, the chapter also provided an evaluative framework for the legality assessment of the DRD, and the PNR and SWIFT Agreements (Hypothesis 3). Respectively, the chapter provided an overview of CJEU and ECtHR generated-principles in relation to data retention and access regimes in the public security context. The principles have been structured according to three key criteria: (i) Is the measure accessible, foreseeable and does it respect the essence of the rights to privacy and data protection?; (ii) Is the measure proportionate in terms of necessity with regard to legitimate objectives pursued?; (iii) Is the measure proportionate in terms of laying down sufficient safeguards against the abuse of power? This three-step framework will be applied in the DRD, the PNR and SWIFT chapters to analyse the legality of each regime.

PART II – INSTITUTIONAL COMPLEXITY AND THE ROLE OF INSTITUTIONAL ACTORS

Part II of the thesis deals with the analysis of three case studies in accordance with the theoretical approach developed in Part I. More specifically, all three case studies will be analysed in respect to Hypothesis 2 and 3. While a more detailed account of the background and nature of the case studies is included in each of the following three chapters, this short section aims to define the common ground of and differences between the three case studies. In regard to the common features, it has to be noted, that:

- All regimes have been adopted in a similar political environment namely as a result of terror events in Europe and the US. The Data Retention Directive has been adopted in the aftermath of the London and Madrid bombings, while the SWIFT and PNR Agreements were adopted shortly after the 9/11 attacks.
- All three case studies concern legislative initiatives emerging at a similar point in time and the pre- and post-Lisbon institutional framework shape the nature of the legislation.
- In all three regimes data that was originally generated for private sector purposes (i.e. airline companies, telecommunication service providers and financial messaging service providers) but is used for public security purposes.

There are also four crucial differences between the three regimes:

- While the DRD is an EU internal legal instrument, both the SWIFT and PNR regimes are international agreements between the EU and the US, which were the result of US policy initiatives that had extraterritorial effects on the EU.[567]
- While in all three case studies personal data is processed for public security purposes the type of processed data differs. Under the DRD, traffic and

[567] 'Extraterritorial effects' shall not be confused with 'extraterritorial jurisdiction' implying "(…) the exercise of jurisdiction, or legal power, *outside* territorial borders" as in the latter case no physical link to US territory is necessary. It has been argued that "national laws may be given extraterritorial application, provided that these laws could be justified by one of the recognized principles of extraterritorial jurisdiction under public international law." These principles are: the active personality principle, the protective principle, the passive personality principle or the universality principle. See: Ryngaert, C. (2015). *Jurisdiction in International Law*. Oxford Scholarly Authorities on International Law. See also: Colangelo, A. J. (2014). What Is Extraterritorial Jurisdiction *99 Cornell Law Review,* vol. 99 (6).

location data is processed.[568] In contrast, the SWIFT Agreement concerns personal data generated when bank transfers are made and the PNR Agreement concerns personal data generated when individuals engage in air travel. While traffic and location data is in any case a special or sensitive category of data as stipulated by the e-privacy Directive, in respect to SWIFT and PNR sensitive data may form part of the data sets. Each case study chapter will provide an explanation as to why and how sensitive data might be concerned.

- All three case studies include provisions on data retention but differences in the data processing cycle need to be acknowledged. The DRD requires service providers to indiscriminately retain traffic and location data which has been collected for billing purposes and for providing the service.[569] In contrast, the PNR and SWIFT Agreements require the transfer of personal data to US authorities while retention is then only regulated after data has been transferred.
- Although the driving force behind all three case studies was terrorism, the SWIFT Agreement is the only measure where the purpose relates exclusively to "(…) the prevention, detection, investigation or prosecution of terrorism and its financing."[570] In contrast, the purpose of the other two measures is extended to the fight against other forms of serious crime.

[568] Considered as special category of data, see: Articles 6 and 9, e-privacy Directive.
[569] 'Access' is regulated by Member State authorities and not the Directive.
[570] Article 1 (1a), SWIFT II Agreement.

CHAPTER 4 –THE RISE AND FALL OF THE DATA RETENTION DIRECTIVE

Introduction

On 14 December 2005 the EP adopted Directive 2006/24/EC (hereinafter Data Retention Directive or DRD) after the first reading under the co-decision procedure. The directive was adopted in the aftermath of the London and Madrid bombings with the aim to fight serious crime and terrorism through the retention of communication data. The DRD requires telecommunication companies to store traffic and location data of fixed, mobile and internet telephony, internet access and email for a period of a minimum of six months and a maximum of two years. This means that detailed information on passive and active telecommunication users is retained.[571] Due to the extensive nature of the measure it was suggested that rather than talking about the retention of data one should refer to the creation of 'digital dossiers' of every telecommunications user.[572] Apart from storage, the Directive also stipulates that data has to be made available to law enforcement agencies if a request has been issued.

In the years subsequent to its adoption, the Directive has been criticised by academics[573], politicians[574] and civil rights organisations[575] due to its disproportionate interference with Articles 7 and 8 CFREU and Article 8 ECHR. Furthermore, constitutional courts in multiple Member States found that the national laws transposing the Directive were unconstitutional.[576] On 8th April 2014 the CJEU annulled the Directive in its entirety.[577] The Court claims that the DRD satisfies an objective of general interest by pursuing the objective of fighting serious crime and by

[571] Passive implies that also data of the receiver of the communication is captured.
[572] Solove, D. (2004) *The Digital Person: Technology and Privacy in the Information Age.* NYU Press
[573] For example: Beyer, P. (2005). Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. *European Law Journal*, vol. 11 (3), pp. 365–375.
[574] For example Sabine Leutheusser-Schnarrenberger (German Minister of Justice, incumbent 2009-2013) criticised the Directive heavily and suggested the 'quick-freeze procedure as alternative. Retrieved 09.01.2017 from http://www.spiegel.de/politik/deutschland/vorratsdatenspeicherung-eu-kommission-verklagt-deutschland-a-836221.html.
[575] NGO Letter to the EU Commission rejecting the Directive on mandatory data retention. Signed by 106 NGOs. Retrieved 09.01.2017 from: http://www.statewatch.org/news/2010/jun/ngo-dataret-letter.pdf
[576] Constitutional courts in Bulgaria, Romania, Germany, Czech Republic.
[577] This however does not mean the end of data retention. For example, just one day after the terror attack on a publishing house in France in January 2015, politicians in Germany started to re-discuss the need for data retention. Retrieved 07. 01.2017 from http://www.spiegel.de/netzwelt/netzpolitik/charlie-hebdo-streitgespraech-ueber-vorratsdatenspeicherung-a-1012141.html

maintaining public security. Nevertheless, it interferes in a particularly serious and disproportionate manner with Articles 7 and 8 CFREU and Article 8 ECHR.[578]

The aim of this chapter is to examine how the institutional framework has been shaping data protection and privacy in regard to the data retention directive. While doing so, it will be assessed whether Hypotheses 2 and 3 are confirmed. In terms of structure, this chapter is divided in five main sections: (i) the nature of the DRD and the agenda-setting period is analysed; (ii) the chapter analyses how the pillar structure – as essential feature of the pre-Lisbon era – shaped the interaction between institutional actors (i.e. policy makers and the CJEU); (iii) it will be assessed how the decision-making procedure shaped the policy outcome on data retention; (iv) the CJEU ruling on the DRD is analysed and its implications on the legality of indiscriminate data retention are assessed; (v) ultimately, the chapter assesses whether the CJEU's *DRI* ruling exhibits features of 'political actorness'.

1. Key features of the DRD

While a detailed analysis of the provisions and legality of the DRD is conducted in the third part of this chapter, in the following the aim is to illustrate that the DRD is formulated in broad terms leading to a lack of legal certainty. First, the aim of the DRD is to harmonise national data retention regimes to ensure that the data is available for "the investigation, detection and prosecution of serious crime as defined by each Member State in its national law".[579] Contrary to this provision, the preamble stresses the usefulness of data retention in regard to the "*prevention*, investigation, detection and prosecution of criminal offences."[580] This inconsistency between the preamble and main text of the directive leads to uncertainty regarding the Directive's actual scope. Second, the Directive refrains from defining 'serious crime' and leaves it open to Member States to determine its meaning. This resulted in a considerable divergence of scope when the Directive was implemented at national level.[581] Third, Article 1 (2) of the Directive limits the material scope of the directive to traffic and location data while explicitly excluding content data. Nevertheless, the privacy implications of processing traffic/location data can be similarly severe as those in

[578] *DRI,* para. 69.
[579] Article 1(1), DRD.
[580] Recital 7, DRD; emphasis added by author.
[581] During an interview with a Commission official it was mentioned that the Commission was often approached by service providers since they were uncertain about the DRD's scope.

relation to content data since both types of data can provide a detailed picture about a person.[582]

Fourth, Article 4 DRD stipulates that access shall only be granted to competent national authorities in specific cases and in accordance with the national law. The Member State can thus decide which authority or agency accesses data. While this may be necessary given the different legal systems in the Member States, it results in different standards in the Member States in terms of frequency of requests, use of data and the agency that accesses data.[583] For instance, most Member States grant the police access to retained data while others grant access rights to secret services, the ministry of interior or the courts. In some Member States all of those actors can access retained data.[584] Depending on the mandate of the national authority accessing data, the risk of illegitimate access might be higher in some Member States than in others. Article 4 DRD not only leaves discretion in terms of accessing data but also in regard to the applicable procedure. Consequently, not all Member States oblige the competent authorities to obtain a judicial authorisation to access data.[585] The failure to define what constitutes a competent authority and the failure to lay down a uniform procedure when access to data is sought can lead to discrepancies in Member States regarding the nature of requirements imposed on service providers. This contradicts the very reason of adopting the Directive (i.e. achieving harmonisation among Member States in regard to the legal requirements imposed on service providers). Fifth, the retention period of all data categories should be between six months and two years at the discretion of the Member States without specifying that the period shall be based on objective criteria.[586] This also creates divergences between Member States and can lead to an asymmetric burden on service providers throughout the EU.

The previously mentioned points illustrate that several concepts and aspects remain undefined and a wide discretion is granted to Member States despite of the

[582] For instance: Constitutional Court of Romania, *Decision No. 1258* of 8 October 2009, established that retained traffic and location data are interfering with the right to privacy similarly like the content of communications.
[583] Article 4, DRD.
[584] Report from the Commission to the Council and the European Parliament - Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), *COM(2011) 225 final*, p. 10.
[585] ibid. For example, in Ireland and Slovakia a request in writing is sufficient.
[586] Article 6, DRD.

'creating effect' of the Directive.[587] This has an impact on legal certainty and undermines the objective of EU instruments of harmonising diverging provisions. The following sections provide an overview on how the Directive emerged and why it took its ultimate form. More specifically, it will be shown how the institutional framework and the way actors interacted with and through the institutional framework shaped privacy and data protection in relation to data retention.

2. The role of the Council, Commission and EP in shaping privacy and data protection in the context of data retention

2.1 The Madrid and London terror attacks: A window of opportunity?

It has often been argued that the Madrid and London bombings in 2004 and 2005 brought about significant changes both in terms of European threat perceptions and legislative initiatives.[588] In this context, data retention was considered necessary to make law enforcement more effective and efficient.[589] The DRD has thus been labelled "the misshapen child" of the terrorist attacks in Europe.[590] While the attacks gave impetus to the swift adoption of the DRD, declaring the bombings in 2004 and 2005 as the sole reason for establishing an EU-wide regulatory framework on data retention is misleading. It disregards the fact that data retention has already been discussed on the EU level well before 2004 while seizing the opportunity of certain events is a tool of policy makers to advocate for their strategic preferences as collectively superior outcomes.

As early as 1993 "International Law Enforcement and Telecommunications Seminars" (ILETS) were held at the FBI academy in the US. The objective was to

---

[587] The AG in *DRI* argues that since the Directive has a 'creating effect' (i.e. it obliges MS to impose requirements on service providers to collect and retain data) to ensure the proper functioning of the internal market the Directive also needs to provide specific guarantees accompanying this requirement (para. 123).

[588] Maras, M. (2011). While the European Union was Sleeping, the Data Retention Directive Was Passed: The Political Consequences of Mandatory Data Retention. *Hamburg Review of Social Sciences*, vol. 6 (1), pp. 1-30. See also: Ruiter, R. & Neuhold, C. (2012). Why is Fast Track the Way to Go? Justifications for Early Agreement in the Co-Decision Procedure and Their Effects. *European Law Journal*, vol. 18 (4), pp. 536-554.

[589] European Commission Evaluation Report on the Data Retention Directive, *COM(2011) 225 final,* p.1.

[590] Konstadinides, T. (2014) Mass Surveillance and Data Protection in EU Law: The Data Retention Directive Saga. In: Bergström, M. and Jonsson Cornell, A. (eds.) *European Police and Criminal Law Co-Operation*. Hart Publishing, pp. 69 – 84.

develop global interception requirements, in form of common "standards for telephone-tapping by police and security agencies to be provided in all telephone networks."[591] After the first ILETS meeting the EU Council of Justice and Home Affairs (JHA) adopted a secret resolution in November 1993[592] stipulating that EU standards in regard to interception of telecommunications shall be comparable to those of the FBI. This was followed by another resolution in January 1995 regulating the obligations of telecommunications companies and law enforcement agencies when engaging in intercepting activities.[593]

In the same context, Directive 97/66 was adopted in 1997 dealing with privacy in the telecommunications sector. In 2002, the e-Privacy Directive 2002/58/EC repealed and replaced Directive 97/66.[594] Article 15 of Directive 2002/58/EC allows Member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in the Directive if it "constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. state security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system (…)."[595]Article 15 (1) of the e-privacy Directive has been criticised as a 'legal loophole' giving Member States a *card blanche* to adopt possibly intrusive legislation.[596]

Based on Council discussions in 2001 on the usefulness of communications data in the fight against crime and terrorism, the Belgian government issued a confidential draft framework decision on approximating data retention requirements.[597] After the document leaked, media across the EU heavily criticised the

[591] Jones, C & Hayes, B. (2013). The EU Data Retention Directive: a case study on the legitimacy and effectiveness of EU counter-terrorism policy. In: *SECILE – Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness*. A Project co-funded by the European Union within the 7th Framework Programme – SECURITY theme, p. 6.
[592] Council Justice and Home Affairs on Interception of telecommunications of 16 November 1993, *Council doc. 10090/93*.
[593] Council Resolution of 17 January 1995 on the lawful interception of telecommunications, *OJ 1996 C 329/01*
[594] Article 19, e-privacy Directive.
[595] Article 15, e-privacy Directive.
[596] Peter Hustinx (2010) The moment of truth for the Data Retention Directive, Speech of 3 December 2010, Retrieved 09.01.2017 from http://www.edps.europa.eu.
[597] Justice and Home Affairs Council Conclusions of 20 September 2001, *SN 3926/6/01*, p. 3; Belgian proposal for Third Pillar legislation Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions. Retrieved 09.01.2017 from: http://www.statewatch.org/news/2002/aug/05datafd.htm

secret proposal.[598] The incumbent Danish Presidency subsequently stated that the secret proposal was only "a request that, within the very near future, binding rules should be established on the approximation of Member States' rules on the obligation of telecommunications services providers to keep information (…) in order to ensure that such information is available when it is of significance for a criminal investigation."[599] The discussions on the confidential draft framework decisions abated in the following months and no actions have been taken.

The discussions reawakened after the Madrid bombings when the European Council adopted a Declaration which stressed the importance of establishing rules on the retention of communications traffic data by service providers.[600] Consequently, France, Ireland, Sweden and the UK used the Madrid bombings in conjunction with the latter declaration as 'window of opportunity' to reawaken the confidential Belgian proposal on obligatory data retention. By relying on Article 34 (2) TEU -an exceptional rule granting the Council the right of initiative in AFSJ matters-[601] they submitted a joint proposal for a framework decision on the retention of communication data to the EU Commission.[602] In response, the Commission acknowledged the joint proposal and started a consultation on the matter resulting in a proposal for a Directive.[603] After a rocky legislative path -which will be explained in the next section- the Data Retention Directive was adopted in 2006.

In sum, data retention has been discussed already before 2004 on national,[604] EU, and international levels. It was even raised before the 9/11 terror attacks, which is often considered as turning point of the threat perception of terrorism and impacted policy making on a global scale. This suggests that the exceptional situation after the Madrid bombings was merely used as a window of opportunity to push through a

[598] *Data retention report is wrong*, says European Presidency. Retrieved 09.01.2017 from http://www.out-law.com/page-2883
[599] Ibid.
[600] *European Council Declaration on Combatting Terrorism* of 25 March 2004. Retrieved from http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf , p. 4.
[601] The Council has only a right of initiative when Judicial Cooperation in Criminal Matters or Police Cooperation is at stake; Article 76 TFEU (ex-Article 34 (2) TEU).
[602] Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism of 28 April 2004, *Council nr. 8958/04*.
[603] Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, *COM(2005) 438 final*.
[604] Examples of data retention on national level, see: UK Regulation of Investigatory Powers Act 2000.

controversial legislative proposal instead of being the cause for data retention discussions.

2.2 Data retention after London and Madrid: Seizing the moment to regulate data retention

In accordance to NI, the following subsections illustrate how cross-pillarisation and the legislation-making procedure revealed that power aspirations of the EP and the Commission were the primary strategic preference while the Council's preference was biased towards high security standards.

2.2.1 Cross-pillarisation and power struggles before the adoption of the DRD

A pre-condition for EU institutional actors to make use of cross-pillarisation is the ambiguity of whether a first or third pillar legal basis is more appropriate. Only if a topic is pursuing objectives of both pillars the involved actors can advocate for the policy solution that is in their favour. In the case of data retention there were clearly two important objectives to be satisfied. On the one hand, obligatory data retention aims to ensure that law enforcement officials have access to relevant data coherently throughout the EU. Particularly due to the considerable growth in the opportunities afforded by electronic communications, data retention became an important tool in the prevention, investigation, detection and prosecution of criminal offences.[605] This suggests that the adequate legal basis is to be found in the third pillar.

On the other hand, data retention also has an internal market dimension. While some Member States had data retention laws in place (e.g. Belgium, Denmark, Finland) other Member States did not have such laws (e.g. Austria, Germany) and others had voluntary regimes in place (e.g. UK).[606] Where data retention regimes existed in Member States they substantially differed in terms of retention period and provisions on access to data.[607] Consequently, businesses were faced which different

[605] Recital 3, Draft Framework Decision on the retention of data, *Council doc. 8958/04*. See also: Communication from the Commission to the Council and the European Parliament of 16 June 2004: Towards enhancing access to information by law enforcement agencies, *COM(2004) 429 final*.
[606] Council of the European Union - Answers to questionnaire on traffic data retention, *Council Doc. 14107/02*. Retrieved 09.01.2017 from: http://www.statewatch.org/news/2003/jan/12eudatret.htm
[607] ibid.

legal requirements when based in more than one Member State or when offering their services in more than one country. Therefore, a measure on data retention aims to harmonize practices across the EU and to create equal conditions for service providers suggesting that an instrument requires a first pillar basis. One has to note, however, that the telecommunication sector is not a 'country of origin' regime raising concerns in regard to the necessity of a measure due to internal market considerations.

The Council or more precisely, France, Ireland, Sweden and the UK initiated the legislative process by suggesting a framework decision (third pillar instrument) to the Commission.[608] The obvious reason for the Council's preference for a third pillar instrument is related to the perception that retention of data serves the purpose of having data available for the case that law enforcement agencies want to access the data. The Council justified this view by reference to the PNR case where the CJEU held that data derived from the private sector (i.e. airlines) used for law enforcement purposes is a third pillar matter.[609] Apart from that, there is also the strategic benefit of diminishing the EP's role in the legislation making process.[610] A marginal influence of the EP implies faster adoption of the instrument and the mitigation of the risk of debates due to the controversial nature of the initiative.

The Commission did not agree with regulating data retention through a framework decision and issued a formal proposal to regulate data retention via a first pillar directive under Article 95 TEC.[611] Interestingly the Commission proposal sets out that the increasing use of electronic communications networks generates traffic and location data that are useful for law enforcement purposes.[612] Only towards the end does it mention that "[d]ifferences in the legal, regulatory, and technical provisions in Member States concerning the retention of traffic data present obstacles to the Internal Market for electronic communications as service providers are faced with different requirements regarding the types of data to be retained as well as the conditions of retention."[613] Furthermore, provisions on data retention of traffic data were previously also based on first-pillar instruments in Directives 2002/58/EC and

[608] Draft Framework Decision on the retention of data, *Council doc. 8958/04*, recital 3.
[609] See section 2.2.2 below.
[610] Article 34, TEU.
[611] Article 95 TEC is post-Lisbon Article 114, TFEU. Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, *COM (2005) 438 final*.
[612] Ibid., p. 2.
[613] Ibid.

95/46/EC. The only reason why data retention was not harmonized in the former Directive was due to the fact that no political agreement on the actual length of retention was reached.[614] Therefore, any further instrument on retention on traffic data must be placed under the first pillar.[615] The fact that the Commission mainly focused on other first pillar measures to justify the first pillar basis shows that the market angle was somehow forced.[616] After Lisbon the Commission would most likely have chosen Article 83 TFEU in conjunction with Article 16 TFEU as legal basis being more in line with the Council's interpretation.[617]

In an attempt to explain why the Commission forced a market angle it was claimed that the Commission regarded the more democratic procedures of the first pillar as better suited to a topic that interferes with the right to the protection of personal data.[618] First of all, a first pillar instrument grants the Commission the right of initiative and the possibility to conduct later revisions of the law through an administrative process (regulatory comitology committee).[619] Second, other supranational actors such as the EP and the EDPS can exercise formal and informal democratic scrutiny. By having a strong stance on data protection and privacy safeguards they can add a valuable dimension to debates.[620] Additionally, the EP in contrast to the Council consults a wide variety of interest groups which contributes to a greater extent to democratic participation and transparency.[621] Furthermore, a first pillar instrument also ensures that Community law relating to data protection applies which increases the level of protection when data is processed.[622]

Another reason for the Commission's preference for a first pillar instrument relates to the ambition to create room for actorness by raising the profile of the Commission in the AFSJ field. Thus, the Commission had obviously a strategic

[614] Ibid.
[615] Ibid, p. 8.
[616] Konstadinides, T. (2014). op. cit.
[617] ibid.
[618] Bignami, F. (2006). Protecting Privacy Against the Police in the European Union: The Data Retention Directive. *GW Law School Law and Legal Theory Paper No. 2013-43*., p. 114. This justification was also mentioned during an interview with a EU Commission official.
[619] Articles 5 and 6, Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, *COM (2005) 438 final*.
[620] De Capitani, E. (2010) The Evolving Role of the European Parliament in AFSJ. In: Monar, J. (ed.). *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice*. College of Europe Studies, Peter Lang, p. 125-126.
[621] Monar, J. (2010a), op. cit.
[622] This argument was also mentioned by the EDPS as intervener in C-301/06, *Ireland v. Parliament and Council*, judgment of the Court of 10 February 2009, para. 55.

interest in pursuing a first pillar basis.[623] This not only implies a right of initiative for the Commission but also generates further spaces where it can exercise influence. For example it allows the Commission: to monitor the evolution of data retention in the Member States on a yearly basis[624], to evaluate the implementation of the Directive and its implications for various actors[625], and to consider whether to propose amendments to the Directive.[626] It is interesting to note the role of the JHA Commissioner Vitorino at the time. Vitorino has been labelled a 'supranational policy entrepreneur' in shaping AFSJ as a whole policy field even though it traditionally lacked the involvement of EU institutional actors.[627] For example, it was argued that Vitorino contributed greatly to the fact that the Commission was a first mover in the field and shaped the debate on anti-terrorism.[628] Furthermore, he contributed to the shaping of an effective policy preparation, monitoring and implementation structure of DG JHA.[629] Thus, Vitorino was a strong political figure which helped the Commission in developing a full policy–making capacity revealing the power of individuals in triggering institutional change.[630] Given Vitorino's strong emphasis on raising the profile of the Commission on AFSJ matters increasing the Commission's influence on AFSJ may have also played a role when the Commission contradicted the Council by suggesting a first pillar instrument to regulate data retention.

The Council ultimately gave in on the idea of a framework decision and supported the directive.[631] The Council's concession on the choice of the legal basis can be explained by the urgency of the matter. By giving up on a third pillar legal basis, the Council avoided a considerable delay in adopting the measure as otherwise the matter would have most likely ended up at the CJEU at the request of the Commission.[632] This is an interesting illustration of how the mere threat of

[623] As stressed in an interview with a European Commission official.
[624] Article 10, DRD.
[625] Article 14, DRD.
[626] Article 12 (3), DRD.
[627] Kaunert, C. (2010) Towards supranational governance in EU counter-terrorism? - The role of the Commission and the Council Secretariat, *Central European Journal of International & Security Studies*, vol. 4 (1), pp. 8-31.
[628] Ibid.
[629] Monar, J. (2006) Cooperation in the Justice and Home Affairs Domain: Characteristics, Constraints and Progress, *Journal of European Integration*, vol. 28 (5), p. 500.
[630] Monar, J. (2010a), op. cit., p. 38.
[631] The Council agreed not to dispute the Commission's proposal for a Directive during the Justice and Home Affairs Council Meeting of 1-2 December 2005, *Council Doc. 14390/05*.
[632] As argued by official of the Swedish Ministry of Justice, see: Ireland to contest data retention law at EU Court. Retrieved 09.01.2017 from: https://euobserver.com/justice/20548.

challenging a policy proposal in front of the CJEU can steer the strategic behaviour of political actors.

2.2.2 Cross-pillarisation and the CJEU rulings on the DRD and PNR

Apart from the fact that the EU institutional actors exploited the pillar ambiguities, the CJEU also contributed to the cross-pillarisation of data retention. While in the ruling on the EU-US PNR Agreement the Court argued that PNR data transfer for law enforcement purposes has to be regulated on a third pillar basis,[633] in the substantially very similar case *Ireland v. Parliament and Council*[634] the Court ruled that data retention for law enforcement purposes has to be based on the first pillar. In this way the CJEU not only created confusion but also influenced the playing field and strategic preference formation of political actors.

After the DRD has been adopted, Ireland challenged its first pillar basis. By referring to the *PNR Agreement* case, Ireland argued that the Directive should have been adopted on a third pillar legal basis since it regulates data retention for law enforcement purposes. The Court rejected the argument brought forward by Ireland claiming that the Directive regulates operations "which are independent of the implementation of any police and judicial cooperation in criminal matters. It harmonises neither the issue of access to data by the competent national law-enforcement authorities nor that relating to the use and exchange of those data between those authorities."[635] Furthermore, "the substantive content of Directive 2006/24 is directed essentially at the activities of service providers in the relevant sector of the internal market, to the exclusion of State activities coming under Title VI of the EU Treaty."[636] At first sight, the Court's interpretation seems to contradict the findings of the *PNR Agreement* case. While both instruments pursue similar objectives, in the case of PNR the third pillar was deemed appropriate while in the data retention case a first pillar basis was considered to be correct.[637] The CJEU explains the difference between the two cases by pointing out that the PNR

[633] Joined Cases C-317/04 and C-318/04 *European Parliament v Council*, judgment of 30 May 2006.
[634] Case C-301/06, *Ireland v. Parliament and Council*, judgment of 10 February 2009, para. 83.
[635] Ibid.
[636] Ibid., Para. 84.
[637] According to an interviewed EU Commission Official this ruling surprised many EU political actors.

Agreement concerned "the transfer of passenger data from the reservation systems of air carriers situated in the territory of the Member States to the United States Department of Homeland Security, Bureau of Customs and Border Protection [CBP]"[638] Consequently, since the Decision regulates the data transfer of private companies to the public authority (namely CBP), the application of Article 3 (2) of Directive 95/46 is triggered stating that in cases related to law enforcement purposes, the Directive does not apply. In contrast, the DRD covers activities of service providers in the internal market and does not contain any rules governing the activities of public authorities.[639] While this observation holds true because the DRD leaves it to Member States to regulate access to data, the judgment has often been criticised because it ignores the fact that the ultimate objective of the DRD is the prosecution and detection of serious crime.[640] In this way, the judgment allegedly lacks consistency compared to the *PNR Agreement* case.[641] Not everyone shares this criticism[642] illustrating the weak and artificial boundary between the pillars. Furthermore, the fact that the Court argued for a first pillar legal basis can also be evaluated as a political statement in the sense that a highly debated topic such as data retention was regarded as better placed in the first pillar environment where more accountability mechanisms existed.[643] Ultimately, the Court decision also set the course for the landmark ruling in *Digital Rights Ireland* which would have not been possible if DRD was regulated under the third pillar.

Although *DRI* dealt with the same Directive as the *Ireland v. Parliament and Council* case, no reference to it is made. In contrast, the AG engages in an intensive dialogue with the 2009 case. He argues that the DRD has a dual functionality. It primarily *harmonises* national rules on data retention that already exist in certain Member States.[644] The AG argues that precisely because of its *harmonising* function,

---

[638] Case C-301/06 *Ireland v. Parliament and Council*, para. 88.
[639] Ibid., para. 91.
[640] In *DRI* the CJEU criticised that the DRD does not provide any safeguards regarding 'access'.
[641] Simitis, S. (2009) Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung. *Neue Juristische Wochenzeitschrift 25*, pp. 1782-1786; Hijmans, H. & Scirocco, A. (2009) Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help? *Common Market Law Review*, vol 46. (5), pp. 1485–1525.
[642] Other academics claim that the interpretation is not inconsistent. See: Böhm, F. (2011), op. cit., p. 112-113. See also: Peers, S. (2011) *Justice and Home Affairs Law*. OUP.
[643] As case intervener in Case C-301/06 *Ireland v. Parliament and Council*, the EDPS argued that in case a third pillar instrument was chosen "the provisions of Community Law relating to data protection would not protect citizens in cases where the processing of their personal data would facilitate crime prevention" (para. 55).
[644] AG Opinion in *DRI*, para. 39; emphasis added by author.

the CJEU was able to rule in 2009 that Article 95 EC was the correct legal basis for data retention. This is because the DRD ensures the proper functioning of the internal market by ending divergent development of existing and future rules.[645] At the same time its secondary function is also to establish a data retention scheme or to make the Member State's system compatible with the DRD.[646] In this way the Directive has a '*creating effect*'.[647]

The AG subsequently pointed out that assessing proportionality in light of Article 5(4) TEU is a difficult undertaking since it raises the question of whether reference has to be made only to the primary objective (internal market) or also to the secondary objective (fighting of crime).[648] This is particularly problematic in the present case since it can be argued that the DRD is disproportionate when looking at its internal market dimension but might be considered proportionate when looking at the prevention of crime dimension: In regard to the primary objective the AG held that the *harmonising* effect of the DRD constitutes an appropriate means in accordance with Article 5 (4) TEU.[649] Nevertheless, the intensity of interference as a consequence of the DRD's *creating effect* is disproportionate to its primary objective of ensuring the functioning of the internal market.[650] Consequently, the DRD "(…) would fail the proportionality test for the very reason which justifies its legal basis. The reason for its legitimacy in terms of its legal basis would, paradoxically, be the reason for its illegitimacy in terms of proportionality."[651] When looking at the secondary objective it might be possible that the DRD can be considered appropriate, necessary and even proportionate in the strict sense.[652] However, ultimately the AG seems to be reluctant to have a clear stance on whether the secondary ground is relevant or not. Consequently, he argues that since proportionality with Article 52 (1) CFREU needs to be established it is not necessary to settle on whether the secondary objective plays a role or not.[653] Although accepting Article 95 EC as legal basis, the AG still indicates a feeling of unease when categorising the DRD unconditionally as a

[645] AG Opinion in *DRI*, para. 42.
[646] Ibid., para. 45; emphasis added by author.
[647] Ibid., para. 47.
[648] Ibid., para. 94.
[649] Ibid., paras. 97 and 98.
[650] Ibid., para. 100.
[651] Ibid., para. 102.
[652] Ibid., para. 104.
[653] Ibid., para. 105.

first pillar instrument. Therefore, he discusses more intensively the law enforcement dimension of the DRD than did the CJEU.

In sum, the CJEU cases discussing the legal basis of the EU-US PNR Agreement and the DRD as well as the opinion of the AG in the *Digital Rights Ireland* case illustrate the difficulty to define the boundary between the pre-Lisbon pillars as well as the implication of the pillar structure on the legality of a measure. Furthermore, the discrepancy between the *Ireland v. Commission and Council* and the *PNR Agreement* case shows the relevance of the CJEU in the pre-Lisbon era in setting the limits for action of policy actors. It has to be noted, though, that legal basis controversies can still play a role post-Lisbon.[654] While post-Lisbon this does not have any relevance for power allocation between legislative actors it has other implications such as whether the EU has at all a competence to act or whether opt-outs for certain Member States are possible.[655]

2.2.3 Legislation-making process after choice of legal basis and power struggles

After having illustrated that the CJEU ruling eradicated any remaining doubts on the first pillar legal instruments, the details of the future legislation were discussed under the ordinary legislation making procedure under fast track. With the aim of enhancing efficiency, Article 251 EC provides the possibility of an early conclusion. While the Treaty does not explicitly mention it, there is a certain extent of discretion to EU institutional actors in shaping the co-decision procedure. This was made clear in the *IATA case* where the Court ruled that the Treaty confers a wide discretion on the Conciliation Committee.[656] While the judgment referred to the second reading conciliation committee, this discretion can be applies *mutatis mutandis* to other aspects of the procedure. Consequently, the EU institutional actors adopted several reports and agreements on the fast-track procedure, which can be regarded as a non-constitutional extension of Article 251 TEC provisions.[657] In NI terms, the fast-track

[654] For example, also in *Opinion 1/15* the AG discusses in-depth the choice of the legal basis since it has implications on the participation of some Member States in the measures (paras. 55 to 135). On the effects of opt-outs, see: Sion-Tzidkiyahu, M. (2008) Opt-Outs in the Lisbon Treaty: What direction for Europe à la Carte. *European Journal of Law Reform*, vol.10 (4).
[655] Chapter 3, section 3.2 of this thesis.
[656] C-344/04 *International Air Transport Association, European Low Fares Airline Association v. Department for Transport*, judgment of 10.1.2006, para. 57 and 58.
[657] For a list of all other relevant acts in regard to informal rules on the co-decision procedure, see: Co-decision and Conciliation - A guide to how the European Parliament co-legislates under the ordinary

procedure can be considered as an informal process which is embedded in the formal institutional framework provided by Article 251 TEC.[658] Due to the increased use of co-decision after the Amsterdam Treaty, scholars started to analyse the conditions for EU institutional actors to engage in informal discussions and the circumstances leading to an early agreement.[659] In addition to that, it has also been assessed how early agreements influence the nature of the law to be adopted.[660] A widely used example of where an early agreement had an impact on the nature of the law is the 2008 Returns Directive.[661] The Directive has often been criticised for its low standards of protection for migrants resulting from the fast-track procedure.[662]

In the case of the DRD, the fast-track procedure and the newly gained EP powers more generally had an effect on the policy outcome by limiting the LIBE Committee's influence. For example, while LIBE was successful in limiting the scope to 'serious crime'[663] the term was not defined in accordance with the EAW as demanded. LIBE also succeeded in removing 'prevention' from the scope of the main text of the directive. However, the reference to 'prevention' remained in the preamble.[664] In regard to the types of data to be retained the LIBE Committee intended to leave it to the Member States to decide whether unsuccessful call attempts are regulated. However, the Council did not give in on this point and thus the directive

---

legislative procedure. Retrieved 09.01.2017 from http://www.europarl.europa.eu/code/information/guide_en.pdf , p. 36-37.

[658] See: Reh, C. et al. (2011) The Informal Politics of Legislation: Explaining Secluded Decision Making in the European Union, *Comparative Political Studies*, vol. 46 (9), p. 1115.

[659] Rasmussen, A. (2008). Time Choices in bicameral bargaining: Evidence from the Co-Decision Legislative Procedure of the European Union. *Paper at 4th Pan-European Conference on EU Politics,* Riga. See also: Reh. C., Héritier, A., Bressanelli, E., & Koop, C. (2005) The Informal Politics of Legislation: Explaining Secluded Decision-Making in the European Union. *Paper at the APSA Annual Convention, 2-5 September*, Washington. See also: Héritier, A. and Reh, C. (2009). Co-decision transformed: Informal Politics, Power Shifts and Institutional Change in the European Parliament. *Paper at UACES Conference on Exchanging Ideas on Europe*, 3-5 September.

[660] See for instance: Ruiter, R. & Neuhold, C. (2012). Why is Fast Track the Way to Go? Justifications for Early Agreement in the Co-decision Procedure and Their Effects. *European Law Journal*, vol. 18 (4), pp. 536-554.

[661] Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, *OJ 2008 L 348*.

[662] Monar, J. (2010a) op. cit.; Acosta, D. (2009). The good, the bad and the ugly in EU migration law: is the European Parliament becoming bad and ugly? *European Journal of Migration and Law*, vol. 11, pp. 19-39 and Ripoll Servent, A. (2006). Setting priorities: functional and substantive dimensions of irregular immigration and data protection under co-decision. *Journal of Contemporary European Research*, vol. 5 (2), pp. 225-242.

[663] Article 1 (1), DRD.

[664] Recital 7, DRD.

requires its retention.[665] The Council also did not agree with LIBE's suggestion of introducing detailed rules on which authority has the right to access data. This area is thus at the discretion of Member States.[666] Ultimately, the Council did not compromise on the retention period. Against both the LIBE Committee and the Commission's suggestion, the Council doubled the period to two years.[667] Additionally, Article 12 even provides for a longer period if "particular circumstances" require it and if the Commission approves it.[668] It can thus be argued that the LIBE Committee lacked assertiveness on the above-mentioned points.

One reason for that is the fast-track procedure as it facilitated that the two biggest EP parties engaged in informal discussions with the Council by excluding the LIBE rapporteur. This is an unusual situation since the rules of the procedure stipulate that the rapporteur is the link between the Parliament and the Council. Furthermore, the two parties also ignored the substantial and procedural concerns of the rapporteur and the LIBE Committee.[669] This is also uncommon since usually MEPs rely on the rapporteur's report given his in-depth knowledge of the topic. There are different explanations for this untypical behaviour during the fast-track procedure and it can be assumed that all played a role to a greater or lesser extent. The first and simplest explanation is that the MEPs of the two majority parties agreed with the Council in regard to the way it suggested to regulate data retention. This goes hand in hand with the interpretation of Claude Moreas who mentioned that MEPs regarded data retention as a matter of urgency.[670] In subsequent years, the growing use of the fast track procedure in AFSJ matters has been interpreted as evidence for the increase of common grounds and dialogue between the EU institutional actors.[671] While this is certainly a possibility it seems to stand in contrast to most other legislative procedures where the EP tended to advocate more for civil liberties than the Council.

A second explanation is related to the EP's 'sensitivity to failure' implying that with the newly gained powers the EP felt the responsibility of being a legislator. More specifically, MEPs were aware of the negative publicity that the EP might have

[665] Article 3 (2), DRD.
[666] Article 4, DRD.
[667] Article 6, DRD.
[668] Article 12, DRD.
[669] As pointed out at the beginning of section 2.2.3 above.
[670] Annual Lecture on the 17th June 2014 of the Centre for Research Into Surveillance and Privacy (CRISP) 'Mass Surveillance, EU Citizens and The State'. Lecture delivered by MEP Claude Moraes at London School of Economics & Political Science.
[671] De Capitani, E. (2010), op. cit.

experienced if it delayed an important legislation.[672] Especially after the bombings in Madrid and London several national governments were proponents of data retention. Thus, it would be difficult for most MEPs 'to sell the delay of process at home.'[673] For example, one MEP expressed his concern that the public expects action to be taken by mentioning that "[p]eople are entitled to have results put in front of them without delay."[674]

Third, the main parties might have prioritized the EP's current and future co-legislative role in AFSJ matters over the substance of the Directive. Institutional bargaining consists of nested games where costs and benefits of on-going negotiations have to be analysed vis-à-vis long-term negotiations.[675] Before 2005, the EP -the LIBE committee in particular- had already been engaged in discussions with the Commission and the Council on data retention. However, the EP's efforts did not result in a change of the Council's course.[676] However, in 2005 the Commission rejected the Council's plan for a framework decision resulting in the Council's compromise to regulate data retention under the first pillar. This was a major success for the EP since it was for the first time a full co-legislator on public security matters. In light of this critical achievement the EP feared that if it delayed the process further the Council would have recourse to its initial plan and adopt a framework decision on data retention. In this way the EP would have lost its newly gained status in AFSJ matters by being only consulted during the legislative procedure.[677] The pressure the EP experienced in this respect is evident in a leaked document from the Presidency to the Parliament[678] and has been confirmed by involved stakeholders.[679]

Besides the fear of being excluded, the EP also considered possible long-term consequences resulting from its performance in negotiating the DRD. In order to

---

[672] Ruiter, R. & Neuhold, C. (2012), op. cit., p. 548.
[673] Ibid.
[674] European Parliament Debate on data retention of 13 December 2005. Retrieved 09.01.2017 from http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20051213&secondRef=ITEM-055&format=XML&language=EN
[675] Tsebelis, G. (1990). *Nested Games: Rational Choice in Comparative Politics*. University of California Press.
[676] See for instance: Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), *2001/2098(INI) final.* See also: The EP's involvement in respect to Regulation 45/2001. For an analysis of the EP's role on the two before-mentioned issues, see: De Capitani, E. (2010), op. cit., p. 129 ff.
[677] Ibid.
[678] Letter from UK Home Secretary Charles Clarke to LIBE Chairman Jean Marie Cavada of 17 October 2005. Retrieved 09.01.2017 from http://www.statewatch.org/news/2005/oct/data-ret-clarke-to-cavada-17-10-05.pdf
[679] Interview with EP official.

convince the EP to swiftly agree, the presidency promised to reach an agreement on data protection in the third pillar which has been a priority for the EP for many years.[680] The presidency also promised to make use of Article 42 TEU in order to extend co-decision in some other AFSJ matters.[681] This might have motivated the EP to compromise on the content of the Directive in order to not endanger its involvement as co-legislator in future AFSJ matters. This shows how fast-track negotiations increase the risk of political 'horse-trading.'[682]

2.3 Summary

By applying NI, as set out in chapter 2, it has been shown that privacy and data protection in respect to data retention was shaped by the institutional framework of privacy and data protection in AFSJ and the way actors exploited and interpreted it. First, it has been shown that the Madrid and London bombings were 'windows of opportunity' for the Council to suggest an instrument on data retention under its exceptional right of initiative. Second, policy-makers made use of cross-pillarisation and respective CJEU proceedings to frame data retention in a way that suited strategic preferences. Ultimately, the newly gained EP powers and the fast track procedure also influenced the way privacy and data protection was shaped in the context of data retention. More specifically, the procedure was marked by a security-bias of the Council -partially due to the UK presidency- and low level of opposition of the EP.

3. The role of the CJEU in shaping privacy and data protection in the context of data retention

In the years following the adoption of the DRD, its transposition triggered legal proceedings in multiple countries:[683] Bulgaria (2010)[684], Cyprus (2011)[685], Czech

[680] De Hert, P., Papakonstantinou, V. & Riehle, C. (2008) Data protection in the third pillar: cautious pessimism. In Maik, M. (ed.), *Crime, Rights and the EU: The Future of Police and Judicial Cooperation*, Justice, p. 163.
[681] The surveillance of telecommunications in the EU (from 2004 and ongoing). Retrieved 25.01.2015 from http://www.statewatch.org/eu-data-retention.htm.
[682] Rapporteur Alvaro feared that the discussions would end up in 'political horse-trading'. See: 'Council pressures Parliament on data retention' of 10.11.2005. Retrieved 09.01.2017 from http://www.euractiv.com/infosociety/council-pressures-parliament-data-retention/article-147671
[683] For an analysis, see for example: Durica, J. (2013) Directive on the Retention of Data on Electronic Communication in the Rulings of the Constitutional Courts of EU Member States and Efforts for its Renewed Implementation. *The Lawyer Quarterly*, vol. 3(2); or: Kosta, E. (2013) The Way to Luxembourg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection. *SCRIPT-ed*, vol. 10(3).
[684] *Decision 8/2014* Bulgarian Constitutional Court Decision of 12 March 2015

Republic (2011)[686], Germany (2010)[687] and Romania (2009)[688]. All courts found that the transposition of the directive was either unconstitutional or overly intrusive.[689] In April 2014 the CJEU declared in the landmark ruling *DRI* the invalidity of the DRD in its entirety and thereby put the practice of pre-emptive data retention as stipulated in the Directive on hold. The case originated from referrals from both the Irish High Court and the Austrian Constitutional Court. In the former case, the Irish NGO 'Digital Rights Ireland' and the referring High Court asked several questions regarding the compatibility of the DRD with fundamental rights. It also asked whether the loyal cooperation principle as laid down in Article 4 (3) TEU requires a national court to assess the proportionality of national implementation measures with the protection afforded by the Charter.[690]

The Austrian case concerned a "class action" brought by 11.231 Austrian Citizens and was led by the NGO 'AK Vorrat' against parts of the implementing act transposing the DRD. The Austrian Constitutional Court referred several questions on the proportionality of the DRD to the CJEU.[691] The CJEU joined the two references for a hearing in July 2013. The ruling was published in April 2014 after Advocate General Cruz Villalón delivered his opinion in December 2013. In the following it is shown that the CJEU follows the inherency approach when assessing the legality of the data retention directive in light of the rights to data protection and privacy. As explained in Chapter 3 this approach is consistent with ECtHR and former CJEU case law and shows the CJEU's path-dependence when analysing privacy and data protection. After assessing the substance of the ruling in accordance with the procedure set out in Chapter 3, its effects will be analysed by arguing that it the judgment reveals conditional 'political actorness'.

---

[685] *Decision 216/14* of the Supreme Court of Cyprus of 27 October 2015.
[686] *Decision Pl. ÚS 24/10* of the Czech Constitutional Court of 22 March 2011.
[687] *Decision 1 BvR 256/08* of the German Constitutional Court of 02 March 2010. De Simone, C. (2010) Putting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German Law Journal*, vol. 11; De Vries, K. et al. (2011) The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)' In: Gutwirth, G. et al (eds) *Computer, Privacy and Data Protection: An Element of Choice*. Springer.
[688] *Decision No 1258* of the Romanian Constitutional Court of 08 October 2009. See: Murphy, C. (2010) Romanian Constitutional Court, Decision No. 1258 of 8 October 2009, *Common Market Law Review*, vol. 47, pp. 933 – 941.
[689] Guild, E. & Carrera, S. (2014). The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive. *CEPS Paper in Liberty and Security* No. 65/May 2014, p. 3.
[690] *DRI*, paras. 17 -18 (The latter question was ignored by the Court)
[691] Ibid., para. 21.

3.1 Digital Rights Ireland and the follow-up case Tele2 Sverige

In *DRI*, the CJEU focused on the question as to whether the DRD is valid in light of Articles 7 and 8 CFREU. It first considers the relevance of those articles with regard to the question of validity of the DRD. The CJEU reasons that Article 8 applies because the retention of data constitutes the processing of personal data.[692] Furthermore, Article 7 CFREU is affected because it requires not only the retention of data but also the access to this data by competent national authorities.[693] Furthermore, the type of retained data, namely traffic and location data, allows "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained (…)."[694] In a second step the Court establishes that the DRD interferes in a "particularly serious" way with Articles 7 and 8 CFREU.

The CJEU states that the interference with Articles 7 and 8 of the Charter is justified since it follows an objective, which is of public interest, and since it does not interfere with the essence of the rights. However, the DRD cannot be considered to be proportionate due to mainly four shortcomings: (i) the purpose and scope of data retention is not sufficiently limited; (ii) no objective criterion exists by which to determine the limits of access to the retained data;[695] (iii) the data retention period is not sufficiently limited because no differentiation is made between the different types of data and their usefulness. Furthermore, the choice of the retention period does not need to be based on objective criteria to ensure that it is strictly necessary;[696] and (iv) no stringent rules exist on data security.[697] Therefore, the CJEU concludes that the directive does not lay down clear and precise rules governing the extent of the interference with the fundamental rights. Thus, the "EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52 (1) of the Charter."[698] There have been debates on the implications of this judgement on the legality of data retention in general. On the one hand the Court criticised severely the indiscriminate character of the DRD hinting at the illegal nature of data retention without the existence of a reasonable suspicion. On

[692] Para. 29. See also: Joined cases C-92/09 and C-93/09 *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, judgment of 9 November 2010, para. 47.
[693] *DRI*, para. 35.
[694] Ibid., para. 27.
[695] Ibid., para. 60.
[696] Ibid., para. 63-64.
[697] Ibid., paras 66 and 68.
[698] Ibid., para. 69.

the other hand, the Court mentioned several safeguards which the DRD did not include indicating that indiscriminate data retention can be proportionate if it includes those safeguards.[699]

Not surprisingly, the uncertainty led to follow-up referrals. In December 2016 the CJEU published its decision in *Tele2 Sverige* which is a joined case resulting from referrals from the Swedish and UK appeal courts. The judgement deals with the question as to whether national legislation on access to data falls under the remit of Article 15 (1) of the e-privacy Directive and whether general data retention can be at all considered proportionate even if it includes all relevant safeguards as stipulated in *DRI*. In a first step the CJEU establishes that any national legislation stipulating the retention of data for public security purposes falls within the remit of Article 15 (1) of the e-privacy Directive.[700] In addition, access to retained data also falls under Article 15 (1) as it is the ultimate purpose of retention and thus the two aspects are intrinsically linked.[701] The Court then interprets Article 15 (1) in light of Articles 7, 8, 11 and 52 (1) of the Charter. After stipulating that the latter has to be interpreted strictly,[702] the CJEU points out that retention is indiscriminate by not differentiating data with regard to a particular time period, geographical area or link to a serious crime.[703] This indiscriminate nature has a particularly negative impact on privacy and leads to a feeling of constant surveillance.[704] The Court does however not specifically mention that preventive data retention is *per se* illegal. Instead if the measure is exclusively aimed for the purpose of fighting serious crime and is sufficiently targeted it can still be regarded as legal.[705] In regard to the latter aspect, two things are pointed out.

First, the CJEU mentions that procedural conditions must be in place to limit the measure. This means that clear and precise rules must exist governing the circumstances and conditions of retention, access and remedies.[706] These safeguards are closely aligned to the ones laid down in *DRI, Schrems* and ECtHR case law: (i)

[699] See AG Opinion on *Tele2 Sverige*, para. 199.
[700] *Tele2 Sverige*, para. 73.
[701] Ibid., para. 79.
[702] Ibid., paras. 89 and 95.
[703] Ibid., para. 106.
[704] Ibid., para. 99 – 100.
[705] Ibid., para. 108.
[706] Ibid., para. 109, see also paras. 19 to 23.

the purpose and scope of data retention must be sufficiently limited;[707] (ii) access to retained data must be subject to prior review by a court or an independent authority;[708] (iii) individuals shall be notified if data has been accessed as long as it does not put the investigation at risk;[709] (iv) the measure must lay down specific rules on data security;[710] (v) review by an independent authority of compliance with the level of protection guaranteed shall exist.[711]

Second, substantive conditions must be in place meaning that there must be a connection between the data to be retained and the objective of fighting serious crime.[712] While this statement implies that indiscriminate data retention is illegal, the Court subsequently specifies that the link has to be 'at least an indirect one'.[713] In practice for instance this could imply using a 'geographical criterion' where the competent national authorities consider one or more geographical areas where a high risk of preparation or commission of such offences could be possible. Another criterion could be to just focus on a particular type of communication service in case that evidence exists that the focus on this type of communication is more effective/efficient in detecting, preventing, or investigating serious criminal offences. Since these are just two examples and the fact that 'an indirect link' is eligible, the judgement leaves the precise limits of what counts as 'indiscriminate' still open and thus some forms of indiscriminate retention might still be legitimate.

3.2 Assessing the CJEU's approach to privacy and data protection in the context of data retention

3.2.1 Interference with Articles 7 and 8 CFREU

As a first step the CJEU focused on assessing whether the retention of traffic and location data as required by the DRD is an interference with Articles 7 and 8 of the Charter. In respect to privacy the Court reasons that "the retention of data for the purpose of possible access to them by the competent national authorities, as provided

[707] Ibid., para. 119.
[708] Ibid., para. 120.
[709] Ibid., para. 121.
[710] Ibid., para. 122.
[711] Ibid., para. 123.
[712] Ibid., para. 110.
[713] Ibid., para.111.

for by Directive 2006/24, directly and specifically affects private life and, consequently the rights guaranteed by Article 7 of the Charter."[714] Subsequently the Court mentions three reasons as to why privacy is not only relevant but also interfered with.

First, the DRD "(…) derogates from the *system of protection of the right to privacy* established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the *confidentiality of communications* and of traffic data as well as the obligation to *erase or make those data anonymous* where they are no longer needed (…)."[715] By framing both Directives as system of protection of the right to privacy the Court neglects that only Directive 2002/58 is aimed at safeguarding privacy through guaranteeing confidentiality of communication (independent on whether communication includes personal data or not).[716] In contrast, Directive 95/46 is mainly concerned with laying down data protection principles while privacy is just one of its final objectives.[717] For example, the CJEU stressed that data subject rights' to erasure or anonymisation when data is no longer needed is a central aspect of privacy. However, it is rather a fair processing principle which is safeguarded under Article 8 (2) CFREU and implemented by the DPD.[718]

Second, the CJEU mentions that since interference with privacy does not presuppose the information to be sensitive or inconvenience the individuals,[719] the mere obligation to retain for a certain period of time data relating to a person's private life constitutes an interference with Article 7.[720] The principle that interference shall

[714] *DRI*, para. 29. See also: C-92/09 and C-93/09 *Volker and Markus Schecke and Eifert*, para. 47.
[715] *DRI*, para. 32; emphasis added by author.
[716] Note that in recital 3 Directive 2002/58/EC mentions generically that the Directive aims to protect the confidentiality of communication and in recital 12 it is mentioned that "[b]y supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy (…)". Note that this is made even clearer in the current proposal to reform the e-privacy Directive where recitals 1 and 2 exclusively focus on the right to privacy and confidentiality of communication. (See: 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), *COM(2017) 10 final*.)
[717] Note that this becomes clear in the GDPR which never refers to the right to privacy. Instead references are exclusively made to data protection. In the DPD references are also made to privacy but as explained in Chapter 3 this relates to the fact that no legal basis to data protection existed at the time when the DPD was adopted.
[718] While only rectification is specifically mentioned in Article 8 (2) CFREU anonymisation or erasure can also be considered as fair processing principle.
[719] *DRI*, para. 33.
[720] para. 34.

not be measured by assessing 'inconvenience to the data subject' or 'sensitivity of data' stems from the *Amann v. Switzerland* and was subsequently re-stated in the CJEU ruling *Österreichischer Rundfunk*. Presumably, this principle has been adopted because it can only be "speculated" as to whether an individual has been or could have been inconvenienced.[721] Thus, it is not a reliable parameter to determine interference. The reason why retention as such already constitutes an interference with privacy is related to the risk of abuse of the data, the feeling of surveillance it generates and the chilling effect it might have on the individual.[722]

Ultimately, Article 7 CFREU is interfered with because the DRD stipulates that access of the competent national authorities to the data has to be granted. Thus, as soon as the public authorities have access to data, 'a further interference' takes place.[723] The fact that the CJEU notes two 'different' interferences shows that retention and access are to be considered separately when establishing an interference and thus logically also when assessing proportionality. In *Tele2 Sverige* the CJEU clarified that although retention and access are to be treated differently in terms of establishing interference this does not mean that 'access' (unlike retention) falls beyond the scope of EU law. The CJEU held that the scope of the e-privacy Directive covers retention and access since the purpose of any retention measure is to make, if required, data accessible to competent national authorities. [724]

In respect to Article 8 CFREU, the CJEU mentions that "(…) such retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article (…)".[725] The Court further reasons that the DRD "(…) constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data."[726] Interestingly, when assessing the relevance of Article 8 CFREU for the case at hand, the Court specifically points out the retention of data without mentioning the access granted to authorities by the DRD. When discussing interference, the court only generically mentions the processing of data. Thus, the importance of data protection in determining the legality of access is

[721] *Amann v. Switzerland*, para. 70.
[722] *DRI*, para. 28.
[723] *DRI*, para. 35.
[724] *Tele2 Sverige*, para. 79 and 80.
[725] *DRI*, para. 29.
[726] Ibid., para. 36.

not sufficiently acknowledged even though later in the judgment references to data protection principles are made when analysing "access". For example, it was stated that no independent oversight mechanism exists to assess whether access to data shall be granted.[727]

By merging Articles 7 and 8 CFREU the Court argues that the interference with both articles is wide-ranging and particularly serious.[728] This is because no real storage requirements are laid down apart from the requirement that data shall be stored in such a way that it can be transmitted to the authorities without undue delay.[729] This seems however mainly an Article 8 CFREU requirement as it refers to data storage which is an aspect of data security. Furthermore, the CJEU argues that Articles 7 and 8 CFREU are both interfered with because retention and subsequent use without the subscriber or registered user being informed is likely to "(…) generate in the minds of the persons concerned the feeling that their private lives are subject to constant surveillance."[730] Here it is unknown whether the Court refers to individuals being informed ex-ante about the indiscriminate retention of data for public security purposes or ex-post if the data of a specific individual has been accessed for public security purposes. The former can be ruled out as users of electronic communication services were informed about the legal requirement to retention when concluding the contract with their service providers.[731] Thus, it is more likely that the court refers to ex-post notification in case the data of individuals has been accessed by law enforcement authorities. Since data protection law does not lay down an ex-post notification requirement this is exclusively a privacy argument (as established with Article 8 ECHR case law)[732] questioning the Court's approach to group this under both Articles 7 and 8 CFREU instead of only the former. The way the CJEU shapes the correlation of privacy and data protection when analysing the interference of both rights is not always consistent making it unclear how privacy and data protection shall be assessed in the proportionality assessment. As mentioned in Chapter 3, the CJEU's

[727] Ibid., para. 62.
[728] Ibid., para. 37.
[729] AG Opinion on *DRI*, para. 77.
[730] *DRI,* para. 37.
[731] While it can be argued that users are not informed due to own negligence when reading contracts with online service providers, in this thesis the view is taken that if the user is informed about certain aspects related to their contract in a transparent manner the "informed-requirement" is met.
[732] For instance in *Ekimdzhiev v. Bulgaria* the ECtHR ruled that individuals need to be notified when they have been subject to surveillance. However, in *Klass and Others v. Germany* the ECtHR mentioned that ex-post notification is not always possible and can be legitimately limited (para. 58).

adoption of the inherency approach shows the CJEU's path dependence to early ECtHR case law.

3.2.2 Justification of interference with Articles 7 and 8 CFREU

The CJEU establishes that the interference was justified by bringing forward four major arguments: (i) electronic communications are a valuable tool in the prevention of offences and the fight against crime; (ii) the DRD pursues the legitimate goals of harmonising Member State practices and fighting serious crime; (iii) the essence of Article 8 is not interfered with; (iv) the essence of Article 7 is not interfered with.

To start with the first two more general points, the court stresses that fighting terrorism and serious crime have been acknowledged as being a matter of general interest since it is a matter of public security.[733] The Court further underpins the importance of public security by stressing that the right to security is laid down in Article 6 CFREU.[734] In addition, the Court mentions that "(…) because of the significant growth in the possibilities afforded by electronic communications (…) data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime."[735] This statement is relatively weak as it emphasises the *growth in possibilities* of electronic communication in justifying its use for crime prevention. Instead the Court should have emphasised the advantages criminals can make of the growing possibilities offered by electronic communications. In a second step the CJEU should then have also discussed the *effectiveness* of using electronic communication in investigating crime. Another critical point is that the Court stresses the advantages of electronic communication for "preventing" crime. Nevertheless, it has to be acknowledged that prevention is only once mentioned in the preamble and is not listed as an objective of data retention under Article 1 DRD.

Turning to the third point the Court argues that the essence of Article 8 CFREU is not interfered with. More specifically the Court mentions that the essence is not infringed since Article 7 DRD provides that "(…) certain principles of data

[733] *DRI*, para. 42. See also: C-145/09 *Tsakouridis*, paras. 46 and 47.
[734] *DRI*, para. 42. While acknowledging Article 6 CFREU as stand-alone article when assessing the justification for interference, the proportionality assessment itself considers security as an exception to privacy/data protection rather than a *sui generis* fundamental right in accordance to the framework established in Chapter 3.
[735] *DRI*, para. 43.

protection and data security must be respected by providers of publicly available electronic communications services or of public communication networks."[736] Thus, Member States are required to ensure that appropriate *technical* and *organisational* measures are adopted against accidental or unlawful *destruction*, accidental *loss* or *alteration* of the data.[737] By specifically pointing out Article 7 of the DRD the CJEU reduces data protection merely to data security. This is striking particularly since Article 8 CFREU does not explicitly mention data security as a core of data protection. Taking Article 8 CFREU as the benchmark, one would at least need to acknowledge fair processing principles, certain data subject rights (i.e. right to access and right to rectification) and independent supervision as parameters to assess whether the core of data protection has been interfered with.

Ultimately, the Court claims that although the DRD constitutes a "particularly serious interference" it does not adversely affect the essence of Article 7 CFREU since the Directive does not allow the acquisition of knowledge of the content of the electronic communication as such.[738] This argument raises interesting questions on whether the clear-cut categorisation of information in 'content' and 'non-content data' makes sense in the contemporary context. It has been pointed out that since traffic and location data can reveal very specific information about the circumstances of a communication, it is possible to create very precise dossiers of individuals including an overview of their movements, their social environment and their habits and interests (via IP addresses).[739] Directive 2002/58/EC acknowledges the special status of traffic[740] and location[741] data by laying down specific safeguards. The CJEU does not sufficiently elaborate on this special status and that traffic and location data can reveal similar information about individuals as content data.[742] This approach is even more surprising since it seems to contradict the earlier finding of the Court where it mentioned that traffic and location data allows for very precise conclusions

[736] Para. 40.
[737] ibid.
[738] Ibid., Para. 39; emphasis added by author.
[739] See for instance: Rauhofer, J. (2006) Just because you're paranoid, doesn't mean they're not after you: Legislative developments in relation to the mandatory retention of communications data in the European Union. *SCRIPT-ED*, vol. 3 (4).
[740] Articles 6 (1) and 5, e-privacy Directive.
[741] Article 9, e-privacy Directive.
[742] Report of the United Nation High Commissioner for Human Rights on the right to privacy in the digital age of 30 June 2014, *A/HRC/27/37*, para. 19. See also: Report of Special Rapporteur (United Nations, General Assembly) on the promotion and protection of human rights and fundamental freedoms while countering terrorism of 23 September 2014, *A/69/397*, para. 53.

concerning the private lives of the persons whose data has been retained to be drawn.[743] One interpretation of this paradox is linked to the CJEU's ambitions to assess also the substance of the DRD. If the Court had found an interference with the essence of Article 7 due to the special nature of traffic and location data, no proportionality assessment of the DRD would have been necessary depriving the CJEU of an opportunity to establish substantive principles in relation to indiscriminate data retention practices.[744] It furthermore shows that the Court does not consider data retention for public security purposes as illegal *per se*.

3.2.3 Proportionality in light of Articles 7 and 8 CFREU

Before engaging in the discussion on the safeguards against abuse of power, the Court first establishes the appropriateness and necessity of the measure. In regard to the former, the CJEU argues that since the importance of electronic communication increased, the DRD allows law enforcement authorities additional opportunities 'to shed light on serious crime' and it is therefore a valuable tool for criminal investigations.[745] Consequently, the CJEU concludes that retention of traffic and location data may be considered to be appropriate for attaining the objective pursued by that directive.[746] When looking at the statistics (although incomplete and inconsistent) on the use of data retention presented by the Commission in October 2013 it becomes clear that law enforcement authorities indeed made use of the data retained under the DRD for the purposes of prosecuting crime.[747] However, the statistics do not reveal whether the data was ultimately useful to convict suspected criminals.

In respect to necessity, the CJEU argues that ensuring public security by fighting terrorism and serious crime may depend on modern investigation techniques.[748] However, regardless of the extent of the usefulness of modern

[743] *DRI*, para. 27. The CJEU mentions that conclusions can be drawn in regard to: habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships and social environments.
[744] Interview with EU Commission official.
[745] *DRI*, para. 49.
[746] ibid.
[747] Statistics on Requests for data under the Data Retention Directive. Retrieved 12.01.2016 from http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/statistics_on_requests_for_data_under_the_data_retention_directive_en.pdf
[748] *DRI*, para. 51.

investigation techniques in safeguarding public security, the latter is not sufficient to justify the measures under the DRD.[749] Instead the CJEU establishes that the respect for private life requires that derogations and limitations to data protection must apply only in so far as strictly necessary.[750] Subsequently the CJEU pointed out that the protection of personal data, especially as enshrined in Article 8 (1) CFREU, is especially important for safeguarding the right to respect private life.[751] In this way the Court applies the inherency approach and reduces the compliance with privacy to the existence of adequate data protection principles. When looking at whether sufficient safeguards against abuse of power exist in three out of four arguments the Court does not differentiate between privacy and data protection and simply refers to "the fundamental rights" or to Articles 7 and 8 commonly.[752]

(i) Scope of application

The Court stresses that the requirement on service providers to retain location, traffic and subscriber data applies to all means of electronic communication and thus entails an interference with 'practically the entire European population.'[753] Furthermore, this retention takes place in a generalised manner without any differentiation, limitations or exceptions[754] and without it being necessary that a link between the data and public security exists.[755] While this indiscriminate nature obviously infringes the data protection principle of non-excessiveness[756] it is not immediately clear why the mere application of data retention to the whole European society leads to the infringement of the 'inner circle'[757] of an individual's private life. Therefore, a second step would have been necessary to this train of thought explaining the *de facto* implications of large-scale retention of *traffic and location data* on the privacy of each individual and the implications for the society as a whole. Since traffic and location data can reveal a detailed picture of an individuals habits and activities and since data is retained of

[749] Note that Member States have constantly failed to provide comprehensive evidence on the usefulness of data retention although this is required under Article 10 of the DRD. Nevertheless, it seems that the CJEU's deliberations would not have been different if more information on the DRD's usefulness would have been provided.
[750] *DRI*, para. 52; emphasis added by author
[751] Ibid., para. 53.
[752] Ibid., paras. 56 and 65.
[753] Ibid., para. 56.
[754] Ibid., para. 57.
[755] Ibid., paras. 58 -59.
[756] As stipulated in Article 6 1 (c) DPD and protected by Article 8 (2) CFREU.
[757] Term used in: *Friedl v. Austria,* Application no. 15225/89, judgment of 31 January 1995; paras. 49-52.

each individual independently of whether a link or suspicion of a link to crime exists this could awaken the data subject's fear that their data can be accessed maliciously, erroneously or because of a wrong suspicion at any time. Especially because no ex-post notification of whether data has been accessed is provided, data subjects have to live with the constant suspicion/fear of their movements, social environment or habits being monitored. While arguably ex-post notification cannot always be provided in the public security context, a measure of such far-reaching scope as the DRD ought to include this safeguard in order to allow individuals to exercise their right to a legal remedy as stipulated in Article 22 of the DPD.[758] Ex-post notification is also necessary to prevent a chilling effect on an individual's willingness to express him/herself. Without ex-post notification it is within the bounds of possibility that data subjects will adapt their behaviours to the likelihood of being watched instead of acting freely without any form of interference. 'Adapting behaviours' could include refraining from searching specific information on the Internet, modifying their interaction with other persons in electronic communication and ultimately it could also have a chilling effect on how they express themselves. All of the previously mentioned aspect could have a negative impact on the identity, personal development and the right to establish and develop relationships with other human beings and the outside world.[759] This is even more relevant in a globalised world where electronic communication has become the main source of most individual's interaction with the outside world. Consequently, generating in the minds of people the feeling of constantly being watched has a negative impact on an individual's self-development and as such has a negative impact on a democratic society as a whole. As such, indiscriminate data retention can have a considerable effect on the right to privacy itself and resulting aspects such as freedom of expression and the development of ones personality.

The CJEU refrains from explaining the above-mentioned *de facto* implications of data retention on individuals weakening the argument. Furthermore, the CJEU indirectly provides some suggestions on how data retention could have been proportionate (i.e. if data pertained to a particular time period, geographic zone, or a person involved in one way or another in serious crime).[760] Some points of this list seem to not definitely preclude indiscriminate retention. For example, it is not clear

[758] *Tele2 Sverige*, para. 121.
[759] As protected by the right to private life. See: *P.G. and J.H. v. the United Kingdom*, para. 56 (with further references).
[760] *DRI*, para. 59.

what "data pertained to a particular time period" means. Would for instance data retention be proportionate if an EU government declares a state of emergency?[761] In this case the retention would still be on a large scale and indiscriminate. Another example refers to the argument of a particular geographic zone. Would data retention be proportionate if in a particular city all data is retained because the presence of a terrorist suspect is assumed?[762] In this case still a vast amount of data needs to be retained and the retention would be indiscriminate in the sense that not only the suspects of crime are concerned. By not having explicitly mentioned that data retention is only possible when data subjects are suspected of a serious crime, the CJEU leaves the door open for indiscriminate retention if sufficient data protection safeguards exist. It is thus clear that the CJEU does not engage in a discussion of the core of privacy which arises from the indiscriminate nature of data retention. Instead it discusses the indiscriminate nature mainly through a data protection paradigm by suggesting safeguard mechanisms that do not completely rule out indiscriminate retention. This approach seems to be confirmed by the *Tele2 Sverige* case.[763]

(ii) Data retention period

Article 6 of the DPD stipulates that personal data shall be retained in a way permitting identification of data subjects for a period that is necessary for the purposes for which the data were collected or for which they are further processed.[764] The DRD translates this provision by merely stating that the retention period should be between six months and two years.[765] The CJEU condemns the fact that this range does not distinguish between the usefulness of the different data sets or the usefulness of the data relating to specific persons. Furthermore, the DRD does not state that the period must be based on objective criteria to ensure that retention is limited to what is strictly necessary.[766] This indicates that a nuanced retention regime would have been acceptable even if the maximum retention period of some data categories was still two years. One example for a more nuanced regime is to lay down a shorter retention period for traffic and location data than for data necessary to trace and identify the

[761] For instance, after the Paris attacks in 2015 France and Belgium declared a state of emergency.
[762] For instance, after the Paris attacks one of the suspects was presumed to be hiding in Brussels.
[763] See section 3.1 of this Chapter.
[764] Article 6 (1e), DPD.
[765] Article 6, DRD.
[766] *DRI*, paras. 63 and 64.

source and destination of a communication.[767] Stricter requirements could have, however, been spelt out when looking at the retention period through the lens of privacy as was done by the AG. He argues that the retention period induces temporal continuity to the DRD and plays a decisive role in classifying the interference with the right to privacy as serious.[768] He argues that a human existence is the convergence of present time and 'historical time'.[769] While admitting that a degree of subjectivity applies he argues that all electronic activity and electronic communications that go beyond one year can be regarded as 'historical time' while everything up to one year can be considered as 'present time'.[770] Particularly since the DRD also lays down a system of extending the ordinary retention period in particular circumstances,[771] the AG is not convinced that an initial period of two years (i.e. retention of present and historical data) is proportionate.[772] The AG's line of argument is less vague than the CJEU's ruling as it categorically rejects any retention period longer than one year. At the same time this approach is however arbitrary since 'historical' and 'present' time could vary greatly depending on the lifestyle of individuals concerned. Furthermore, it is one-dimensional since it does not consider the requirements of law enforcement authorities. For instance, from the perspective of conducting a criminal investigation, this period might be either too short or too long.

(iii) Safeguards on accessing data

The CJEU ruled that the DRD fails to lay down any objective criteria by which to specify access to the retained data.[773] The Directive's only requirement is that access is limited to the purpose of the "investigation, detection and prosecution of serious crime" as defined by Member States.[774] The Court regards this limitation as insufficient and names three substantive and procedural criteria regulating access and subsequent use. First, the Court criticises the fact that the directive leaves a margin to Member States to define the authorities/persons accessing data. The Court states that the DRD "does not lay down any objective criterion by which the *number of persons*

[767] For example the Council of Europe Cybercrime Convention makes a distinction between subscriber data (Article 18) and traffic data (Article 20).
[768] AG Opinion on *DRI*, para. 142.
[769] Ibid.,, para. 146.
[770] Ibid.,, para. 148.
[771] Article 12 (2), DRD.
[772] AG Opinion on *DRI*, para. 151.
[773] *DRI*, para. 60.
[774] Ibid., para. 60. (See Article 1 (1) DRD)

authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued."[775] This wording is quite vague as limiting the *amount* of persons just provides limitation in quantitative terms instead of limiting access to a particular agency. Second, the CJEU criticises the fact that Article 4 DRD does not expressly provide that access and the subsequent use of data must be strictly limited to the purpose of "(…) preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto (…)".[776] Third, the CJEU criticises that the directive does not define the procedures to be followed in order to gain access to the retained data. In this respect, the DRD should have included a provision regulating that access by the competent national authorities to the data retained is made dependent on a prior review carried out by a court or by an independent administrative body.[777] Respectively, supervisory bodies must be able to examine with complete independence whether data processing complies with the requirements of privacy and data protection.[778]

(iv) Data security

While being the only point in the proportionality test where the court exclusively refers to only one fundamental right (namely Article 8 CFREU) the CJEU criticises the lack of data security standards in the Directive. In this regard the CJEU mentions that the DRD fails to specify that data security needs to take the vast quantity, sensitive nature and the risk of unlawful access to that data into account.[779] While the previously mentioned considerations seem to be valid, the CJEU also criticised that since there is not a particularly high level of protection and security required by service providers, they can take economic considerations into account when determining the level of security. This argument can however be criticized since economic considerations are acknowledged to be important under EU law since it is a matter of general interest.[780]

In addition to the above-mentioned point the CJEU also criticises the fact that the Directive does not require that data needs to be stored in the EU. Consequently,

[775] Ibid., para. 62; emphasis added by author.
[776] Ibid., para. 61. It has to be noted that the CJEU refers to prevention although this is not explicitly mentioned as objective in Article 1 DRD.
[777] Ibid., para. 62.
[778] Ibid., para. 62. See also: *Tele2 Sverige*, para. 120 and *Szabó and Vissy v. Hungary*, para. 77 and 80.
[779] *DRI*, para. 66.
[780] As explained in Chapter 3 (section 3.1.3) of this thesis.

data security principles cannot be controlled.[781] While this criticism seems to have been inspired by the political environment during which the judgement was issued (i.e. shortly after the Snowden revelations) it has significant implications for electronic communications, which had previously taken place in a largely borderless environment. The introduction of territorial boundaries to the flow and storage of data has also been reiterated in *Tele2 Sverige*. It was there determined that national data retention regimes shall ensure that data is stored within the respective national territory.[782]

3.2.4 Summary

The aim of Section 3 was to critically assess the CJEU Decision in *Digital Rights Ireland* and *Tele2 Sverige.* It has been demonstrated that the CJEU sticks to the interpretation of the ECtHR by correlating privacy and data protection according to the inherency approach. In this way the CJEU acts in a path-dependent manner in accordance with HI as established in Chapters 2 and 3. Particularly in the proportionality assessment the failure to clearly differentiate the two rights leads to confusion in assessing whether large-scale data retention is *per se* incompatible with CFREU or whether the DRD merely did not include sufficient data protection safeguards. The lack of clarity is also reflected among commentators and policy-makers. While some academics claim that the judgment marks the end of indiscriminate and large-scale data retention, the Commission and Council seem to follow a different approach.[783] The judgment in *Tele2 Sverige* still does not provide a definite answer as to whether and in which form indiscriminate data retention is legitimate. However, at the same time it does further elaborate on safeguards and controversial issues raised by the *DRI* judgment. This includes for example the clarification that indiscriminate traffic and location data retention cannot be regulated on national level as it falls under EU law, the reiteration of the territoriality-requirement of storage and the introduction of notification as a safeguard against abuse of power.[784]

[781] Ibid., *DRI*, para. 68.
[782] *Tele2 Sverige*, para. 122.
[783] As pointed out in an interview with an EU Commission official.
[784] See: *Tele2 Sverige,* paras. 121- 122.

3.3 Digital Rights Ireland as an example of 'political actorness' of the CJEU?

The ruling has often been described as a milestone judgment both by the press and scholars.[785] The CJEU 'dared' to issue a decision with far reaching consequences because it felt empowered by the recent adoption of the CFREU.[786] At the same time the CJEU's decision to annul the DRD was also driven by jurisprudence of national constitutional courts holding that the implementing laws of the DRD were unlawful.[787] In addition, the Snowden revelations led to increasing suspicion against measures facilitating mass surveillance.[788] In this way, *DRI* can be regarded as a response to multiple dynamics including constitutional developments, national jurisprudence as well as the practical implications of data retention and access legislation.[789] These factors certainly provided the CJEU with a justification to deliver such a ground-breaking judgement which had considerable implications for current and future political landscapes.

First of all, to a certain extent the CJEU judgement contributes to European integration in regard to public security. The CJEU argued that that the DRD was disproportionate mainly because of four different reasons: (i) the purpose and scope of data retention is not sufficiently limited; (ii) the Directive fails to lay down any objective criterion by which to determine the limits of access to the retained data; (iii) the data retention period is not sufficiently limited because no differentiation is made between the different types of data and their usefulness; and (iv) the Directive does

[785] See for example: '*Surveillance judgment is a victory for democracy*' Retrieved 28.01.2017 from: http://www.independent.ie/opinion/analysis/surveillance-judgment-is-a-victory-for-democracy-30172786.html or: Granger, M. & Irion, K. (2014) The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection. *European Law Review,* vol. 39 (4), pp. 835-850.
[786] Interview with EDPS official.
[787] It is worth noting that the CJEU followed the German Constitutional Court's deliberations concerning the "feeling of surveillance" generated by the data retention regime. See: BVerfG, 125 BVerfGE 261 and *DRI*, para. 37).
[788] See for example: European Parliament Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, *P7_TA(2014)0230*.
[789] Fabbrini discusses this in terms of vertical dialogue (i.e. when the CJEU reacts directly and indirectly to national court judgments) and horizontal dialogue (i.e. when the CJEU takes political considerations into account). Fabbrini, F. (2015) The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court, *iCourts Working Paper Series*, no. 15, p. 19.

not lay down specific rules on data security.[790] Thus, any future initiatives of data retention will need to be negotiated on the EU level. This is because the same reasons justifying the adoption of the DRD still apply, namely safeguarding the functioning of the internal market and ending/preventing divergent rules across Member States. All four points stressed by the Court show that if a Directive similar to the DRD would be considered, its provisions need to be sufficiently clear and precise. This creates a dilemma since Member States mostly have an interest in minimising EU integration in fields such as activities related to public security. By laying down conditions for a potential future law, the CJEU does not only indicate 'political actorness' but the judgment might result in a more integrationist approach of future policy initiatives.[791]

Second, the referrals of Austrian and Irish Court in *Digital Rights Ireland* can be regarded as providing a window of opportunity for the CJEU to increasingly shape public security matters and its appropriate balance with privacy and data protection. By putting an end to the DRD the Court did not only rule out one type of indiscriminate data retention (i.e. traffic and location data). Instead the ruling created uncertainty regarding the legitimacy of several other data retention regimes. It has to be noted that jurisprudence is in general indeterminate due to the "(…) tension between the abstract nature of the social norm on the one hand, and the concrete nature of human experience on the other. Any particular social situation is in a meaningful sense unique, whereas norms are specified in light of an existing or evolving typology of fact contexts (…)."[792] Nonetheless, it cannot be denied that there are relevant parallels between the DRD and other regimes such as the PNR and SWIFT Agreements.[793] This obviously led to discussions at the policy-making level of the applicability of the findings in *DRI* to those regimes. As a consequence the CJEU was soon faced with a request for an Opinion on whether the EU-Canada PNR

[790] *DRI*, paras 66 and 68.
[791] While the *DRI* ruling does not discuss competency issues, the AG Opinion on *DRI* reveals a clearer bias towards further EU integration. In para. 120 the AG criticises that "access to data" is exclusively a Member State competence. Respectively the AG argues that in order to not render the provisions of Article 51 (1) CFREU meaningless the Union must "(...) assume its share of responsibility by defining at the very last the principles which govern the definition, establishment, application and review of observance of those guarantees [i.e. guarantees to justify the interference with Articles 7 and 8 CFREU]"
[792] Sweet Stone, A. (2002) Path Dependence, Precedent, and Judicial Power. In: Stone Sweet, A. & Shapiro, M. (eds.). *On Law, Politics, & Judicialization*, Oxford University Press, p. 122.
[793] As shown in the subsequent two chapters of this thesis.

Agreement is proportionate in light of *DRI*.[794] Furthermore, other related requests followed such as questions on the general compatibility of data retention for law enforcement with Articles 7 and 8 CFREU. The Swedish Communication Service Provider *Tele2 Sverige* stopped retaining and providing access to law enforcement authorities after *DRI* resulting in court proceedings and the referral to the CJEU. Furthermore, the decision of two UK parliament members to challenge the UK legislation DRIPA (Data Retention and Investigatory Powers Act) was founded on findings in *DRI*.[795] The case can thus be evaluated as having a spill over effect by triggering further cases dealing with similar initiatives. Interestingly, the CJEU's ruling in *Tele2 Sverige* still leaves the question of whether indiscriminate data retention is lawful partially unanswered. This hints at the CJEU's dilemma of, on the one hand, doing justice to its own interpretation of the protection of privacy and, on the other hand, leaving some leeway to policy makers to draft legislation.

Third, 'political actorness' does not only derive from the fact that the DRI judgement triggers cases on similar initiatives. Instead the Court's ruling provides a strategic tool for EU legislative actors to steer policy-making debates according to their strategic preferences. For example in an interview with a Commission official it has been argued that although the Commission is of the view that *Digital Rights Ireland* does not rule out data retention for law enforcement purposes currently no follow-up instrument is proposed due to the concerns that the Parliament might challenge any new measure.[796] In addition to that during negotiations of the recently adopted PNR Directive, the EP frequently referred to *Digital Rights Ireland* findings to support its arguments.[797] Thus, the Court does not only on a case-by-case basis shape privacy and data protection in regard to public security. Instead the CJEU's reasoning has been instrumentalised by legislative actors such as the EP and thus steers political debates.

Conclusion

[794] *Opinion 1/15* Request for an Opinion submitted by the European Parliament on the Draft Agreement between Canada and the European Union on the Transfer and Processing of Passenger Name Record data
[795] Both requests were combined (i.e. *Tele2 Sverige* judgment).
[796] Interview with EU Commission official.
[797] Second Report on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime; *COM(2011)0032*.

The aim of this chapter was to assess how the EU institutional framework shapes data protection and privacy in respect to the DRD. The chapter confirms both Hypothesis 2 and 3 as presented in Chapter 2 of this thesis. To start with, three arguments have been put forward supporting the second hypothesis: "*The EU institutional framework enables EU legislative actors to pursue strategic preferences in the legislation-making process and thereby influences the way privacy and data protection is shaped in the public security context.*" First, it has been illustrated that data retention inititatives were already discussed in the 1990s. However, terror events in conjunction with AFSJ-related institutional particularities functioned as a 'window of opportunity' legitimizing data retention initiatives. Second, it has been shown how the pillar structure encouraged policy-making actors to exploit cross-pillarisation to increase their influence in the legislation-making procedure. Third, it has been shown that granting the EP co-legislative rights led to lower data protection safeguards than initially expected.

Apart from confirming the second hypothesis, two arguments have been put forward to support Hypothesis 3: "*The transitional nature of the EU institutional framework contributed to the CJEU's evolution from a 'legal basis arbiter' to a political actor in its own right that increasingly determines substantial aspects relating to privacy and data protection in the public security context*." First, the pre-Lisbon pillar structure led to an important role of the CJEU as arbiter on legal pillar struggles and has thus become an important strategic tool used by policy actors. Second, it has also been shown that post-Lisbon the CJEU shaped privacy and data protection by ruling on the substance rather than the legal basis of the DRD. It has been demonstrated that the CJEU applies the inherency approach when discussing data protection and privacy in the data retention context. Thus, the Court's reasoning is path dependent to previous CJEU as well as ECtHR case law. This approach left room for interpretation in regard to the question whether pre-emptive data retention for public security could exist in other forms or whether the judgment ruled out similar practices. At the same time, it has been shown that the CJEU's *DRI* ruling can be interpreted as example of 'political actorness' as it may trigger EU integration; has a spill-over effect on similar data retention and access regimes and is used by legislative actors as strategic tool in other legislative debates.

CHAPTER 5 – THE SWIFT AGREEMENT: FROM A SECRET US REGIME TOWARDS A TRANSNATIONAL AGREEMENT

Introduction

In 1973, 239 banks from 15 different countries created the Society for Worldwide Interbank Financial Telecommunication (SWIFT). It is a member-owned cooperative, with the goal of enabling standardized and automated execution of financial transactions. The idea behind SWIFT is to substitute the telex[798] with a more reliable and secure way of sending financial instructions between financial institutions. In practice, when a person instructs a financial institution to send money to a recipient of choice, SWIFT transfers this message. However, not the money but only the instruction is sent through SWIFT.[799] To illustrate how SWIFT operates, the Belgian Data Privacy Commission exemplified its services with envelopes and letters.[800] The envelope contains the customer's information, information of the sending institution, the bank's identifier code, the time and date of the scheduled transfer and information about the other financial institution involved in the transaction. The 'letter' is a codified message containing the amount that is transferred, the identity of the parties, the methods of transfer and again the participating financial institutions. The information from both 'envelope' and 'letter' is stored for 124 days on servers in the EU and on servers in the US.[801]

Nowadays, almost all financial organisations use SWIFT services giving it a systemic character[802] and making it an indispensible tool for banks and the operation of the worldwide financial system as a whole.[803] After 9/11, SWIFT's wealth of

[798] Telex is a network similar to a telephone network serving the purpose of sending text-based messages.
[799] Shea, C. (2008). A Need for Swift Change: The Struggles between the European Union's Desire for Privacy in International Financial Transactions and the United States' Need for Security from Terrorists as evidenced by the SWIFT Scandal. *Journal of High Technology Law*, vol. 8 (1), pp. 143-168.
[800] Belgian Data Protection Authority Opinion on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas. *Opinion No. 37 / 2006* of 27 September 2006, p. 27.
[801] Ibid. The rationale of storing the information in both locations is to avoid data loss. See also: Information Note: EU-US agreement on the processing and transfer of financial messaging data for purposes of the US Terrorist Finance Tracking Programme (TFTP) of November 2009. Retrieved 10.01.2017 from: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/111559.pdf
[802] Connorton, P. (2007). Tracking Terrorist Finance through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide. *Fordham Law Review*, vol. 76 (1), p. 288.
[803] Amicelle, A. (2011) The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the "SWIFT Affair", *Research Questions No. 36, May 2011*, Centre d'études et de recherches internationales, SciencePo, p. 6.

personal information relating to financial transactions was discovered as useful tool for safeguarding public security. Newly introduced US laws required SWIFT to provide personal data to the CIA if administrative subpoenas were issued. While SWIFT had its headquarters in the EU it retains most of its data in the US. Thus, SWIFT was in the midst of contradictory requirements.[804] On the one hand it needed to comply with the obligations generated by the administrative subpoenas[805] issued by US authorities. On the other hand it was obliged to comply with the rights to privacy and data protection in the EU. While SWIFT data was provided secretly to US authorities before 2006, an Agreement between the EU and US was negotiated in 2009 on an interim basis. In 2010, the European Parliament rejected the Agreement thus requiring new negotiations. This led to a new Agreement adopted in July 2010.

The aim of this chapter is to analyse how the EU institutional framework shaped data protection and privacy in relation to the SWIFT Agreement. In line with Hypothesis 2 it is argued that the institutional framework allowed legislators to pursue strategic preferences which in turn influenced how privacy and data protection was shaped. It is further claimed that Hypothesis 3 is partially confirmed since the second SWIFT Agreement does not meet the standards of applicable jurisprudence. However, the likelihood of 'political actorness' of the CJEU is limited due to institutional constraints.

The chapter is structured according to four parts. First, the origins of TFTP and the SWIFT Agreement are explained. Second, three arguments are presented in respect to strategic preference formation of the EP, the Commission and the Council. Third, the provisions of the SWIFT Agreement will be assessed by applying the framework established in Chapter 3. The aim is to analyse whether and how CJEU jurisprudence is applicable to the SWIFT Agreement. Ultimately, it will be explained that timing is critical in determining 'political actorness' and that the chances of CJEU actorness are low.

[804] Pfisterer, V. (2010). The Second SWIFT Agreement between the European Union and the United States of America – An Overview. *German Law Journal*, vol. 11, pp.1173-1190.
[805] Amicelle, A. (2011), op. cit., p. 4: "An administrative subpoena is an order from a government official to a third party, instructing the recipient to produce certain information. Because the subpoena is issued directly by an agency official, it can be issued as quickly as the development of an investigation requires."

1. The emergence of TFTP in the US and EU reactions

The terrorist network behind the attacks on 9/11 relied on the global banking system to finance the execution of the attacks. All hijackers transferred large sums among various accounts in different countries without raising suspicion.[806] Therefore, post-9/11, two crucial laws were adopted to tackle terrorist financing in a direct and efficient manner.[807] First, the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism' (PATRIOT) Act extended the competences of law enforcement authorities to tackle terrorist financing resulting in some extraterritorial powers of those authorities.[808] Second, the Executive Order 13224 was adopted pursuing the objective of interrupting the financial flows from and to Al Qaeda.[809] Executive Order 13224 served as legal basis for the Terrorist Finance Tracking Program (TFTP), which was executed by the CIA.[810] The creation of TFTP was inspired by a discussion between a senior official of the Bush-administration and a Wall Street executive.[811] During the conversation the wealth of financial data contained in the SWIFT database was discussed. Once introduced, TFTP made use of administrative subpoenas when requesting information from SWIFT.[812] The difference between an administrative and judicial subpoena is that the former does not depend on prior judicial authorization. Instead it only has to pass a reasonableness standard test instead of the typical probable-cause test required for criminal subpoenas.[813] According to the judgment in *United States v. Powell*, administrative subpoenas are legal if they fulfil a four- part test[814] and correspond to

[806] A Nation Challenged: Money Trail, U.S. makes Inroads in Isolating Funds of Terror Groups. Retrieved 10.01.2017 from http://www.nytimes.com/2001/11/05/world/nation-challenged-money-trail-us-makes-inroads-isolating-funds-terror-groups.html
[807] Contributions by the Department of the Treasury to the financial war on terrorism, U.S. Department of Treasury, Fact Sheet 2 (2002). Retrieved 10.01.2017 from https://www.treasury.gov/press-center/press-releases/Documents/2002910184556291211.pdf
[808] PATRIOT ACT: Pub. L. No. 107-56, 115 Stat. 272 (2001), codified in 50 U.S.C. para. 1861
[809] Executive Order 13,224, 66 Fed. Reg. 49,079.
[810] Shea, C. (2008), op. cit., p. 151.
[811] *Bank Data Sifted in Secret by U.S. to Block Terror*, published in New York Times 23 June 2006.
[812] Santolli, J. (2008). Note: The Terrorism Financing Tracking Program: Illuminating the Shortcomings of The European Union's Antiquated Data Privacy Directive. *The George Washington International Law Review*, vol. 40, pp. 553-582.
[813] For a more detailed explanation, see: Scherb, K. (1996). Administrative Subpoenas for Private Financial Records: What Protection for Privacy Does the Fourth Amendment Afford? *Wis. L. Rev*, vol. 1075, pp. 1076-85.
[814] The four conditions that need to be fulfilled are: (i) the evidence is competent and relevant for the investigation, (ii) the demand for information is definite, (iii) the purpose of the investigation is authorized by law, (iv) proper administrative steps are followed in issuing the subpoena.

the purpose of the investigation.[815] Since the TFTP was based on Executive Order 13224 the justification for issuing administrative subpoenas to SWIFT of countering terrorism would most likely contribute to a positive test by courts in the US. However, none of the subpoenas has been challenged before a court.

In October 2001, the Treasury Department issued the first administrative subpoena to SWIFT followed by 63 more in the following five years.[816] In order to access the information a multi-step process takes place. First, the subpoenas were always issued when data has been previously sent from EU servers to US servers in order to ensure that the requested data was available and to avoid the applicability of EU data protection laws.[817] Second, the information that was provided by SWIFT in the US was then placed in a "black box". In order to access the information inside the black box the Treasury department made use of a special software. The software enabled the search of SWIFT data on suspicious transactions or on suspected individuals. This search did not take place in real time since a lag exists between requesting the information via a subpoena and the transfer of the information.[818] In accordance with the overall aim of TFTP, the goal of the subpoenas was the investigation of terrorism. However, the definition of terrorism is very broad since according to US law it includes activities which "involve a violent or dangerous act that threatens human life, property or infrastructure; and has the goal of intimidating or threatening the civilian population; influencing the actions of government through mass destruction, kidnapping, intimidation or hostage taking."[819] The administrative subpoenas by the Treasury Department did not specify any individual or particular transaction that the State deemed to be connected to terrorism making it almost impossible to apply effective oversight mechanisms.[820] As a consequence in 2003 SWIFT expressed for the first time a reluctance to continue to react to Treasury requests.[821]

The Treasury Department reacted to SWIFT's concerns by stressing that it

---

[815] *United States v. Powell*, 379 U.S. 48, 57-58 (1964).
[816] Statement released on the SWIFT legal document centre for compliance matters, retrieved 01.10.2017 from www.swift.com.
[817] Santolli, J. (2008), op. cit.
[818] Ibid.
[819] Executive Order 13,224, 66 Fed. Reg. 49,079, Sec. 3.
[820] Prime Minister Condemns SWIFT Data Transfers to U.S. as "Illegal", of June 2006. Retrieved from: http://www.privacyinternational.org/article.shtml.cmd[347]x-347-543789.
[821] *Bank Data Sifted in Secret by U.S. to Block Terror*, published in New York Times 23 June 2006.

will not monitor routine financial transactions such as using an ATM or debit card.[822] Nevertheless, these transactions do not make use of the SWIFT network and thus the Treasury could not get hold of this information in this manner anyways.[823] The Treasury also attempted to provide more detailed justifications in the administrative subpoenas. Nevertheless they still left a large margin of appreciation. For instance, a request was regarded as sufficiently justified if the suspected individual is placed on a terrorist watch list without further investigation.[824] Consequently, the newly introduced safeguard mechanisms can be regarded as relatively weak.

Before 2006, the US obtained bank data from SWIFT without the knowledge of the EU. However, in June 2006, the newspaper *The New York Times* disclosed the existence of the secret TFTP.[825] In the EU the revelations concerning TFTP led to sharp criticism. For instance, the Belgium data protection Commission,[826] the EU Article 29 Working Party[827] and the EP[828] expressed concerns about TFTP's violations of national and EU data protection legislation. Nevertheless, the EU Council was not reluctant to initiate negotiations with US authorities since it also benefited from the TFTP's investigation results.[829] Consequently, in 2009 the first SWIFT Agreement was concluded, followed by the second Agreement in 2010.

2. Shaping privacy and data protection at the legislative level

In accordance with NI, this section focuses on the dynamics between the policy-makers in the process of negotiating the SWIFT Agreement. Three different institutional aspects can be observed. First of all, the role of the ECB and its relationship with other EU level policy actors will be explained. The latter is an

[822] Testimony of Stuart Levey, Under Secretary Terrorism and Financial Intelligence U.S. Department of the Treasury Before the House Financial Services Subcommittee on Oversight and Investigations, Retrieved 10.01.2017 from: Legal Document centre for Compliance matters, www.swift.com.
[823] Ibid.
[824] Santolli, J. (2008), op. cit.
[825] *Bank Data Sifted in Secret by U.S. to Block Terror*, published in New York Times 23 June 2006.
[826]Belgian Data Protection Authority Opinion on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas. *Opinion No. 37 / 2006* of 27 September 2006, retrieved 10.01.2017 from http://www.privacycommission.be/communiquE9s/opinion_37-2006.pdf.
[827] Article 29 WP Press Release on the SWIFT Case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) of 23 November 2006. Retrieved 10.01.2017 from: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2006/pr_swift_affair_23_11_06_en.pdf
[828] European Parliament Resolution on SWIFT, the PNR Agreement and the transatlantic dialogue on these issues of 14 February 2007, *B6-0042/2007 / P6_TA-PROV(2007)0039*
[829] Pfisterer, V. (2010), op. cit.

example on how different EU actors operate in different normative paradigms leading to different value judgments and uncoordinated actions. More specifically, the fact that there was no *conceptual agreement* on the value of data protection and civil liberties more generally led to asymmetries of information before the revelation of the SWIFT affair in 2006. Second, the role of the EP in the legislation-making procedure illustrates that *power aspirations* were prevalent during the negotiations towards the first and second SWIFT Agreement. This explains why the EP agreed to the second Agreement even though not all of its requests were met. The third section shows how actors engaged in *strategic transgovernmentalism* in order to increase the strength of their mandate in the negotiations.

2.1 Disjointedness of EU institutional frameworks

As described earlier, the main EU institutional actors were not informed about the access of US authorities to EU financial data before 2006. Nevertheless, investigations by the Belgium data protection authority, the Article 29 Working Party and the European Data Protection Supervisor revealed that the European Central Bank (ECB) had been informed about the data transfer to the US from the start since it belonged to the SWIFT supervisory committee.[830] The G10 Group established an oversight mechanism in order to avoid any risks to financial stability and the integrity of financial infrastructures.[831] Although the ECB belongs to the G10 Group and was consequently informed about the data transfer since 2002 it did not notify any other European institutional actor. This non-disclosure conflicts with Article 13 (1) and (2) TEU respectively. Article 13 (1) TEU states that all institutional players shall aim to promote EU values and serve the interests of EU citizens and ensure consistency, effectiveness and continuity of its policies. By accepting silently the data transfer from EU citizens to the US the ECB failed to ensure consistency since the data transfer appears to conflict with the existing EU legal framework on data protection and privacy. Secondly, Article 13 (2) TEU establishes that "[t]he institutions shall practise mutual sincere cooperation."[832] By not informing other institutional actors, the

[830] Article 29 Data Protection Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT); EDPS Opinion of 1 February 2007 on the role of the European Central Bank in the SWIFT case.
[831] EDPS opinion of 1 February 2007 on the role of the European Central Bank in the SWIFT case.
[832] Article 13 (2), TEU.

ECB's non-disclosure of the TFTP's existence also contradicts the provisions of Article 13 (2) TEU.

Justifying the non-disclosure, the ECB referred to the strict secrecy rules of the G10 Group's supervisory committee.[833] Furthermore, it argued that breaches of data protection rules were not in the mandate of the ECB's oversight function and that SWIFT is not a financial institution but a communications platform. Therefore the overseeing function of the ECB is more directed towards moral standard-setting within SWIFT as well as ensuring that no risk to financial stability exists instead of explicitly influencing the company.[834] The EDPS challenged this narrow interpretation.[835] He claims that, the "rules of professional secrecy should not prevent independent scrutiny by data protection supervisory authorities, which is one of the basic principles of European data protection law."[836] The different views on the ECB's responsibilities as a member of SWIFT's oversight board illustrates that actors are guided by different institutional frameworks in their preference formation. By referring to merely mandate-related issues, the ECB reveals that its strategic preference formation relates to aspects of financial regulation rather than data protection. In contrast, the EDPS as well as the European Parliament are structuring their preferences around the institutional framework related to data protection and privacy. This illustrates the disjointedness of different EU institutional frameworks and how this impacts upon the strategic choices of actors.

It is also interesting to note that some officials of the G10 Group decided to inform their governments about the existence of the TFTP.[837] In addition, other Member States where informed about the TFTP through informal bilateral relations.[838] Nevertheless, none of the informed Member States contacted the relevant EU authorities. An US official argued that the Member States preferred to sideline the EU institutional actors because Member States benefited from the investigative results of

[833] Article 38, Protocol on the Statute of the European System of Central Banks and the European Central Bank annexed to the TEU and the TFEU. *OJ 2010 C 83*. Read in conjunction with Memoranda of Understanding (MoU) between the National Bank of Belgium and the central banks co-operating in the oversight of SWIFT. Information about MoU available at www.swift.com.
[834] EDPS Opinion of 1 February 2007 on the role of the European Central Bank in the SWIFT case.
[835] ibid.
[836] ibid.
[837] Amicelle, A. (2011), op. cit., p. 13.
[838] As indicated by the European Coordinator in the fight against terrorism during the conference: *The exchange and storage of data*, Science Po, Paris, 10-11 October 2008.

the TFTP programme and feared EU opposition.[839] The situation illustrates that there is both a lack of practical coordination between Member States and EU authorities as well as between different EU institutional actors. This reveals the rudimentary state of affairs regarding EU inter-institutional cooperation and coordination in the 'SWIFT affair'. Furthermore, it shows that the EU institutional actors do not have a coherent view on the value of data protection in the international context.

2.2 Legislation-making procedure and power struggles

After the existence of the TFTP has been disclosed, the US made representations to the EU explaining the programme's legal basis in the US.[840] Subsequently, the Council authorised the Presidency assisted by the Commission to enter into negotiations with US authorities in accordance with pre-Lisbon Article 24 (1) TEU and 38 TEU. The goal of these negotiations was to create a legal basis for the previously secretly executed bank data transfers to the US through SWIFT. Four months after the start of the discussions an Interim Agreement[841] was concluded just one day before the Lisbon Treaty entered into force. The Council and Commission's expedited negotiation procedure can be interpreted as a deliberate move. The pre-Lisbon decision-making procedure did not provide the EP with the right to vote in external security matters as it exclusively foresees approval by the Council.[842] This means that the Agreement was concluded under the intergovernmental process of the old third pillar excluding the EP.[843] This changed after the implementation of the Lisbon Treaty entitling the EP to participate in the decision-making process.[844]

Concluding the Agreement just one day before Lisbon intensified the tensions between the Parliament and the Commission and Council, which was expressed in several ways. First, the EP criticized the substance of the Agreement on various

[839] Interview with US official.
[840] Terrorist Finance Tracking Program, Representations of the United States Department of the Treasury *OJ 2007 C 166/18*.
[841] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program *OJ 2010 L 195/5*
[842] Pfisterer, V. (2010), op. cit.
[843] Although before Lisbon the EP did not have any competence in decision-making procedures of agreements in AFSJ, it still aimed at maximizing its power in other ways. See: Santos, J. (2013). The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon. *Centre for the Law of EU External Relations (CLEER) Working Papers 2013/2*, pp. 1-31.
[844] Article 218 (6) (2) (a) TFEU.

grounds, such as the lack of EU data protection standards, the lack of procedural rights granted to EU citizens, its disproportionality, and lack of reciprocity.[845] Second, the procedure was regarded as dishonourable vis-à-vis the EP because the Council and Commission deliberately excluded the Parliament from the policy-making process.[846] Third, the EP also criticized the fact that the Agreement was forwarded only after its conclusion with a considerable delay. Thus, the EP had less time to review the provisions before it was able to vote on it in February 2010.[847] The lack of cooperation between the EU institutional actors was still a concern in 2014 –long after the SWIFT Agreement entered into force. In the EP Resolution of 12 March 2014 the Parliament requested that all relevant information and documents relating to the SWIFT Agreement should be made available to the Parliament. This request has been ignored by the Council illustrating the ongoing lack of cooperation.[848] In July 2014 the Court ruled in *Council v. In 't Veld* on transparency and access to files related to SWIFT and TFTP. The CJEU argued that the Council has some discretion in deciding whether the disclosure of a document effectively harms the public interest.[849] However, the Council must provide detailed information on why it withholds these documents.[850] The Council provided two justifications, (i) protection of international relations and (ii) legal advice, which were both rejected by the Court.[851] The CJEU mentioned that any limitations to disclosure of documents must be "reasonably foreseeable and not purely hypothetical."[852] Respectively, the Council failed to provide evidence on how the disclosure of the document would "specifically and actually" threaten the protection of the two interests identified by the Council.[853] This judgment can be seen as a victory of the EP vis-à-vis the Council in the sense that the Court acknowledged the unjustified exclusion of the EP from the negotiation process and from access to information. Furthermore, it also illustrates how the CJEU is

[845] European Parliament Motion for a Resolution of 5 May 2010 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing. *B7-0038/2009*.
[846] Pfisterer, V. (2010), op. cit.
[847] This delay was explained with translation issues by the Council and Commission. See: Monar., J. (2010b). Editorial Comment. The Rejection of the EU–US SWIFT Interim Agreement by the European Parliament: A Historic Vote and Its Implications. *European Foreign Affairs Review*, vol. 15, p. 143.
[848] European Parliament Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, *2013/2188(INI)*.
[849] Case C-350/12 P, *Council v. In 't Veld*, judgment of 3 July 2014, para. 106.
[850] Ibid., para. 52.
[851] Ibid., para. 54.
[852] Ibid., para. 102.
[853] Ibid., para. 101.

actively involved in steering political processes as its judgements are instrumentalised by political actors.

When the Interim Agreement of 2009 was due to be made permanent in 2010, the EP retroactively got the right to vote on it in February 2010.[854] The vote resulted in the rejection of the Agreement with 378 in favour to 196 votes against and 31 abstentions.[855] "It did so against appeals from the Commission and the EU Presidency, against significant pressure from several Member States and against an unprecedented direct lobbying from the US side, and it did so both on grounds of protecting citizens' safeguards regarding the transfer and use of personal financial data and for affirming its own prerogatives."[856] By flexing its muscles in this way, "[i]t is not difficult to conclude that the behaviour of the EP exhibits elements of a 'turf war' for more power and influence."[857] This is also reflected in the press and in political discourse. It was frequently mentioned that the rejection of the SWIFT Agreement is a milestone showing the EP's newly gained influence in the decision-making procedure as well as a victory against the Council, the Commission and civil liberty-intrusive practices.[858]

Subsequent to the rejection, the Parliament issued a Resolution that expressed its privacy and data protection concerns to the Commission and the Council.[859] Based on this document, the Council mandated the Commission to start new negotiations with the US Treasury Department.[860] The new negotiations led to a revised Agreement which was formally adopted on 13 July 2010.[861] It can be argued that the Parliament consented to the terms of the new agreement due to two equally important reasons.

---

[854] Due to Article 24 (5) TEU the SWIFT Agreement was only provisional and with the entry into force of the Lisbon Treaty all provisional legislation automatically needed to be agreed under new procedures.

[855] Debate of the European Parliament about the Agreement between the EU and the USA on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme, *CRE 10/02/2010*.

[856] Monar., J. (2010b), op. cit, p. 143.

[857] Pawlak, P. (2009b). Network Politics in Transatlantic Homeland Security Cooperation. *Perspectives on European Politics and Society*, vol. 10 (4), pp. 560-581.

[858] For instance: MacKenzie, A. (2011). A US Driven Security Agenda? EU Actorness in Counter-Terrorism Co-operation with the US. Paper presented at *EUSA Twelfth Biennial International Conference Boston*, *Massachusetts*. See also: MEPs say 'no' to SWIFT. Retrieved 10.01.2017 from http://www.euractiv.com/justice/meps-swift-news-258160

[859] European Parliament Resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorize the opening of negotiations for an Agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing. *Eur. Parl. Doc. 0129*.

[860] Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program. *OJ 2010 L 195/3*, recital 1.

[861] In accordance with: Articles 218 (2) and (6)(1) TFEU.

First, there were improvements in data protection standards and secondly, it felt fully informed and integrated in the negotiation process.[862] However, as discussed later in this chapter, the second SWIFT Agreement also raises several data protection concerns. In this respect, it can be argued that power aspirations played a more important role than the actual improvement of the Agreement's provisions.[863] An alternative interpretation of the Parliament's agreement to the second Agreement is that the EP realised that it is with its newly gained powers responsible to the Member States security concerns.[864] This last point shows that the EP became '*sensitive to failure'*.[865]

2.3 EU's negotiation power and transgovernmentalism

The degree of strategic and procedural coherence of EU institutional actors has a significant impact on the performance of the EU as an international player.[866] Since the Lisbon Treaty entered into force, the EP is an important player in the decision-making process. In general neither the Council nor the Commission can take the support of the EP for granted. While in democratic parliamentary systems the government is usually supported by a parliamentary majority this is not the case in the EU. This implies that in order to appear as a strong negotiator when discussing international agreements, the Commission and the Council need to have strong communication and consultation procedures in place in order to build a majority within the EP.[867] However, as pointed out in the previous section in the case of SWIFT, struggles between EU institutional actors and conceptual disagreement have prevented effective communication and majority building between Council,

[862] Santos, J. (2013), op. cit., p. 18.
[863] Ibid.
[864] Servent, A. & MacKenzie, Al (2011). Is the EP Still a Data Protection Champion? The Case of SWIFT. *Perspectives on European Politics and Society*, vol. 12 (4), pp. 390-406. See also: Servent, A. (2014). The Role of the European Parliament in international negotiations after Lisbon. *Journal of European Public Policy*, vol. 21 (4), pp. 568-586 and Kaunert, C., Léonard, S. & MacKenzie, A. (2012) The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT, *European Security*, vol. 21 (4), pp. 474-496.
[865] See also in Chapter 4, section 2.2.3.
[866] Gebhard, C. (2011). Coherence. In: Hill, C. & Smith, M. (eds.). *International Relations and the European Union*. Oxford University Press.
[867] Monar., J. (2010b), op. cit, p. 147.

Commission and the EP. Thus, the EU did not act with a coherent mandate while being confronted by US counterparts.[868]

It has to be acknowledged that the US was naturally in a stronger negotiation position. This is due to the fact that US legislation stipulates the importance of high international standards in the fight against terrorism. In this way, the US put itself in the position of an agenda-setter and catalyst while the EU is more reactive and acts as a norm-taker.[869] Additionally, the SWIFT Agreement was 'the extended arm' of an already existing US policy (i.e. TFTP) as described at the beginning of this chapter. Consequently, the SWIFT Agreement did not have to pass the usual legislative hurdles in the US as was the case in the EU. In addition to the latter situation, the US negotiators were also able to take advantage of the EU's fragmentation to assert counter-terrorism measures that do not comply with EU data protection standards. [870]

The US took advantage of this situation in two ways. First, it built strategic alliances on an informal basis with actors from the Council and the Commission. Second, it tried to lobby members of the EP which had reservations about the SWIFT Agreement. In regard to the first point the US and EU established in 2004 the High-Level Political Dialogue on Border and Transportation Security (PDBTS). The aim of this forum was to informally discuss new security policies that might be regarded as controversial by the EU or US authorities. The network is mainly composed of officials dealing with security on the US side (Department of Homeland Security) and by the relevant Council and Commission security officials (Council Presidency and Commission DG's). Several discussions in the PDBTS framework provided US and EU actors with the opportunity to exchange information and build trusted relationships.[871] The combination of information exchange and building trust through PDBTS help to "push things forward" in security cooperation.[872] In addition to this forum, the High-Level Contact Group on data protection (HLCG) was established by

[868] Argomaniz, J. (2009) When the EU is the 'Norm-taker: The Passenger Name Records Agreement and the EUs Internalization of US Border Security Norms. *Journal of European Integration*, vol. 31 (1), pp. 119-136.
[869] US as catalyst, see: Pawlak, P. (2009a). Made in the USA? The Influence of the US on the EU's Data Protection Regime *CEPS, November 2009* pp. 1-28. EU as norm-taker, see: Argomaniz, J. (2009), op. cit., p.119. For this point, see also: Kaunert, C., Léonard, S. & MacKenzie, A. (2012) The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT, *European Security*, vol. 21 (4), pp. 474-496.
[870] Missiroli, A. (2001). European Security Policy: The Challenge of Coherence. *European Foreign Affairs Review*, vol. 6 (2), pp. 177-96.
[871] Pawlak, P. (2009a), op. cit., p. 12.
[872] Ibid.

a decision of the EU-US Justice and Home Affairs Ministerial Troika on 6 November 2006. The goal of this group was to bring EU and US policy-makers together to achieve similar effects on data protection like those created on security by PDBTS. The group consisted of senior officials from the Commission, the Council presidency and the US Departments of Justice, Homeland Security and State.[873] Both the PDBTS and the HLCG did not foresee the participation of Members of the EP or of the data protection authorities. Therefore, the emphasis in discussions was primarily on security and to a lesser extent on data protection and civil liberties. In this way, organisational homogeneity between EU and US 'securocrats'[874] was created. Consequently, an alliance between EU Commission and EU Council and the US emerged while in the EU internally the rivalries and conflicts between these EU institutional actors and the EP were aggravated.[875] The reasons for the nature of this informal relationship between the US and the EU can be interpreted in two ways: (i) there was a natural transnational coalition building due to similar attitudes of the actors on security related issues; (ii) the US authorities focused on coalition building with the Commission and the Council since they perceived those actors as most relevant in the legislation-making procedure.

A second way the US authorities dealt with fragmentation among EU institutional actors was its focus on lobbying the EP. When the US administration discovered the possible rejection of the interim Agreement, the Secretary of State attempted to convince the EP President of the importance of the SWIFT Agreement. Furthermore, the US authorities offered the LIBE Committee an in-depth briefing on the purpose of TFTP and the SWIFT Agreement and more intense strategies were applied. The US Treasury also expressed a warning to the EP that a rejection of the SWIFT Agreement would be a 'tragic mistake' and the US Ambassador to the EU warned the EP that the US would potentially bypass the EU via bilateral agreements with the EU Member States.[876] In addition, the Council President and the Commission tried to urge the Parliament to agree to the SWIFT Agreement by attending the EP

[873] Ibid.
[874] Ibid. Term used by Pawlak, P. (2009a) op. cit., to describe political officials that deal with security-related matters.
[875] Pawlak, P. (2009b), op. cit.
[876] Clinton Presses European Parliament to Back Terror Data Deal. Retrieved 10.01.2017 from: http://www.eubusiness.com/news-eu/us-attacks-banks.215

plenary session. In return for agreeing to the SWIFT deal they offered the EP access to classified documents.[877]

Notwithstanding the efforts of the US administration the Parliament ultimately rejected the SWIFT Agreement. However, the EP approved the second Agreement although it did not comply fully with EU data protection standards either. Before agreeing to the second Agreement the US adopted a different lobbying effort. Instead of urging and threatening the Parliament a "US charm offensive"[878] took place. Among others, MEPs were invited to Washington and the US Vice-President delivered a speech about the SWIFT Agreement to the EP two months before the second Agreement was discussed in the plenary session.[879] Consequently, actively including the EP and regarding it as an equal actor might have contributed to the Parliament's more uncritical acceptance of the Agreement's critical provisions. It can even be argued that the new way of lobbying led to norm internalization of US values by the EP.[880]

In sum, it has been shown that dynamics between EU institutional actors are crucial for determining how the EU performs when negotiating international agreements. It has been demonstrated that while the US was generally in a better starting position, it also took advantage of EU internal power struggles and conceptual disagreements through alliances building and the application of strategic lobbying. Ultimately, this does not only affect the EU's counter terror strategy but it might also harm the EU's international credibility since third parties might question the EU's status as respectable negotiation partner.[881]

2.4 Summary

So far this chapter has focused on how the EU institutional framework shaped data protection and privacy in respect to the formation stage of the SWIFT Agreement. It has been demonstrated that the EU institutional framework has provided space for strategic preference formation in three ways: (i) the fact that the principle of sincere

[877] New Offer to Save EU-US Data Deal. Retrieved 10.01.2017 from: http://www.politico.eu/article/new-offer-to-save-eu-us-data-deal/.
[878] Cremona, M. (2011b). Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement. Institute for European Integration Research. *Working Paper No. 04/2011*, p. 19.
[879] Ibid.
[880] Servent, A. & MacKenzie, A. (2012). The European Parliament as a 'Norm-Taker'? EU-US Relations after the SWIFT Agreement. *European Foreign Affairs Review*, vol. 17, pp. 71–86.
[881] Monar, J. (2010b), op. cit, p. 143.

cooperation between institutional actors was not complied with before SWIFT entered on the agenda can be ascribed to the fact that actors were subject to different institutional frameworks impacting preference formation; (ii) the institutional framework encouraged power struggles between the EP and the Council; and (iii) the institutional framework led to strategic transgovernmentalism between EU and US actors.

3. The applicability of existing case law on the SWIFT Agreement

The first SWIFT Agreement has been criticised for breaching EU law[882] while the second Agreement was often deemed to comply with EU data protection and privacy standards.[883] In the following it will be assessed whether and at which extent CJEU and relevant ECtHR jurisprudence is applicable to the SWIFT Agreement. Subsequently, the CJEU's political actorness will be assessed in a separate section.

When assessing the interference with Articles 7 and 8 CFREU it is argued that Article 7 is interfered with since the SWIFT Agreement permits the access to financial messaging data by US national authorities. Furthermore, this interference is particularly serious since the categories of data to be transferred can reveal a detailed picture of a person's private life. Article 8 CFREU is interfered with since data is processed under the Agreement. The interference of both rights can be justified since fighting terrorism has been acknowledged as being a matter of public security. Subsequently, a proportionality assessment is conducted in respect to both rights in accordance to the framework established in Chapter 3.

3.1 Interference with Articles 7 and 8 CFREU

3.1.1 Interference with Article 7 CFREU

First of all, it needs to be specified whether the data at stake can be classified as personal data revealing information about the private life of the data subjects. Under

[882] European Parliament Resolution on the Recommendation from the Commission to the Council to authorize the opening of negotiations for an Agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing. *Eur. Parl. Doc. 0129/ 2010*.
[883] For instance: MacKenzie, A. (2011). A US Driven Security Agenda? EU Actorness in Counter-Terrorism Co-operation with the US. Paper presented at *EUSA Twelfth Biennial International Conference Boston*, *Massachusetts.*

the SWIFT Agreement, data on financial transactions may include personal information such as: "identifying information about the originator and/or recipient of the transaction, including name, account number, address and national identification number."[884] To establish an existence of an interference with the right to privacy, it does not matter whether the "(…) information in question is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference."[885] Thus, the mere fact that data is accessed by public authorities without allowing the individual the opportunity to refute it amounts to an interference with Article 7 CFREU.[886] While the previous findings derive from case law in relation to EU acts they apply *mutatis mutandis* to international agreements concluded by the EU since the lawfulness of such agreements depends on their compliance with fundamental rights protected in the EU legal order.[887] Based on the foregoing it can be concluded that since the SWIFT Agreement grants US authorities access to requested personal data stored in the territory of the European Union this amounts to an interference with Article 7 CFREU.

On previous occasions, the Court stated that an interference is "particularly serious" if two conditions are met. First, if the data is retained and used without the knowledge of the data subject as it generates "in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[888] Through the publication of SWIFT Agreement in the Official Journal of the European Union citizens have the opportunity to be informed ex-ante about the potential use of their financial data when making transactions. Furthermore, Article 15 of the SWIFT Agreement stipulates ex-post notification by mentioning that "any person has the right to obtain, following requests made at reasonable intervals, without constraint and without excessive delay at least a confirmation (…) whether any processing of that person's personal data has taken place in breach of this Agreement."[889] Persons may also be able to get access to their personal information processed under the Agreement but this might be subject to limitations to safeguard the prevention,

[884] Article 5 (7), SWIFT II Agreement.
[885] *Schrems*, para. 87; *DRI*, para. 33; *Österreichischer Rundfunk and Others*, para. 75.
[886] *DRI*, para. 35. In regard to Article 8 ECHR see also: *Leander v. Sweden*, para. 48; *Rotaru v. Romania*, para. 46 and *Weber and Saravia v. Germany*, para. 79.
[887] AG Mengozzi on *Opinion 1/15,* para. 171.
[888] *DRI*, para. 37.
[889] Article 15 (1), SWIFT II Agreement.

detection, investigation and prosecution of crime.[890] While this allows individuals to obtain information on whether their data has been processed under the SWIFT Agreement, it is regrettable that no automatic ex-post notification takes place once it is no longer liable to jeopardise the investigations undertaken by authorities.[891]

Second, interference is 'particularly serious' if it is considered to be wide-ranging.[892] On the one hand, interference is not limited to what is strictly necessary since SWIFT is not in a position to filter out all irrelevant data before transferring it to the US.[893] On the other hand, interference is not wide-ranging in a sense that all data is transferred indiscriminately. This is because personal data needs to be requested by US authorities and approved by Europol before it is transferred and accessed by US authorities. When data is requested sufficient reasons need to be provided on why the data is relevant in the fight against terrorism and its financing. Consequently, it can be argued that interference under SWIFT does not qualify as wide-ranging in the narrow sense but may well be qualified as wide-ranging when considering that data has to be delivered in bulk due to technological reasons.

3.1.2 Interference with Article 8 CFREU

Article 8 CFREU is interfered with if a measure stipulates the processing of personal data.[894] According to the GDPR "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[895] It has to be noted that the initial 'collection' of data by SWIFT does not amount to an interference under the scope of the Agreement as this is related to commercial activities carried out by banks and thus does not relate to processing under the Agreement itself.[896] However, other forms of processing are at stake. First, the Agreement stipulates the transfer of the data to US authorities

[890] Article 15 (2), SWIFT II Agreement.
[891] *Tele2 Sverige*, para.121
[892] *DRI*, para. 37.
[893] See more details in section 3.3.1 below on 'access to data'.
[894] *DRI*, para. 36. See also: *Volker and Markus Schecke and Eifert*, para. 60.
[895] Article 4 (2), GDPR.
[896] See AG Mengozzi on *Opinion 1/15*, paras. 177 - 179.

(disclosure by transmission). Second, the Agreement regulates the 'access' and 'use' of the data after the data has been transferred. Ultimately the SWIFT Agreement regulates the 'storage' and 'destruction' by US authorities.

3.2 Justification for interference with Articles 7 and 8 CFREU

Interference with Articles 7 and 8 CFREU can be deemed justified in accordance with Article 52 (1) CFREU if three conditions are met. First, it needs to be 'provided for by law.' As the Agreement was concluded according to procedures set out in Article 218 TFEU the Agreement qualifies as an'international agreement' under the Treaties. Both ECtHR and CJEU case law have confirmed that international agreements are automatically incorporated into national law and an integral part of the EU legal order.[897] Thus, the Agreement is provided for by law.

Second, interference is justified as long as the essence of a right is not interfered with. Personal data collected under the SWIFT Agreement can reveal a detailed picture of a person's life similar to traffic and location data. It reveals the location and identity of recipient and sender and the transferred amount provides insights in the financial status of the data subject giving a precise view on his funds and spending. Furthermore, it allows drawing detailed conclusions about a person's social environment, activities or movements. While the special status of the data has to be acknowledged the essence of Article 7 CFREU is not interfered with since the data in question is limited to patterns in relation to financial transactions between EU and non-EU countries. Therefore, no precise conclusions on the essence of an individual's private life can be drawn. Furthermore, the SWIFT Agreement also includes numerous data protection principles as explained in the next section. Therefore, the essence of Article 8 CFREU is not infringed either.[898]

Third, the reason for interference needs to follow an objective of general interest. Fighting terrorism has been acknowledged as being a matter of general

[897] See: *Neulinger and Shuruk v. Switzerland*, Application no. 41615/07 of 6 July 2010, para.99; *Fernández Martínez v. Spain*, Application no. 56030/07 of 12 June 2014, para. 118; See also: C-308/06, *Intertanko and Others* of 3 June 2008, para. 42 and C-401/12 *Council and Others v Vereniging Milieudefensie and Stichting Stop Luchtverontreiniging Utrecht* of 3 January 2015, para. 52.
[898] *DRI*, para. 40.

interest since it aims to maintain international peace and security.[899] Furthermore, law enforcement and governmental authorities found financial messaging data to be a useful tool to fight crime.[900] Therefore, the SWIFT Agreement pursues a legitimate goal. Nevertheless, fighting serious crime such as terrorism 'however fundamental it may be' cannot justify general and indiscriminate access to data.[901] In regard to the SWIFT Agreement, data access is however not indiscriminate in the narrow sense as outlined above.

3.3 Proportionality of interference with Articles 7 and 8 CFREU

Since the SWIFT Agreement does not require the company SWIFT to retain personal data for a time period longer than is necessary for its own business-related purposes, interference with the rights to privacy and data protection only arise when data is transferred to US authorities. Furthermore, the technological particularities of how transfers and subsequent storage of data take place, make it a special case when assessing proportionality in light of Articles 7 and 8 CFREU.

Before analysing proportionality in terms of the existence of sufficient safeguards against abuse of power, the appropriateness and necessity of the SWIFT Agreement needs to be analysed. While the SWIFT Agreement is mainly concerned with sending data located in the EU to US authorities, there is a reciprocal element since emerging intelligence ought to be shared with the EU.[902] Therefore, it can be argued that the SWIFT Agreement is appropriate since detecting sources of financing of terrorist organisations is a crucial first step in preventing and investigating terrorism and thus contributes to maintaining public security in both the US and the EU. In respect to necessity, ensuring public security by fighting terrorism and its financing may depend on data-driven investigation techniques. However, regardless of the usefulness of the latter, the threats posed to data protection and private life

[899] *DRI*, para. 42. See also: Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation v Council and Commission*, para. 363 and Cases C-539/10 P and C-550/10 *P Al-Aqsa v Council*, para. 130.
[900] Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *COM(2013) 843 final.*
[901] *Tele2 Sverige*, para. 103.
[902] Articles 7b, 9 and 10, SWIFT II Agreement

requires that derogations and limitations thereof must apply only in so far as strictly necessary. In the following, it will be assessed whether the SWIFT Agreement includes sufficient safeguards against the abuse of power.

3.3.1 Transfer and access to data

Article 4 of the SWIFT Agreement explains the procedure on how requests for data are made. The US Treasury Department has to send a data request to SWIFT which has to be approved by Europol.[903] The requests shall detail as clearly as possible the data that are relevant for the "purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing",[904] and the necessity of the data.[905] Furthermore, the data request shall be tailored as narrowly as possible in order to minimise the amount of data requested.[906] After Europol has approved the US request, SWIFT is authorised and required to provide data to the US authorities on a 'push basis'.[907] Article 5 of the Agreement regulates the safeguards after the data has been sent to US authorities. First of all, data shall be processed exclusively for the purpose of preventing, investigating, detecting, or prosecuting terrorism or its financing.[908] Furthermore, data mining or any other type of algorithmic or automated profiling or computer filtering shall be prohibited and data shall not be interconnected with any other database.[909] In addition, data security standards such as secure storage, limited access to data, protection from manipulation and alternation are specified in Article 5.[910]

Given those safeguards, it seems that data transfer to the US and subsequent access is limited to what is strictly necessary raising the question as to why data transfer and access would disproportionately interfere with Articles 7 and 8 CFREU? The problem of the SWIFT regime is that even if US authorities are searching for very specific data, SWIFT is technologically not able to extract the requested data. In other words, one request by US authorities may result in multiple hits and SWIFT is

[903] Ibid., Article 4 (4).
[904] Ibid., Article 4 (2) (a).
[905] Ibid., Article 4 (2) (b).
[906] Ibid., Article 4 (2) (c).
[907] Ibid., Article 4 (6).
[908] Ibid., Article 5 (2).
[909] Ibid., Article 5 (3).
[910] Ibid., Article 5 (4).

not in a position to filter out the data that is not relevant to US investigations. Therefore, whenever data is requested from SWIFT, the company can only send data in bulk to US authorities. The authorities in turn assess which of those financial payment messages are useful for law enforcement purposes and which are not.[911] The inability of SWIFT to provide specific data raises concerns as to how targeted such a regime in fact is. While it could be argued that it would be less intrusive to let SWIFT do a pre-selection of the data based on an automated searching tool, such a tool does not yet exist. Furthermore, this would imply that intelligence work needs to be carried out in close cooperation with SWIFT to enable the search. This would imply a 'privatisation of law enforcement' and increase the risk of unlawful processing or accidental loss.

As a consequence of the bulk data transfer the US Treasury is confronted with a data set composed of data of innocent and suspected individuals alike. What is even more concerning is that the data can in exceptional circumstances also include sensitive data.[912] While in some cases it might not be avoidable to be confronted with sensitive data, it would have been useful to make it explicit that sensitive information shall only be further processed if strictly necessary.[913] The fact that personal and sensitive data is retained of individuals with only a weak link or suspicion of crime could awaken the fear of data subjects to be under constant surveillance. This is particularly the case since SWIFT data can provide a picture of a person's movements, economic situation and social environment. As such the feeling of surveillance could have a negative impact on personal development and the right to establish and develop relationships with other human beings and the outside world.[914] This is even more relevant in a globalised world where electronic financial flows have become important for many individuals' daily lives.

Despite the concerns pointed out above, in most cases international bank transfers will not be as frequent and allow one to draw as many conclusions about a person's personal life to come to the conclusion that a feeling of *constant* surveillance

[911] Joint Review Report of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *COM(2014) 513 final*, p. 9
[912] Article 5 (7), SWIFT II Agreement.
[913] For instance Article 7of the SWIFT II Agreement regulates onward transfer of data without differentiating between sensitive and non-sensitive personal data.
[914] As protected by the right to private life. See: *P.G. and J.H. v. the United Kingdom*, para. 56, with further references.

is generated as in the case of the DRD. Furthermore, recent case law has pointed out that an indirect link between a data subject and serious crime can justify indiscriminate data processing for public security purposes.[915] It thus seems that the inability to pre-select only data of suspects can be offset if adequate safeguards exist.

When analysing the proportionality of access to data for public security purposes, the five safeguards that need to apply were established in the framework set out in Chapter 3. First, access to data should be strictly limited to the purpose of preventing and detecting serious offences.[916] The Agreement complies with this parameter since "all searches of provided data shall be based upon pre-existing information or evidence which demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing."[917] Furthermore, it is also mentioned that each individual search of provided data shall be narrowly tailored and demonstrate the belief that a nexus to terrorism exists.[918]

Second, the nature of crime giving rise to the applicability of the legislation needs to be defined.[919] In this respect, the Agreement improved significantly in comparison to its predecessor which defined terrorism only in very broad terms.[920] Article 2 of the SWIFT Agreement provides a detailed definition of terrorism which builds on the approach of Article 1 of Council Framework Decision 2002/475/JHA.[921] The Agreement mentions that terrorism refers to acts of "a person or entity that involve violence, or are otherwise dangerous to human life or create a risk of damage to property or infrastructure, and which, given their nature and context, are reasonably believed to be committed with the aim of: (i) intimidating or coercing a population; (ii) intimidating, compelling or coercing a government or international organization to act or abstain from acting; or (iii) seriously destabilizing or destroying the fundamental political, constitutional, economic, or social structures of a country or an

[915] *Tele2 Sverige*, para. 111.
[916] *DRI,* para. 61 and *Tele2 Sverige*, para. 102. See also: *Zakharov v. Russia*, para. 244 (in the latter case the ECtHR criticised that the measure in question can be applied for minor offences.)
[917] Article 5 (5), SWIFT II Agreement.
[918] Ibid., Article 5 (6).
[919] *Zakharov v. Russia*, para. 244, see also: *DRI*, para. 60.
[920] Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II), *OJ 2010 C355/10*.
[921] Council Framework Decision of 13 June 2002 on combating terrorism, *OJ L 164/3*.

international organization."[922] Acknowledging the efforts to conceptualise the notion of terrorism, obviously every definition thereof is problematic due to its complex nature.[923]

Third, the number of persons authorised to access and use data has to be specified.[924] Article 5 of the SWIFT Agreement stipulates that "access to Provided Data shall be limited to analysts investigating terrorism or its financing and to persons involved in the technical support, management and oversight of TFTP".[925] While this limitation of access at least provides some guidance on who may access data, it does not lay down a limited range of organisations, which in fact access the data. Therefore, the SWIFT Agreement falls short of this requirement.

Fourth, the target group liable to interception needs to be defined by law.[926] The Agreement stipulates that requests for data can be made upon a designated provider (i.e. SWIFT) present in the territory of the United States in order to obtain data stored in the territory of the EU. The SWIFT Agreement further stipulates that no data that refers to the Single Euro Payments Area (SEPA) can be sought.[927] While the SWIFT Agreement excludes SEPA data it does not stipulate in positive terms who is within the scope of the Agreement. While it can be assumed that the target group consists of any persons who transfer money internationally with an exception of SEPA internal transactions, it would have been preferable if the Agreement had stated this in positive terms.

Fifth, access and use of data needs to be dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary.[928] One parameter to analyse whether the oversight body qualifies as independent is to analyse the legal status and independence of the members of the oversight committee.[929] The SWIFT

---

[922] Article 2 (a), SWIFT II Agreement.
[923] For an attempt of conceptualisation, see: Richards, A. (2014) Conceptualizing Terrorism. Studies in *Conflict & Terrorism*, vol. 37 (3). For a legal assessment, see: Tiefenbrun, S. (2002) A Semiotic Approach to a Legal Definition of Terrorism. *ILSA Journal of International & Comparative Law*, vol. 9, p. 357; Beckman, J. (2015) *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*. Roudledge.
[924] *DRI*, para. 62
[925] Article 5 (4c), SWIFT II Agreement.
[926] *Liberty and others v. UK*, para. 64; *Szabó and Vissy v. Hungary*, paras. 66 -67; *DRI*, paras. 56 to 59; *Tele2Sverige*, paras. 97 to 106.
[927] Article 4 (2) (d) SWIFT II Agreement.
[928] *DRI*, para. 62; *Tele2 Sverige*, para. 120; *Szabó and Vissy v. Hungary*, para. 73.
[929] *Zakharov v. Russia*, para. 278. See also: C-288/12 *Commission v. Hungary*, para. 51 including cited jurisprudence.

Agreement entitles Europol to verify US requests for access to data. Europol's newly acquired oversight role is inappropriate. Being a law enforcement agency it has interests in the intelligence activities of the US[930] and thus might be biased when verifying/rejecting a request. In fact, none of the requests of US authorities has been rejected so far. While the acceptance of all requests could simply mean that they were all legitimate, it is likely that Europol –being a law enforcement agency- is rather uncritical.[931] Another option would be to entrust SWIFT with reviewing the data before transferring it to the US. This seems however inappropriate given SWIFT's ignorance on the content of any particular investigation file.[932] Thus, a less biased oversight mechanism would have been to task national data protection authorities with reviewing US requests.[933] Due to their expertise they are best positioned to carry out the oversight. Furthermore, they can filter out sensitive or unnecessary information, which is technologically not possible to remove in advance.[934] In practical terms, one representative of the national data protection authority of the country where the data originates could be appointed to analyse the requests of the US authorities. While these bodies should have full access to all relevant information on the investigation in question[935] Europol's inputs may still be useful given its experience in judging the usefulness of specific data from a law enforcement perspective. Therefore, national data protection authorities should be in a position to consult Europol.

While the SWIFT Agreement falls short of some of the parameters pointed out above, it is not inconceivable that if the Agreement was equipped with effective safeguards, the access to SWIFT data would be proportionate since (i) no less intrusive measures are technologically feasible, and (ii) although data transferred to the US does not only include data of suspects it does neither include data of

[930] Article 1 (b), SWIFT II Agreement stipulates that "relevant information obtained through the TFTP is provided to law enforcement, public security or counter terrorism authorities of Member States, or Europol or Eurojust, for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing."
[931] Joint review of the SWIFT Agreement (*COM(2014) 513*), Annex III shows that all requests have been verified.
[932] AG Opinion on *Tele2 Sverige*, para. 236.
[933] Particularly in *Schrems* the CJEU stressed the important role of national supervisory authorities in evaluating the proportionality of data processing (para. 40). See also: C-614/10 *Commission v. Austria*; C-518/07 *Commission v. Germany*; C-288/12 *Commission v. Hungary*.
[934] AG Opinion on *Tele2 Sverige*, para. 235.
[935] *Zakharov v. Russia*, para. 281.

'practically the entire EU population' but only data of a limited amount of persons who engage in international bank transfers.

3.3.2 Retention period

Article 6 of the SWIFT Agreement regulates the retention and deletion of data by differentiating between extracted (information that has been extracted from data sent by SWIFT) and non-extracted data (information that has not been extracted from data sent by SWIFT). In regard to non-extracted data it is stipulated that the Treasury Department shall conduct an annual evaluation and delete all non-extracted data if it is no longer necessary to combat terrorism and as soon as technologically feasible.[936] Furthermore, all non-extracted data received under the current agreement shall be deleted no later than five years from receipt.[937] In regard to extracted data, the SWIFT Agreement does not stipulate a particular retention period but only mentions that the data shall be retained as long as it is necessary for specific investigations or prosecutions for which they are used.[938]

Three parameters exist to analyse the proportionality of the retention period. First, the determination of the retention period needs to be based on objective criteria.[939] This criterion is difficult to apply since the assessment of what retention period is strictly necessary obviously includes a certain level of arbitrariness since it requires making a judgment on the future value of data.[940] A certain margin also needs to be granted to the legislator to determine the retention period as long as sufficient evidence for its usefulness can be provided. According to case law, 90 days and 6 months retention periods have been deemed to be appropriate.[941] In the last review of the SWIFT Agreement, the 5-years retention period of non-extracted data was defended since a "reduction of the TFTP data retention period to less than five years would result in a significant loss of insights into the funding and operations of

[936] Article 6 (1), SWIFT II Agreement.
[937] Ibid., Article 6 (4).
[938] Ibid., Article 6 (7).
[939] *DRI*, para. 64.
[940] The uncertainty regarding the usefulness of the retention period is evidenced by the fact that the Agreement stipulates that the usefulness of the 5- year retention period shall be reviewed annually (Article 6 (5) SWIFT II Agreement).
[941] *Szabó and Vissy v. Hungary*, para. 74 and *Zakharov v Russia*, para. 255.

terrorist groups."[942] While some critics have considered this period to be excessive[943] it is necessary to grant a certain margin to Member States in determining what constitutes 'objective criteria' in determining the retention period.[944] This does however not imply that other safeguards surrounding the retention period will not be thoroughly assessed as shown below.

Second, when data is stored, the retention period shall take into account the usefulness of different categories of data and the usefulness of data on different categories of concerned persons.[945] The SWIFT Agreement acknowledges a difference between the treatment of extracted and non-extracted data showing that a distinction is recognised between data that is useful for fighting terrorist and data that is less useful. Nevertheless, a more nuanced retention of five years of non-extracted data is necessary. For example, the PNR Agreement require that non-extracted data is depersonalised and masked (i.e. pseudonymisation) after six months and subsequently shifted to a dormant database.[946] Given the similarity of the purpose of the PNR and SWIFT regimes, it is striking that the SWIFT regime does not require depersonalisation after six months.[947]

Third, personal data shall not be kept longer than necessary[948] and it shall be irreversibly destroyed at the end of the prescribed data retention period.[949] In regard to extracted data the SWIFT Agreement mentions that data shall be kept as long as necessary for specific investigations or prosecutions for which they are used. This shows that extracted data could potentially be retained even longer than five years which can be considered to be an 'element prone to abuse'.[950] In regard to non-extracted data, the SWIFT Agreement meets this standard since a periodical review of the usefulness of the data is conducted whereas any data which is no longer necessary to combat terrorism and its financing needs to be deleted. [951] Furthermore, it is clearly

[942] Joint review of the SWIFT II Agreement (*COM(2014) 513*), p. 16.
[943] EDPS Opinion on SWIFT II Agreement, *OJ 2010 C355/10*, para. 21.
[944] A margin of appreciation in adopting security measures has been granted for instance in *Klass and Others v. Germany*; and in *Leander v. Sweden.*
[945] *DRI*, para. 63.
[946] Article 8, 2012 PNR Agreement.
[947] See assessment in Chapters 4 and 6 of this thesis.
[948] *Zakharov v. Russia*, para. 255; *Klass and Others v. Germany*, para. 52; *Kennedy v. United Kingdom*, para 162.
[949] *DRI*, para. 67.
[950] *Szabó and Vissy v. Hungary*, para. 74.
[951] Article 6 (1) SWIFT II Agreement. See: *Zakharov v. Russia*, para. 255.

mentioned that all non-extracted data shall be deleted after 5 years.[952] However, it is questionable how effective this is considering the nexus between legality and technological possibility. The requirement to annually delete non-extracted data depends on whether this is *technologically feasible*.[953] In the 2014 review of the SWIFT Agreement the US authorities confirmed that the technical complexity of the system still poses challenges to the deletion process.[954] Since this is an inherent feature of the SWIFT regime it is questionable whether this feature is acceptable since no less intrusive alternative was available or whether the 'pre-cautionary principle' (in contrast to the evidence-based approach) should be applied.[955] The AG in *Tele2 Sverige* discussed the link between technology and law in regard to the filtering out of sensitive information. He argues that 'it would be desirable' if technology allowed automatic filtering.[956] Later on, he argued that if the filtering out is technologically not feasible this task shall be conducted by independent data protection supervisory authorities. This suggests that as long as sufficient safeguards exist limitations to technological capabilities shall not render a regime disproportionate.

3.3.3 Remedies

Article 8 (2) CFREU grants a prominent role to the rights of data subjects by pointing out "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[957] Furthermore, the right to the availability of effective remedies is also a standalone right enshrined in the CFREU. Article 47 stipulates that "[e]veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal (…)."[958] Case law further specifies that a right to legal remedy needs to be granted to individuals[959]

---

[952] Article 6 (3) and (4), SWIFT II Agreement.
[953] Article 6 (1), SWIFT II Agreement.
[954] Joint review of the SWIFT II Agreement *(COM(2014) 513)*, p. 15-16.
[955] Applying the pre-cautionary principle implies that the SWIFT regime as such shall not operate since technological uncertainties lead to a situation where protection with privacy cannot be guaranteed. For an elaboration of the pre-cautionary principle in the surveillance context, see: Galetta, A. & De Hert, P. (2014) Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance. *Utrecht Law Review*. 10(1), pp.55–75.
[956] AG Opinion on *Tele2 Sverige*, para. 212.
[957] Article 8 (2) CFREU.
[958] Article 47 CFREU.
[959] *DRI*, para. 54; *Tele2 Sverige,* para. 121.

and particularly stresses the important role of independent data protection authorities in safeguarding rights of individuals.[960]

While the first SWIFT Agreement only partially granted rights to data subjects, the second SWIFT Agreement stipulates the right to access, rectification, erasure or blocking.[961] In order to have access to remedies it is important that the data subject is informed/notified about his data being processed.[962] Article 15 (1) of the second SWIFT Agreement stipulates that "any person has the right to obtain, following requests made at reasonable intervals, without constraint and without excessive delay, at least a confirmation transmitted through his or her data protection authority in the European Union as to whether that person's data protection rights have been respected (…) and, (…) whether any processing of that person's personal data has taken place in breach of this Agreement."[963] Subsequently, Article 15 (2) mentions that the disclosure of data processed under the SWIFT Agreement "may be subject to reasonable legal limitations applicable under national law to safeguard the prevention, detection, investigation, or prosecution of criminal offences, and to protect public or national security, with due regard for the legitimate interest of the person concerned."[964] Article 15 leaves a margin of appreciation to the authorities as to whether data is made available to the data subject.[965] As a consequence of denied access, the rights to rectification, erasure and blocking might be unavailable.[966] It would have been preferable if the agreement provided for an automatic ex-post notification that does not depend on individuals requesting the data proactively. Furthermore, while limitations to notify individuals obviously may still apply in order

[960] *Schrems*, para. 95.
[961] Article 15 and 16, SWIFT II Agreement.
[962] *Ekimdzhiev v Bulgaria Application*, para. 90.The ECtHR mentioned: "as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned." See also: *Tele2 Sverige*, para.121.
[963] Article 15 (2), SWIFT II Agreement.
[964] Article 15 (2) SWIFT II Agreement.
[965] Fahey, E. (2013). Law and Governance as Checks and Balances in Transatlantic Security: Rights, Redress and Remedies in EU-US Passenger Name Records and the Terrorist Finance Tracking Program. *Yearbook of European Law*, vol. 32 (1), pp. 368-388.
[966] Note that in order to exercise the right to rectification, erasure or blocking, "a precise identification of the record, including a description of the record, the date, and any other identifying details" needs to be made. See: "Terrorist Finance Tracking Program Redress Procedures for Seeking Access, Rectification, Erasure, or Blocking" Retrieved 04.04.2017 from: https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/Revised%20Redress%20Procedures%20for%20Web%20Posting%20(8-8-11).pdf

to not harm the investigation, it would have been useful to specify that notification should be provided as soon as it does not harm the investigation anymore.

(i) Administrative remedies

Article 12 of the SWIFT Agreement establishes a sort of 'overseeing authority'. Being composed of EU Commission and US officials, the overseeing authority relies on a reciprocal relationship between EU national data protection authorities as well as the Privacy Officer of the US Treasury Department. The authority has the power to monitor compliance with the strict counter terrorism purpose limitation of the Agreement and the safeguards on data security in Article 5 and data retention in Article 6. Thus, the overseeing authority has the power to block any or all searches that contradict the previously mentioned provisions. However, it has neither any power in regard to any other provisions of the agreement, nor does it have the authority to hear individual complaints.

Articles 15 (3) and 16 (2) of the SWIFT Agreement lay down the procedures for obtaining access and requesting rectification, erasure and blocking. It is stipulated that the individual needs to approach its national data protection authority that then communicates with the Privacy Officer of the US Treasury Department. The task of the US Privacy Officer is to make all necessary verifications pursuant to the request. Subsequently, he or she shall without undue delay inform the DPA whether data may be disclosed, rectified, erased or blocked. The DPA is then required to communicate the US decision to the individual. This four-step procedure is time consuming and complex and thus might deter individuals to request access, rectification, erasure and blocking in the first place. While this administrative hazard might limit the effectiveness of redress mechanisms it seems to be a natural outcome of international legislation where two different legal systems need to be respected in the process. Thus, it cannot be considered to be a specific flaw of the SWIFT regime.

However, apart from the administrative complexity, the legitimacy of the limited power granted to DPAs in this process is also questionable. Essentially, under the SWIFT Agreement EU DPAs are merely intermediaries entrusted with a 'communication role' and do not possess any investigative powers or competencies to check the legitimacy of data processing to the US. Instead the competence of assessing whether access, rectification, erasure or blocking is granted rests exclusively within the US authorities. Since the DPAs' control of processing is "an

essential component of protection"[967] to the individual, EU legislation cannot eliminate nor reduce powers expressly accorded to DPAs under Article 8 (3) CFREU to examine claims of data subjects.[968] Thus, the fact that DPAs do not have any real competences either when access is granted in the first place (this is done by Europol as pointed out earlier) or when a claim is lodged by data subjects contradicts the provisions of Article 8 (3) CFREU.[969]

It could be argued that the limited competence of DPAs in investigating individual claims can be justified since their mandate is limited to data processing carried out on their own territory and thus they do not have any powers once processing is carried out in a third country.[970] Nevertheless, since Article 15 of the SWIFT Agreement allows the individual to get a confirmation as to whether data has been processed 'in compliance with this Agreement' an assessment would naturally also include the initial transfer to the US. Thus, the territoriality requirement is met implying that DPAs have competence to act.[971] In addition to that, it has to be noted that on previous occasions, the CJEU extended its rulings also to redress mechanisms in the US. For example, in *Schrems* the CJEU found that the dispute resolution mechanism under the former Safe Harbour Agreement provides insufficient protection since they are -unlike the EU national supervisory authorities- mainly designed to assess whether undertakings comply with Safe Harbour principles. Therefore, they do not guarantee effective legal protection against interference from the state.[972] Also in the case of the SWIFT Agreement, the US authority in charge of assessing individual claims –the Privacy Officer within the Treasury Department- can be criticised. It does not seem to qualify as an independent authority as required under EU law since the positioning within the Treasury department does not guarantee that "decision-making power is independent of any direct or indirect external influence on the supervisory authority.[973] Thus even if the limited role of EU DPAs themselves could be justified due to the missing territoriality link, EU case law still seems to apply to the analysis of US bodies in charge of reviewing individual claims. This does

[967] Case C-518/07 *Commission v. Germany*, para. 23.
[968] *Schrems*, para. 53.
[969] *Tele2 Sverige*, para. 123.
[970] Article 28 (1) and (6) DPD and *Schrems*, para. 44.
[971] *Schrems*, para. 45.
[972] *Schrems*, para. 89; AG Opinion on *Schrems*, para. 204-206.
[973] Case C-518/07 *Commission v Germany*, para. 19.

not only illustrate the importance the EU grants to data subject rights but also shows the increasing extraterritorial effects of EU jurisprudence.

(ii) Legal remedies

When interference with Articles 7 and 8 CFREU takes place, individuals should have the option to lodge a legal complaint with a court.[974] In case that data has been processed contrary to the SWIFT Agreement or in case that right to access, rectification, erasure or blocking was denied, individuals can seek administrative and judicial redress via Article 18 of the SWIFT Agreement.[975] The article stipulates that redress can be requested in accordance with the laws of the EU, its Member States, and the United States, respectively. The Article mentions further: "(…) for this purpose and as regards data transferred to the United States pursuant to this Agreement, the U.S. Treasury Department shall treat all persons equally in the application of its administrative process, regardless of nationality or country of residence. All persons, regardless of nationality or country of residence, shall have available under U.S. law a process for seeking judicial redress from an adverse administrative action."[976] This provision is in contrast to the US FISA legislation which does not grant redress rights to non-US individuals.[977] This shows the positive developments made in the second SWIFT Agreement in comparison to the first Agreement. Recital 12 of the SWIFT Agreement mentions a variety of laws that can be accessed by EU citizens seeking redress, namely: the Administrative Procedure Act of 1946, the Inspector General Act of 1978, the Implementing Recommendations of the 9/11 Commission Act of 2007, the Computer Fraud and Abuse Act, and the Freedom of Information Act. Nevertheless, the most relevant Act (Privacy Act of 1974) is not among those laws accessible by EU citizens. A positive development is the entering into force of the Judicial Redress Act in 2016 providing further judicial redress to EU citizens.[978] It is however unclear whether EU citizens can make use of this Act as it is not specifically mentioned in the SWIFT Agreement as a source of redress.

[974] E.g. *Zakharov v. Russia*, para. 234; see also *Kennedy v. United Kingdom*, para. 167.
[975] Article 18, SWIFT II Agreement.
[976] Article 18 (2), SWIFT II Agreement.
[977] Foreign Intelligence Surveillance Act (FISA), PUBLIC LAW 95-511—OCT. 25, 1978, Sec. 110
[978] The Judicial Redress Act of 2015 (PUBLIC LAW 114–126—FEB. 24, 2016) has been adopted in 2016.

3.3.4 Onward transfer

The SWIFT Agreement mentions the possible onward transfer of information to third countries that might not fulfil the data protection requirements of the EU.[979] However, data processing tools for public security need to include precautions when data is transferred to third parties.[980] Article 7 of the SWIFT Agreement introduces several provisions for onward transfer. First, only information that is derived from an individualised search shall be shared.[981] Second, information shall be shared only with law enforcement, public security, or counter terrorism authorities in the US, the EU Member States or third countries. Additionally, sharing data with Europol, Eurojust or another international body with the respective mandate is permitted.[982] While this provision intends to limit the scope of the onward transfer, it still leaves a wide margin especially since there is no clear definition of institutions that deal with public security. Third, Article 7 stipulates that "such information shall be shared for lead purposes only and for exclusive purpose of the investigation, detection, prevention, or prosecution of terrorism or its financing."[983] This provision is confusing since "lead purposes" do not necessarily need to have a link to terrorism, while the second part of the sentence does require this link.

Fourth, when the US Treasury Department intends to share data with a third country involving information of a citizen residing in an EU Member State it needs to ask for prior consent of the competent authority. However, the Article mentions that this requirement is void when "an immediate and serious threat to public security of a Party to this Agreement, a Member State, or a third country exists."[984] Although in some cases it is difficult to evaluate whether an immediate and serious threat exists, this provision needs to be specified in regard to which authority determines the existence of such a threat. Fifth, the Article also stipulates that the US Treasury Department shall request the third party or the third country to delete the sent data as

[979] Breach of Article 25 (1), DPD.
[980] *Weber and Saravia v. Germany*, para. 95.
[981] Article 7 (a), SWIFT II Agreement.
[982] Ibid., Article 7 (b).
[983] Ibid., Article 7 (c).
[984] Ibid., Article 7 (d).

soon as it is no longer necessary for the purpose for which it was shared.[985] There are two major problems with this provision. First, as soon as data is transferred to a third party or country, the compliance with adequate data protection standards cannot be controlled anymore. Second, while internally the SWIFT Agreement sets a limit to data retention to five years, it sets no clear limit to the storage of data when it is in the possession of a third party. This is surprising given that data protection standards in other countries could potentially be lower.

An interesting point on onward transfer was also raised in *DRI*. The CJEU argued that the DRD did not require data to be stored in the EU implying "(…) that it cannot be held that the control, explicitly required by Article 8 (3) of the Charter, by an independent authority of compliance with the requirements of protection and security (…) is fully ensured."[986] Further the Court argues that such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to processing of personal data.[987] The transfer to the US under the SWIFT Agreement can be considered as justified since it is stipulated by the Agreement itself. However, onward transfer to a third country is a different matter. While the SWIFT Agreement does mention that prior consent is required of the competent Member State authorities of the data subject, this is not to apply when essential for the prevention of an immediate threat to public security. In the latter cases, competent authorities of the data subject's Member State only need to be informed "at the earliest opportunity"[988] depriving them of the ability to control whether the third state complies with the requirements of protection and security. Consequently, it can be argued that the 'onward transfer' provisions of the second SWIFT Agreement do not comply with standards laid down by CJEU case law.

3.3.5 Data security

An adequate data security strategy needs to account for: (i) the vast quantity of data whose retention is required; (ii) the sensitivity of the data; and (iii) the risk of

[985] Ibid., Article 7 (e).
[986] *DRI*, para. 68. See also: *Tele2 Sverige*, para. 122.
[987] Ibid.
[988] Article 7 (d), SWIFT II Agreement.

unlawful access to data.[989] Article 5 of the SWIFT Agreement sets out data security standards to be complied with after the data has been transferred to the US authorities. Respectively, five data security standards are mentioned reflecting the previously mentioned CJEU criteria. First, data shall be held in a secure environment, stored separately from other data and maintained with high-level systems and physical intrusion controls.[990] Second, data shall not be interconnected with any other database.[991] Third, access shall be limited to analysts investigating terrorism and persons involved in support, management and oversight of TFTP.[992] Nevertheless, here to further enhance the protection against unlawful access it might have been useful to include a requirement that all data access needs to be authorised and subject to record keeping. Fourth, data shall not be subject to manipulation, alteration or addition.[993] Ultimately, no copies shall be made other than for disaster backup.[994] Overall, these five security provisions illustrate that under the Agreement SWIFT data should be stored in a 'clear and distinct manner' to ensure their full integrity and confidentiality and by minding the risks of unlawful access and the sensitive nature of the data.[995]

However, it is interesting to note that recently there have been attacks on the SWIFT infrastructure and operations to conceal money flows from SWIFT have been successful.[996] The attacks raise two concerns. First, the vulnerability of SWIFT infrastructure raises concerns about the effectiveness in practice of the company's data security standards. Second, the fact that criminals managed to conduct illegal transactions by circumventing the SWIFT messaging system questions the quality of data within SWIFT for law enforcement purposes. In other words if criminals increasingly possess the means to circumvent the recording of financial messaging data via SWIFT, the usefulness of that data for law enforcement purposes seems to diminish.

[989] *DRI*, para. 66; *Tele2 Sverige*, para. 122.
[990] Article 5 (4) (a) SWIFT II Agreement.
[991] Ibid., Article 5 (4) (b).
[992] Ibid., Article 5 (4) (c)
[993] Ibid., Article 5 (4) (d).
[994] Ibid., Article 5 (4) (e).
[995] *DRI*, para. 66.
[996] 'Hacker dringen in Zahlungssystem Swift ein'. Retrieved 10.01.2017 from: http://www.spiegel.de/wirtschaft/service/swift-hacker-sind-zahlungssystem-eingedrungen-a-1089390.html

4. The SWIFT regime and 'political actorness' of the CJEU

It has been demonstrated that existing jurisprudence is applicable to the SWIFT Agreement and has an impact on its legality. It is however also worth addressing whether and under which circumstances it could in fact have a spill over effect implying political actorness of the CJEU. It is interesting to note that the EP requested shortly after the *DRI* judgement its legal service to elaborate on the impact of the judgment on the PNR and SWIFT Agreements.[997] As elaborated in Chapter 6, the EP took the opportunity to question the EU-Canada PNR Agreement in front of the CJEU as this has been negotiated at the time of the *DRI* judgment. Nevertheless, the timings and legislation-making procedure prevents this in the case of the SWIFT Agreement. Article 218 TFEU on the conclusion of international agreements stipulates that "[a] Member State, the European Parliament, the Council or the Commission may obtain the opinion of the Court of Justice as to whether an Agreement envisaged is compatible with the Treaties. Where the opinion of the Court is adverse, the agreement envisaged may not enter into force unless it is amended or the Treaties are revised."[998] Since the SWIFT Agreement has already been adopted no institutional actor could question the compatibility with the Treaties by requesting an opinion from the Court.

Once an Agreement is concluded, two options remain to challenge the legal basis of an international Agreement. First, Article 263 TFEU stipulates that the CJEU shall have jurisdiction to review the legality of legislative acts that produce legal effects vis-à-vis third parties. Both Member States and institutional actors are eligible to bring actions to the CJEU on the grounds of "(…) lack of competence, infringement of an essential procedural requirement, infringement of the Treaties or of any rule of law relating to their application, or misuse of powers."[999] However, Article 263 TFEU also mentions that any proceedings provided for in this Article shall be instituted within two months of the publication of the measure. Since the SWIFT Agreement is already in force since 2010 the institutional actors can thus not invoke Article 263 TFEU.

---

[997] See: EP Legal Service on LIBE - Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others* - Directive 2006/24/EC on data retention - Consequences of the judgment, *SJ-0890/H.*
[998] Article 218 (11) TFEU
[999] Article 263 TFEU

Second, the Agreement may form the object of a reference under Article 267 TFEU stipulating that the CJEU shall have jurisdiction to give preliminary rulings concerning the validity and interpretation of Union acts.[1000] However, annulment of an Agreement via this route is more complicated for two reasons. First of all, it is debatable whether the CJEU has indeed jurisdiction under Article 267 TFEU. The Article mentions that the CJEU shall have jurisdiction to give preliminary rulings concerning "the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union".[1001] Since international treaties such as the SWIFT Agreement are concluded by EU institutional actors, the SWIFT Agreement can be subject to the CJEU's ruling if invoked at national level. The CJEU has already accepted jurisdiction in those cases.[1002] However, it has also been argued that strictly speaking international agreements are not 'acts of the institutions'. Instead only the decision granting competence to conclude the Agreements can be considered as 'acts of institutions'.[1003] Therefore, "[i]t is obvious that the reference to the Court of Justice, by a court or tribunal in a Member State, of questions of interpretation of an agreement is useful only if (a) the Court has jurisdiction to interpret and (b) the referring court may or must give effect to the provisions of the agreement in the case before it."[1004]

Another Treaty-based option to suspend the Agreement without involving the CJEU is provided in Article 218 (9) TFEU. It is stipulated that "[t]he Council, on a proposal from the Commission or the High Representative of the Union for Foreign Affairs and Security Policy, shall adopt a decision suspending application of an agreement and establishing the positions to be adopted on the Union's behalf in a body set up by an agreement (…)."[1005] This provision provides the Commission theoretically with the opportunity to suspend the Agreement. In practice there are no indications that recent case law prompted the Commission to consider invoking Article 218 (9) TFEU. In an impact assessment accompanying a Commission Communication in 2013 it was even considered to establish an EU-internal TFTP regime. While the assessment concluded that such a regime was not necessary, the

[1000] Article 267 (b) TFEU
[1001] Article 267 (b) TFEU
[1002] For example, Case C-181/73 *Haegeman v. Belgium* of 30 April 1974
[1003] Hartley, T. (1998) *The Foundations of European Community Law*. Oxford University Press.
[1004] Eeckhout, P. (2011) EU External Relations Law. *Oxford EU Law Library*, pp. 275 -76
[1005] Article 218 (11) TFEU. Article 21 (2) of the SWIFT II Agreement stipulates that "either Party may terminate this Agreement at any time by notification through diplomatic channels. Termination shall take effect six (6) months from the date of receipt of such notification."

reasons were mainly related to costs rather than to privacy and data protection considerations.[1006] The Communication also evaluated the option of amending the current EU-US SWIFT Agreement. However this was discarded without detailed assessment since amending the Agreement depends on "the consent of a third country [which] makes it weak."[1007] The option of terminating the Agreement was also mentioned but rejected since it would have a negative effect on EU intelligence gathering in regard to the prevention of terrorist offenses in the EU.[1008] While the impact assessment at least briefly discusses these options, the Commission Communication does not even mention the possibility of terminating or amending the SWIFT Agreement. It is unlikely that the Commission would come to a different conclusion after the *DRI* judgement, as the reasons for not having considered them in 2013 are still relevant. Furthermore, the Commission's '*institutional memory'* of the difficulty of negotiating the Agreement with the US counterpart would lead to its preference of maintaining the status quo.[1009] It can thus be concluded that while some findings of the existing CJEU and ECtHR jurisprudence seem to apply to the SWIFT Agreement, political actorness is not very likely due to timing and the more limited CJEU competence once an international agreement has been adopted.

Conclusion

The aim of this chapter was to analyse how the EU institutional framework shaped data protection and privacy in respect to the SWIFT Agreement. The second hypothesis (i.e. "*The EU institutional framework enables EU legislative actors to pursue strategic preferences in the legislation-making process and thereby influences the way privacy and data protection is shaped in the public security context*) has been confirmed. The chapter has identified three strategic preferences among EU policy actors at the policy formation stage which in turn shaped privacy and data protection. First, the lack of sincere cooperation between EU institutional actors shows that actors were subject to different institutional frameworks impacting their preference formation during the initial stages of TFTP in the US. Second, the institutional

[1006] Communication from the Commission to the European Parliament and the Council - A European terrorist finance tracking system (EU TFTS), *COM(2013) 842 final*, p. 13.
[1007] Ibid., p.21.
[1008] Ibid., p.22.
[1009] See Section 2 of this Chapter.

framework encouraged power struggles for more legislative influence between the EP and the Council which led to a revision of the SWIFT Agreement and thus to the re-shaping of privacy and data protection. Third, the institutional framework fostered strategic transgovernmentalism between EU and US actors which played a role in shaping privacy and data protection both when the first and the second Agreement were adopted. It has been shown that the US was in a stronger negotiation position than the EU due to the TFTP programme originating in the US and due to the complex institutional framework that existed in the EU.

The chapter also assessed Hypothesis 3 (i.e. "*The transitional nature of the EU institutional framework contributed to the CJEU's evolution from a 'legal basis arbiter' to a political actor in its own right that increasingly determines substantial aspects relating to privacy and data protection in the public security context*").

On the one hand, it has been shown that some provisions of the Agreement are not proportionate in light of the framework established in Chapter 3: (i) the Agreement does not strictly limit the persons who are authorised to access and use data under the SWIFT Agreement; (ii) while the Agreement specifies that no data that refers to the Single Euro Payments Area (SEPA) can be sought, it fails to define the actual target group liable to interception; (iii) the SWIFT Agreement falls short of the requirement that an independent administrative authority or a court needs to review access. This is because the law enforcement authority Europol is entrusted with this task which does not qualify as independent as it could potentially benefit from investigation results emerging from US analysis of SWIFT data; (iv) the Agreement does not sufficiently limit the retention period of non-extracted personal data since no requirement to depersonalise the data exists; (v) the retention period in respect to extracted data is not sufficiently limited since the SWIFT Agreement fails to explicitly require the deletion of extracted data; (vi) the Agreement does not grant sufficient competences to European Data Protection Authorities in assessing whether rights of data subjects have been infringed and in assessing the treatment of personal data when it was transferred to third parties; and (vii) while the adoption of the Judicial Redress Act has strengthened legal remedies available to EU citizens, it is unclear whether it could be invoked for issues relating to the SWIFT Agreement.

The chapter also analysed under which circumstances the CJEU case law can shape preference formation among policy actors and thus exhibit features of political actorness. It has been shown that the EP requested shortly after the *DRI* judgement its

legal service to elaborate on the impact of the judgment on the PNR and SWIFT Agreements. However, as shown timing and corresponding institutional rules determines whether a judgment can directly shape strategic preferences of policy makers.

CHAPTER 6 – PNR AGREEMENT: THE SPILL-OVER EFFECT OF A UNILATERAL DECISION

Introduction

In 2016 the Passenger Name Record Directive was adopted which is the latest addition to several EU legislative tools that regulate the processing of passenger name records for public security purposes.[1010] Apart from the PNR Directive, the EU has concluded PNR agreements with the United States, Canada, and Australia and agreements with other countries are currently under discussion.[1011] This chapter focuses on the EU-US PNR Agreement as it introduced the practice of processing PNR data for security purposes to the EU and because it is the most controversial of its kind. To a more limited extend the chapter also assesses the PNR Directive since it is considered to be an example of EU norm-taking of US practices.

The EU-US PNR Agreement is based on the US Aviation and Transportation Security Act (ATSA) which was introduced as a reaction to 9/11.[1012] The act stipulates that air carriers need to provide the US Customs Service[1013] access to passenger name records (PNR) for purposes of security screening of individuals travelling to and from the US. More specifically, PNR is key to the operation of the US Automated Targeted System (ATS) which uses a wide range of databases (e.g. law enforcement and FBI databases) in order to assess if travellers pose a risk by being involved in terrorism or criminal activities. If this is the case they can be subject to further examination before departure.[1014] PNR is data collected through airline reservation systems for commercial purposes and the data includes various fields of personal information ranging from name and address to 'frequent flier programmes' and available contact

[1010] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *OJ 2016 L 119*.
[1011] Joint statement on the beginning of negotiations between Mexico and the European Union on PNR data transmission. Retrieved 01.04.2017 from: http://europa.eu/rapid/press-release_STATEMENT-15-5374_en.htm
[1012] US Aviation and Transportation Security Act 2001 implemented by the US Bureau of Border and Customs Protection (CBP)), Public Law 107-71, 107th Congress.
[1013] With the creation of the United States Department of Homeland Security (DHS), the Customs Service became the United States Department of Homeland Security's Bureau of Customs and Border Protection (CBP).
[1014] Department of Homeland Security, Privacy Office, A Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union *(2008) 38*.

and payment/billing information. Although all of these fields appear inconspicuous, combining them in a certain way can reveal sensitive information.[1015]

The US Office of Homeland Security stresses that the war on terrorism is and must be a global effort requiring the cooperation of nations around the world.[1016] However, the US legislators did not take potential conflicts with non-US legal frameworks into account when enacting ATSA. Therefore, air carriers were in the midst of conflicting legal obligations. On the one hand they had to comply with ATSA requirements while on the other hand they were subject to the DPD. Ultimately, the EU Commission was forced to approach the US because European airlines were not allowed to land on US soil without allowing US authorities access to PNR data. This first step towards a transatlantic agreement permitting the transfer of PNR data in accordance with EU law marks the beginning of the 'EU-US PNR Agreement saga'. It includes a first Agreement in 2004, the CJEU's annulment of the first Agreement in 2006, an interim Agreement in 2006, the second Agreement in 2007, and the third PNR Agreement in 2012. Furthermore, the EU-US PNR Agreement also triggered the adoption of the PNR Directive in 2016.

The aim of the chapter is to illustrate how the EU institutional framework shapes data protection and privacy in respect to the PNR Agreement. Hypothesis 2 guides the assessment of the extent to which strategic considerations of the involved actors shaped privacy and data protection in the pre-Lisbon environment. It is argued that the Commission used the PNR negotiations as way to increase its influence in AFSJ matters and external relations. To do so, it made use of several institutional variables such as transgovernmentalism, conceptual framing through cross-pillarisation and strategic communication with the EP. Furthermore, the EP attempted to increase its influence in the legislation-making procedure by making use of cross-pillarisation (i.e. by starting legal proceedings), through venue shopping and through the co-decision procedure. Ultimately, it will be demonstrated that the EU policy-makers were norm-takers since they internalised US rules to an extent that an internal PNR regime has been adopted. It is also assessed to what extent Hypothesis 3 is applicable. In this respect it is first of all assessed to what extent current ECtHR and CJEU jurisprudence is applicable to the EU-US Agreement and the PNR Directive.

[1015] Papakonstantinou, V. & De Hert, P. (2009). The PNR Agreement and Transatlantic Anti-Terrorism Co-operation: No Firm Human Rights Framework on either Side of the Atlantic. *Common Market Law Review*, vol. 46 (1), p. 886-87.
[1016] Ibid., p. 48.

To do so, the framework developed in Chapter 3 will be applied. It has to be noted that the currently pending *Opinion 1/15* on the EU-Canada Agreement will be relevant for the analysis due to the Agreement's similarity to the EU-US Agreement. The section therefore takes the AG Opinion into account which had already been published at the time of completion of this thesis. As a second step, it is then analysed to which extent political actorness can be identified and it will be shown that post-Lisbon political actorness takes place but only on a conditional basis.

1. The origins of the PNR regime

The implementing rules of ATSA can be categorised as a 'national solo effort' disregarding the transnational dimension of PNR data.[1017] The Article 29 WP questions whether these unilaterally adopted US measures are compatible with international agreements and conventions concerning air traffic and transportation, with national laws and with the DPD.[1018] Sending EU PNR and passenger manifests to the US authorities may lead to four conflicts with the DPD. First, data subjects are not in all cases informed about the fact that data is sent to the US authorities at the point of data collection contradicting the principle of fair processing of data. In the case of PNR, the principle of fair processing cannot be limited on grounds of fighting crime and maintaining national security[1019] since the data processing is systemic. Furthermore, the need to inform data subjects can only be waived in particular instances such as if required for in national law.[1020] While PNR data transfer was required by US law, there was no basis for this in EU or Member State laws. Second, in respect to data security, the Article 29 WP claims that technical requirements imposed on airlines by the US are not sufficient as they might leave data exposed to non-authorised access by third parties. It is however not further specified why technical standards are not high enough and it is thus not clear on which factors this assumption is based. Third, the data processing to the US is not aligned to the original purpose for which the data is collected, namely to fulfil contractual obligations vis-à-

[1017] On US 'global unilateralism', see: Rees, W. and Aldrich, R. (2005). Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence? *International Affairs*, vol. 81 (5), pp. 390-406.
[1018] Article 29 WP Opinion 6/2002 of 24 October 2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, *11647/02/EN WP 66*, p. 4.
[1019] As stipulated in Article 13, DPD.
[1020] Article 11, DPD.

vis the passenger. Thus, the processing does not comply with the purpose limitation principle.[1021] However, in accordance with Article 13 DPD, the EU or Member States can adopt legislative measures in order to relax the purpose limitation principle for the sake of safeguarding public security or to investigate/prevent criminal offences. Fourth, the DPD also stipulates that any personal data transfer to a third country requires an adequate level of protection in the respective country. While the Safe Harbour Agreement existed at that time, its scope is limited to companies and can thus not apply to data transfer to government authorities.[1022] Therefore, an adequacy decision was considered to be necessary leading to a dialogue between the EU and the US authorities.

2. EU institutional dynamics leading to the PNR Agreement

In accordance with NI, assessing how privacy and data protection is shaped in relation to the PNR Agreement requires the analysis of how the institutional framework influences the behaviour of policy actors. In the following, five strategic activities of legislative actors will be discussed that shaped privacy and data protection in the PNR context: transgovernmentalism, cross-pillarisation in regard to conceptual framing, cross-pillarisation in respect to legal proceedings, venue-shopping and norm-taking.

2.1 Initial negotiations: EU Commission's solo effort

After the EU Commission learnt that a US law requiring PNR to be transmitted will enter into force in early 2003 it informed the EU Council Working Party on aviation during a meeting on the 28 of January 2003 about the precarious situation such a law would cause for EU airlines.[1023] Furthermore, the Commission informed the Council that a meeting between US Customs officials and the Commission was planned before the adoption of the US law.[1024] The Council suggested that national data protection

[1021] Article 6 (1) (b), DPD.
[1022] Note that the US Privacy Act which regulates data protection/privacy when data is processed by public authorities did not apply to non-EU citizens at that time.
[1023] Aviation - New legal requirements by US on 'Advanced Passenger Information System' (APIS) and 'Passenger Name Records' (PNR); *Council Doc. 6051/03*.
[1024] New Legal Requirements by US on 'Advanced Passenger Information System' (APIS) and 'Passenger Name Records' (PNR). Exchange of Views on the Position of the Member States. Discussion by Working Party on Aviation on 28 January 2003, *Council Doc. 6051/03*.

authorities should be involved in the following meetings in order to discuss various options.[1025] In the subsequent early stages of the negotiations national data protection authorities did not play a role and instead the Commission managed to become the key player of the PNR negotiations. It achieved this status in three ways: (i) forming a strategic partnership with US negotiators right from the beginning (i.e. transgovernmentalism), (ii) marginalising the EP, and (iii) conceptually framing PNR as a data protection matter.

First, right from the start the Commission did not only take the lead in the negotiations but also demonstrated its willingness to compromise. In 2003 a Commission delegation met US Customs authorities in order to discuss the implications of PNR transmissions from the EU to the US. Instead of being initial discussions, the meeting resulted in a joint statement stressing the full commitment to the US objective of preventing and combating terrorism and the "(…) need for practicable solutions that would provide legal certainty for all concerned."[1026] In addition to that, both sides agreed on the need to reach a bilateral arrangement (i.e. the adequacy decision) under Article 25 (6) DPD in due time.[1027] Since it seemed unlikely that an adequacy decision could be reached until the US law entered into force, the Commission made an appeal to data protection authorities not to take enforcement actions against airlines complying with the US requirements until an agreement between the US and EU has been reached.[1028] In addition to the Commission's collaborative efforts towards the US, it is interesting to note that it also suggested multilateral agreements via the UN Civil Aviation Organisation (ICAO).[1029] This indicates that the Commission does not only readily accept the US norms but that it even had an interest in elevating those norms to a wider international level. After the conclusion of the joint statement, the Commission reported back to the Council Working Party on Aviation and to national experts on data protection and confronted them with a *fait accompli*.[1030]

Second, during the first phase of negotiations the relationship between the

[1025] Ibid.
[1026] European Commission/US Customs Talks on PNR Transmission, Joint Statement. *Brussels, 17/18 February*, para. 2. Retrieved 11.01.17 from http://ec.europa.eu/justice/policies/privacy/docs/adequacy/declaration_en.pdf
[1027] Ibid., para. 6.
[1028] Ibid., para. 4.
[1029] Ibid., para. 8.
[1030] How US Customs bounced the European Commission into a quick decision. Retrieved 11.01.17 from http://www.statewatch.org/news/2003/mar/02usdata2.htm

Commission and the EP was marked by lack of cooperation and different views on the substance of how to regulate access to PNR data. The EP expressed concerns about the Commission's joint statement in a Motion for a Resolution.[1031] In response, Commission officials attended the plenary session of the EP mentioning that "[i]t [the Commission] had no intention to conceal. It was more a question of when to bring this matter to the attention of Parliament and in what form."[1032] This indicates that communication between the two players was linked to strategic considerations and did not happen by default undermining the principle of 'sincere cooperation'.[1033] The EP ultimately adopted a highly critical resolution 'on transfer of personal data by airlines in the case of transatlantic flights' which questions the legal basis of the joint statement and criticised that the statement could be understood as an "(…) indirect invitation to the national authorities to disregard Community law."[1034] Furthermore, the EP also condemned the fact that it had not been informed before signing the joint statement.[1035]

Third, by successfully framing PNR data transfer as a first pillar matter the Commission also framed PNR as a data protection matter. This allowed the Commission to cave out competences from the Council and the EP via the comitology procedure. Comitology is a procedure by which a legally binding Union act identifies the need for uniform conditions of implementation. Thus it requires the adoption of implementing acts by the Commission under the supervision of the Member States.[1036] The comitology procedure under the DPD takes the form of granting the Commission the power to adopt "adequacy decisions". More specifically, Article 25(6) DPD stipulates that the Commission may find that a third country ensures an adequate level of data protection enabling Member States to transfer data to that country. While the aim of comitology is to facilitate the implementation of Union acts and increase efficiency, concerns about democratic legitimacy and the balance of power between

---

[1031] European Parliament Motion for a Resolution further to the Commission statement pursuant to Rule 37(2) of the Rules of Procedure by Jorge Salvador Hernández Mollar on behalf of the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs on transfer of personal data by airlines in the case of transatlantic flights**,** *B5-0187/2003*.
[1032] Ibid.
[1033] Article 13 TEU.
[1034] European Parliament Resolution on transfer of personal data by airlines in the case of transatlantic flights, *P5_TA(2003)0097*, para. 3.
[1035] Ibid., para. 1.
[1036] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, *OJ 2011 L 55.*

EU institutional players may arise since additional legislation is adopted without the usual policy-making procedures. The Commission's efforts to reach an adequacy decision were cumbersome. While the Commission showed on many occasions resistance to accept US solutions, the adopted adequacy decision still reveals that significant concessions had been made. During the negotiations, the EP continuously attempted to influence the negotiations and gain more (in)formal competences in the legislation-making process. One example of this is the threat of the incumbent EP rapporteur that if the Commission acts against the principle of loyal cooperation the EP would take legal action in order to "protect parliamentary prerogatives."[1037] Disregarding the concerns of the Parliament[1038] the adequacy decision was ultimately adopted on the 14th of May 2004.[1039] Three days later, the Council signed a Council Decision on the Agreement.[1040] Ultimately on the 28th of May the first PNR agreement was signed by both US and EU authorities.[1041]

2.2 Adoption and annulment of the first PNR Agreement: Is the EP the victim of cross-pillarisation?

In Chapter 4 it was claimed that EU institutional actors made use of cross-pillarisation at the beginning of the legislation-making procedure to maximize their influence in respect to the policy outcome of the DRD. Nevertheless, in the PNR case, cross-pillarisation became apparent only after the PNR Agreement has been adopted namely when the EP challenged the first Agreement's legal basis resulting in the change of pillars.[1042]

Already before the adoption of the adequacy decision and the PNR

[1037] EU-US PNR: Council to ignore Parliament and go ahead with "deal". Retrieved 11.01.2017 from http://www.statewatch.org/news/2004/may/06eu-us-nr-deal.htm

[1038] It has to be mentioned, though, that the Parliament ignored the request of the Council for an expedited procedure in delivering its opinion on the proposal due to the lack of all language versions. Thus, the Council felt legitimised to act without the EP's opinion.

[1039] Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, *OJ 2004 L 235*.

[1040] Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States Department of Homeland Security, Bureau of Customs and Border Protection, *OJ 2004 L183/83*.

[1041] Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, *CE/USA/en 1*.

[1042] Note that apart from the PNR, DRD and SWIFT cases, the EP does not seem to frequently engage in litigation: see: Fahey, E. (2015) Of One Shotters and Repeat-Hitters: A Retrospective on the Role of the European Parliament in the EU-US PNR Litigation. In Davies, B. and Nicola, F. (forthcoming) *EU Law Stories*, Cambridge University Press. Available at SSRN: https://ssrn.com/abstract=2605793

Agreement, the EP submitted a request for an opinion to the CJEU on the Agreement's compatibility with the Treaty.[1043] Before the Court could deliver the opinion, the agreement was adopted turning this request *sans objet*. Therefore, the EP took further legal actions both against the Agreement and the Commission's adequacy decision after receiving the recommendation of the EP legal committee.[1044] In regard to the adequacy decision 2004/535/EC the EP advanced four pleas for annulment.[1045] In the first the EP claimed that the decision was *ultra vires* because it infringes Article 3 (2) DPD on the exclusion of activities which fall outside the scope, *ratione materiae,* of the Directive and Community law.[1046] Second, the EP argues that the adequacy decision is a breach of the fundamental principles of Directive 95/46/EC. Third, it was asserted that fundamental rights are breached since the law is not accessible and foreseeable (accordance with law requirement of Art. 8 ECHR). Fourth, the EP believed that the principle of proportionality is infringed since the number of transferred PNR data categories and the time period of data storage is excessive. In regard to Decision 2004/496[1047] the EP advanced six pleas for annulment: (i) Article 95 EC is not the correct legal basis because the Decision's aim is not the establishment and functioning of the internal market but to enable processing of personal data for anti-terror purposes; (ii) the second subparagraph of Article 300 (3) EC was infringed because Directive 95/46 was amended; (iii) the right to protection of personal data has been infringed; (iv) the principle of proportionality has been breached; (v) a sufficiently precise statement of reasons for the adoption of the Decision was lacking; (vi) the principle of cooperation in good faith laid down in Article 10 EC had been breached.[1048] Since the CJEU rejected the EP's request for an expedited procedure the court ruling was only published in 2006.[1049]

The Court ignored all EP pleas besides the ones on the legal basis. The Court mentions that recitals 6 and 7 of the adequacy decision make references to the US law

[1043] Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities* of 30 May 2006, para. 39.
[1044] Ibid.
[1045] Ibid., para. 50. The adequacy decision contains the assurances of the US to the EU on how data is adequately protected in the US.
[1046] Ibid., para. 51.
[1047] The Decision lays down the *modus operandi* of the Agreement.
[1048] Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*.
[1049] Ordonnance du Président de la Cour 21 Septembre 2004 'Procédure accélérée' Dans l'affaire C-317/04, ayant pour objet un recours en annulation au titre de l'article 230 CE, introduit le 27 juillet 2004.

requiring PNR transfer[1050] and stipulate that the legislation concerns the enhancement of security and the conditions under which persons my enter and leave the country. Recitals 8 and 15 stipulate that the EU is fully committed to support the US in the fight against terror and that PNR data is strictly used for preventing and combatting terrorism, related crimes and other serious crimes.[1051] Thus, the Court concluded that PNR data transfer to CBP "(…) constitutes processing operations concerning public security and the activities of the State in areas of criminal law."[1052] The CJEU acknowledges that the initial collection of data takes place under Community law since the sale of airline tickets is a matter of supply of services. Nevertheless, data processing regulated by the adequacy decision concerns safeguarding public security and serves law enforcement purposes.[1053] In addition to that, the CJEU also reverses the Commission's argument that Article 3 (2) DPD only applies to activities conducted by the state.[1054] In fact, it does not play a role that data is collected and transferred by private actors (i.e. airlines). Instead the purpose of the transfer is decisive namely the safeguarding of public security.[1055] As a consequence the Court determines that the adequacy decision does not fall within the scope of the DPD and must be annulled.[1056] In regard to the EP's plea for annulling the Council Decision 2004/496 the Court also exclusively focused on the EP's argument that Article 95 EC was chosen as an incorrect legal basis. The Council defended the legal basis by arguing that a measure was necessary to avoid distortions of competition since some airlines decided to comply with US requirements while some did not.[1057] The Commission made a more trivial argument by complaining that the EP has not suggested an appropriate legal basis during the legislation-making procedure.[1058] By keeping its reasoning very short, the Court argued that "[a]rticle 95 EC, read in conjunction with Article 25 of the Directive, cannot justify Community competence

[1050] Title 49, United States Code, section 44909 (c) (3) and Title 19, Code of Federal Regulations, section 122.49b.
[1051] Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*, para. 55
[1052] Ibid., Para. 56.
[1053] Ibid., Para. 57.
[1054] The Commission relies on C-101/01, *Lindqvist,* para. 43.
[1055] Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*, para. 58.
[1056] Ibid., paras. 59 and 61.
[1057] Ibid., para. 64.
[1058] Ibid., para. 65.

to conclude the Agreement."[1059] It further mentions that the Agreement relates to the same transfer of data as the adequacy decision and is thus excluded from the scope of DPD.[1060] Therefore, the Court also annulled Decision 2004/496.[1061] The annulment took effect after 90 days as stipulated under paragraph 7 of the Agreement.[1062]

The ruling has been described as 'failure for the European Parliament'[1063] or as 'pyrrhic victory'.[1064] This argument was mainly advanced because in the aftermath of the Decision the PNR Agreement had to be re-negotiated under the third pillar excluding the EP from the decision-making process. In the case that the EP's legal action against the Commission and Council was an attempt to show 'actorness'[1065] and to show its intention to influence how data protection and privacy is shaped in the context of PNR, it failed.[1066] Obviously, the EP manoeuvred itself in to this precarious situation since it questioned the legal basis in one of its pleas in front of the CJEU. Thus, the EP proactively took the risk that the Court would find that the legal basis of the Agreement is wrong leading to its exclusion from the policy-making procedure. This raises the question of why the EP challenged the legal basis instead of relying exclusively on the other numerous pleas it advanced? It has been argued that the ideological rationale was the strongest driving force behind the EP decision to take legal action.[1067] The EP found that adequate data protection safeguards were missing and that the US executive branch exercised too much influence on EU internal

[1059] Ibid., para. 67.
[1060] Ibid., para. 68.
[1061] Ibid., para. 70.
[1062] For reasons of legal certainty the adequacy decision will thus also be valid for the subsequent 90 days.
[1063] De Hert, P & De Schutter, B. (2008). International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift. In Martenczuk, B. & Van Tiehl, S. (2008). *Justice, Liberty, Security. New Challenges for EU External Relations*. Brussels University Press, p. 304.
[1064] Mitsilegas, V. (2015). The Transformation of Privacy in an Era of Pre-emptive Surveillance. *Tilburg Law Review*, vol 20 (2015), p.39; Monar, J. (2010a), op. cit., p. 36. See also: Gilmore, G. and Rijpma, J. (2007). Joined cases C-317/04 and C-318/04. *Common Market Law Review*, vol. 44 (4), pp. 1081-1099.
[1065] 'Actorness' for this purpose means having a tangible influence on the nature of a policy or a policy field. The term 'actorness' originally stems from research on the stance of the EU on the global level and the role it plays. For a detailed analysis, see: Bretherton, C. & Vogler, J. (2006). *The European Union as a Global Actor*, Routledge; Smith, H. (2002) *European Union Foreign Policy: What it is and what it does.* Pluto Press; Smith, K. E. (2003) *European Union Foreign Policy in a Changing World*. Polity Press.
[1066] The fact that actors litigate to gain influence has been raised in: Barros, X. (2012) The external dimension of EU counter-terrorism: the challenges of the European Parliament in front of the European Court of Justice, *European Security*, vol. 21 (4), pp. 518-536.
[1067] Ibid., p. 525.

affairs.[1068] This shows that normative principles can in fact play a role in the policy-making process.

Nevertheless, while the EP might have been partially guided by normative aspirations, the EP did not achieve its objective of safeguarding privacy and data protection. The judgment created a loophole in the protection of European citizens because under the third pillar passenger data is used without being protected by the DPD.[1069] It is worth mentioning that at that time Council Framework Decision 2008/977/JHA on the protection of personal data in the third pillar did not yet exist and thus the judgement indeed created a *lacuna legis*.[1070] Furthermore, the EP also argued that transfer based on a 'pull' system cannot be defined as transfer within the meaning of Article 25 DPD. Both the EDPS and the AG argued that restricting the concept of transfer to one based on a 'push system' makes it easy to evade conditions laid down by Article 25 DPD and thus impairs data protection provided for in the article.[1071] Since the EP either failed to foresee or ignored these consequences, it can be doubted that ideological concerns were the key driver when the EP challenged the PNR Agreement. Instead the pleas submitted to the CJEU suggest that the EP indiscriminately advanced various arguments in order to maximise the possibility of the Court annulling the Agreement. Another likely explanation is thus that the struggles between EU institutional actors before the adoption of the Agreement seemed to have motivated the EP to give the Council and the Commission a warning at all costs to not exclude the EP in the future. A similar strategy of balancing current loss with future gains has also been observed in the negotiations on the DRD.[1072] Thus, overall the EP might have still achieved a long-term strategic goal with the Court decision.

[1068] Ibid.
[1069] EDPS first reaction to the Court of Justice judgment of 30 May 2006, retrieved 11.01.2017 from https://secure.edps.europa.eu. See also: Hatzopoulos, V. (2008) With or without you... Judging politically in the field of area of freedom, security and justice. *European Law Review,* vol. 33 (1), p. 52; Kosta, E.. Coudert, F. & Dumortier, J. (2007) Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive, *International Review of Law, Computers & Technology*, vol. 21 (3), pp. 347-362.
[1070] It has however been argued that, once adopted, the Framework Decision did not substantially improve the situation. See for instance: De Hert, P. & Papakonstantinou, V. (2009) The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for. *Computer Law & Security Review*, vol. 25 (5), pp. 403–414.
[1071] AG Opinion on Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*, paras. 79 and 91.
[1072] See: Chapter 4 (section 2.2.3) of this thesis.

2.3 The interim and second PNR Agreement: third pillar procedures and venue shopping

The negotiations for the new PNR Agreement started in July 2006 under Article 24 TEU implying that the Council presidency led the negotiations assisted by the Commission "as appropriate".[1073] Although Article 24 TEU excludes the EP from the new legislation making procedure, the EP made several attempts to convince the Council and the Commission of the need for close cooperation - a strategy which can be considered as a type of *venue shopping*.[1074] First, the former EP president approached both the Council and the Commission to stress the importance of acting jointly in accordance with the principle of loyal cooperation between the EU institutional players. He urged both actors to keep the Parliament informed about any new developments and to take its views into consideration.[1075] Subsequently, the LIBE Committee adopted a draft recommendation on the new PNR Agreement containing suggestions on the adequate negotiation procedure and substantial aspects of the agreement.[1076]

Second, the EP requested full co-decision rights on PNR when the interim agreement was due to be reviewed in 2007. Legally this would be possible if the 'passerelle' clause was invoked allowing the Council by unanimous decision, to move policy areas from one decision-making procedure to another (i.e. in this case to the co-decision procedure).[1077] Notwithstanding the EP's efforts, the Council strictly applied third pillar proceedings leading to the adoption of an interim agreement in 2006.

Third, when the second PNR Agreement was negotiated there was still no third pillar data protection framework in place. Consequently, this legislative vacuum

---

[1073] Article 24 TEU.
[1074] The term venue shopping was coined by Guiraudon, V. (2000) European Integration and Migration Policy: Vertical Policy Making as Venue Shopping, *Journal of Common Market Studies*, vol. 38 (2), pp. 241-271. Guiraudon originally used the term to explain how national actors used policy venues at EU level to circumvent national opposition to a certain policy initiative. However, 'venue shopping' can also take place exclusively on EU level when actors frame issues in a certain way in order to trigger the application of a specific policy making procedure.
[1075] Letters from Josep Borrell Fontelles (former EP President) to Mr. José Manuel Barroso (former Commission President) and to Wolfgang Schüssel (former President of the European Council). *09.06.2006*, Brussels, retrieved 11.01.17 from: http://www.statewatch.org/news/2006/jun/eu-usa-pnr-borrell-letter2.pdf and http://www.statewatch.org/news/2006/jun/eu-usa-pnr-borrell-letter1.pdf.
[1076] European Parliament Report of 19 July 2006 with a Proposal for a European Parliament recommendation to the Council on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime, including organised crime, *A6-0252/2006*.
[1077] Article 48, TEU.

in the third pillar was informally 'filled' by first pillar actors. For instance, the EP demanded access to all documents related to the EU-US PNR negotiations and the EU-US High Level Contact Group on Data Protection.[1078] Furthermore, it adopted a resolution on how PNR should be regulated, for instance by enabling the EP to enter into a dialogue with the US Congress.[1079] Other stakeholders were aware that the EP's views had to be factored in to avoid new legal actions. For example US authorities aimed to influence MEPs[1080] and the US Undersecretary of Homeland Security visiting the EP LIBE Committee in the midst of the negotiations.[1081] The EP took this opportunity to communicate its concerns to the US side and to stress the necessity of greater involvement of the EP in the discussions on the second PNR Agreement and the High-Level Contact Group on Data Protection.[1082]

2.4 Towards the third PNR Agreement: EP power aspirations and sensitivity to failure

Besides the EP's fierce criticism on the second PNR Agreement no legal actions followed this time, clearly because the EP waited until it was granted a retroactive say after the Treaty of Lisbon has been adopted. In 2010 the Council asked the EP to approve the PNR Agreement in accordance to post-Lisbon procedures.[1083] The EP immediately made use of its newly acquired powers and postponed its vote.[1084] Before voting on the Agreement the EP requested the Commission to establish a single set of model principles to serve as a basis for agreements with third countries.[1085] The Parliament set out seven principles that should be included in the model, such as the

[1078] Letter from ALDE MEPs to the Council and the Commission, retrieved 11.01.2017 from http://www.statewatch.org/news/2007/sep/eu-pnr-alde-info-request.pdf
[1079] European Parliament resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues, *P6_TA(2007)0039*.
[1080] US authorities met with several MEPs and other relevant stakeholders on a mission at the beginning of May to discuss the PNR Agreement, See for instance: "Chief U.S. Data Privacy Officers reach out to EU", retrieved 11.01.2017 from http://useu.usmission.gov/may0707_horvath_teufel.html
[1081] European Parliament Press Release on US Secretary of Homeland Security Michael Chertoff debates data protection with MEPs. Retrieved 11.01.2017 from http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20070514IPR06625&language=SV
[1082] European Parliament Committee on Civil Liberties, Justice and Home Affairs Transatlantic Dialogue of 14 May 2007. Retrieved 11.01.2017 from http://www.statewatch.org/news/2007/may/ep-us-pnr-chertoff.pdf
[1083] The retroactive consent of the EP was necessary since the 2007 Agreement was just in place on a provisional basis as not all national parliaments had ratified the Agreement by 2009. See explanations in Chapter 3 of this thesis.
[1084] European Parliament Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, *P7_TA(2010)0144.*
[1085] ibid, para. 7.

general principle that data shall be pushed instead of pulled and that sufficient data protection safeguards should apply.

When the EP finally voted on the new Agreement the Rapporteur Sophie in't Veld recommended the Parliament not to accept the draft in its current form since the seven principles outlined in the EP's resolution in 2010 had not been fully respected in the draft Agreement.[1086] A considerable number of LIBE Committee members shared this point of view. However the majority was of the opinion that it was better to have a partially satisfactory agreement than no agreement at all.[1087] As a consequence LIBE as well as the plenary accepted the draft PNR Agreement which entered into force on 1 July 2012.[1088]

While from the beginnings of the PNR saga the EP continuously demanded stricter data protection safeguards it now accepted an agreement that still did not match its own demands. This naturally raises the question of what triggered the EP's change of opinion. Although granting the EP more powers the ordinary legislation making procedure could have partially led to the consent to the new PNR Agreement.[1089] As has been argued in the data retention chapter the fact that the EP was now able to influence the outcome of negotiations made it more *sensitive to failure*. This means that as soon as the EP became the 'co-legislator' it shared legislative responsibility. As a consequence, a failure in the negotiations could have resulted in diminished trust between the EP and national government/the electorate.[1090]

Additionally, the EP has an integrationist bias underpinning its sensitivity to failure and supporting the preference for a sub-optimal outcome instead of no outcome at all.[1091] In regard to sensitivity to failure, scholars have observed that

---

[1086] European Parliament Committee on Civil Liberties, Justice and Home Affairs Draft Recommendation of 01 February 2012 on the Draft Council decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security; *17433/2011–C7-0511/2011– 2011/0382(NLE).*

[1087] Santos Vara, J. (2013). The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon. *CLEER Working Papers 2013/2*.,p. 26.

[1088] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security *OJ 2012 L 215.*

[1089] Other reasons such as a changed threat perception seems to not have played a role.

[1090] Ripoll Servent, A. (2013) Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision. *Journal of European Public Policy*, vol. 20(7), p. 977.

[1091] Ibid.; With reference to: Hörl, B., Warntjen, A. and Wonka, A. (2005). Built on quicksand? A decade of procedural spatial models on EU legislative decision-making. *Journal of European Public Policy, vol.* 12(3), pp. 592–606; Kreppel, A. and Hix, S. (2003). From "grand coalition" to left–right confrontation: explaining the shifting structure of party competition in the European Parliament, *Comparative Political Studies,* vol. 36(1–2), pp. 75–96.

legislative bodies revert very rarely to the status quo. First, this is due to the policy-maker's assumption that the current situation in respect to a given policy field needs to be changed by all means. Second, by analysing EU politics through the lens of game theory another explanation is that failure to reach a policy outcome damages relationships with other parties and actors. Thus, there is the risk that "hard feelings carry over into other, unrelated issues."[1092] Furthermore, empirical studies revealed that the two big EP parties form a grand coalition on institutional and integration issues and internal procedural issues with the mandate to foster EU integration.[1093] The reasons for the overall pro- integrationist attitude of the two big parties can be ascribed to the *collective institutional interest* to increase the influence of the EP as a whole. Since the EP was traditionally the weakest institutional actor it had to act collectively to strengthen its role vis-à-vis the Council and the Commission.[1094]

Applying the notion of sensitivity to failure to the PNR Agreement, it can be argued that until being more actively involved in the negotiations the EP underestimated the limited room of manoeuvre due to the strict mandate of US authorities. Thus, without deviating from its original position it was likely that no agreement would have been achieved. The likely consequences of no agreement would have been a legal vacuum for airlines and data subjects and a cumbersome process of concluding bilateral agreements between the EU Member States and the US. This would not only have been perceived badly by national authorities and the electorate but also undermined the legitimacy of the EU as a global actor. Consequently the EP was pressured into more pragmatic decision making in order to prevent being the cause of a potential failure.

2.5 Proposal for a EU-internal PNR regime and norm-taking?

Already in 2003 the Commission stressed that the "(…) EU's approach cannot be limited to responding to the initiatives of others." [1095] Thus, the Commission suggested

[1092] Achen, H.C. (2006) Institutional realism and bargaining models In: Thomson, R., Stokman, F.N., Achen, C.H. and König, T. (eds) *The European Union Decides*. Cambridge University Press, p. 101-2.
[1093] Hix, S., Kreppel, A. and Noury, A. (2003) The party system in the European Parliament: collusive or competitive? *Journal of Common Market Studies,* vol. 41(3), p. 318.
[1094] Ibid.
[1095] European Commission Communication on Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, *COM(2003) 826 final*, p. 4.

the adoption of a framework decision in 2007.[1096] The proposal suggested obliging airlines flying to and from EU territory to share private data on their passengers with so-called 'Passenger Information Unit' (PIU) that are established in each MS.[1097] The legislation-making procedure subsequent to the issuance of the proposal coincided with the adoption of the Lisbon Treaty.[1098] Consequently, framework decisions as legislative instruments ceased to exist resulting in the proposal's withdrawal.[1099] Afterwards, it took the Commission a further three years to issue a new proposal.[1100] When the proposal for a directive was finally issued, the EP rejected it.[1101] Nevertheless in 2015, the threat posed by 'foreign terrorist fighters' and the Paris terror attacks initiated new discussions.[1102] Therefore, the EP and the Council urged the Commission to revise the PNR proposal by taking the Court findings of the *Digital Rights Ireland* case into consideration.[1103] In this context, the LIBE Committee presented a proposal on how to modify the original Commission proposal for a Directive.[1104] Based on this proposal the PNR Directive was adopted in April 2016.[1105]

The adoption of the PNR Directive is an example of how the EU internalises US norms. For instance, an involved Commission official has mentioned that the "EU thinks a PNR Directive is useful only because the US does."[1106] However, the fact that an EU measure has only recently been approved after more than nine years of being

[1096] European Commission proposal for a draft Framework Decision on the use of Passenger Name Record for law enforcement purposes of 6 November 2007, *COM (2007) 654 final*.
[1097] Ibid., Article 3.
[1098] The latest results of the negotiations before the 2007 proposal lapsed are documented in: Council of the European Union Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, *Council document 5618/2/09 REV 2*.
[1099] European Commission Communication on Consequences of the entry into force of the Treaty of Lisbon for ongoing inter-institutional decision-making procedures, *COM(2009) 665 final*, para. 1(4).
[1100] European Commission Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *COM (2011) 32 final.*
[1101] European Parliament Report on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *COM(2011)0032 – C7-0039/2011-2011/0023(COD*).
[1102] In an interview with an EU Commission official it was mentioned that the terror attacks in Paris triggered the adoption.
[1103] European Parliament Resolution of 11 February 2015 on anti-terrorism measures. *2015/2530(RSP)*. See also: European Council "Follow-up to the statement of the Members of the European Council of 12 February 2015 on counter-terrorism: Report on implementation of measures Report on implementation of measures by the EU Counter-Terrorism Coordinator", *Council Doc. 9422/1/15.*
[1104] European Parliament Draft Legislative Resolution on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *COM(2011)0032 – C7-0039/2011 – 2011/0023(COD).*
[1105] Directive (EU) 2016/681, op.cit.
[1106] Interview with EU Commission official.

on the agenda shows that "norm-taking" is not a linear process. There are three reasons explaining why the US emerged as a catalyst while the EU was rather a recipient of norms. First of all, the institutional architecture to fight terrorism has been revised and strengthened in the US after 9/11 while this has not been the case in the EU due to the lack of supranational power.[1107] Second, the US is in general known for its unilateral and extraterritorial approach which takes little account of the views of others.[1108] Third, the fragmentation of the EU was an advantage for US actors as the US could apply strategic lobbying with a more critical EP and it could build alliances with more sympathetic forums such as Council working groups or Commission officials.[1109]

The process of "norm-taking" in the PNR case happened in three stages: (i) initial forceful norm advocacy by the US, (ii) bargaining leading to norm acceptance and (iii) norm incorporation accompanied by mirroring and imitation."[1110] The initial forceful norm advocacy by the US took place in the form of imposition of requirements on EU airlines without discussing with EU authorities the practicalities of this new requirement. Subsequently, the discussions leading to the PNR Agreements were crucial to set the scene and convince EU actors on the details when accepting norms imposed by US authorities. In this respect, it is interesting to note that other EU institutional players tried to convince MEPs of the adequacy and advantages of adopting the US approach.[1111] Ultimately, the mirroring and imitation took place by incrementally introducing internal measures on PNR. On the one hand, the Commission launched a project to incentivise Member States to adopt national PNR schemes.[1112] Through this initiative more Member States started testing PNR regimes contributing to a lack of harmonisation between Member State laws. On this basis, the PNR Directive is merely a EU response to a situation created by the EU

[1107] Argomaniz, J. (2009) When the EU is the 'Norm-taker: The Passenger Name Records Agreement and the EUs Internalization of US Border Security Norms. *Journal of European Integration*, vol. 31 (1), p. 127.
[1108] Ibid.
[1109] See Chapter 5 of this thesis.
[1110] Argomaniz (2009), op. cit., p. 124.
[1111] Interview with EP official.
[1112] The Commission awarded 50 million EUR to 14 Member States who replied to the Commission's call for proposals on national PNR schemes. See: European Commission, list of awarded projects. Retrieved 01.04.2017 from: http://ec.europa.eu/dgs/home-affairs/financing/fundings/pdf/isec/isec-grants-awarded- 2012_en.pdf.

itself instead of a requirement due to diverging laws.[1113] One the other hand, imitation becomes clear when comparing the recently adopted PNR Directive with the EU-US PNR Agreement.[1114] Whilst similar, the PNR Directive includes several more safeguards showing that even if norms are imported from external actors, the interaction of those norms with internal EU standards prevents a full assimilation.

The effect of establishing EU-internal legislation that formerly only existed in respect to EU external relations raises interesting concerns about the EU's role as an international actor in AFSJ. EU institutional actors are concerned with expressing the importance of strict standards of fundamental rights in external relations. Article 3(5) TEU confirms that "in its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens."[1115] Moreover, the Commission has stressed that "[w]e need to strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations."[1116] Consequently, scholars have claimed that the EU is a normative power or a 'force of good' that respects and promotes human rights in its foreign policy.[1117]

However, in the case of PNR a different trend can be observed. Instead of pro-actively promoting and enforcing internal EU standards on data protection and privacy in relations with the US, the relevant EU stakeholders did not do justice to its own discourse. Even an adverse effect can be observed where norms and standards that were formerly refused as too low have turned into EU internal tools. Consequently, the aspiration of EU actors to spread high standards of data protection and privacy in international relations remains unfulfilled. Further, an adverse effect can be observed where international relations even lower EU internal standards on data protection and privacy through norm internalisation.

[1113] European Data Protection Supervisor, Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *Opinion 5/2015*, para. 15.

[1114] Further explanations follow later this Chapter (section 3.6).

[1115] The importance of values when acting on an international level is further stressed in Articles 21 (1) and 21 (2) TEU and Article 205 TFEU.

[1116] Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Delivering an area of freedom, security and justice for Europe's citizens - Action Plan Implementing the Stockholm Programme, *COM(2010) 0171 final*.

[1117] See for example*:* Manners, I. (2006). Normative power Europe reconsidered: beyond the crossroads. *Journal of European Public Polic*y, vol. 13(2), pp. 182–99.

2.6 Summary

Different dynamics during the legislation-making procedure are relevant to understand how data protection and privacy are shaped in regard to the PNR Agreement. First, EU institutional actors attempt to maximize their power during the process of concluding the PNR agreements. For instance, at the initial stage the Commission asserted itself as the main actor through transgovernmentalism and conceptual framing. Second, the EP made use of cross-pillarisation by challenging the legal basis of the first PNR agreement. Third, the EP abandoned some of its principles after it became a co-legislator due to sensitivity to failure and an integrationist bias. Fourth, the adoption of the PNR Directive is an example of norm-taking as it was triggered by the EU-US PNR Agreement.

3. The applicability of existing jurisprudence on the PNR Agreement

The aim of this section is to assess the PNR Agreement in light of the framework established in Chapter 3. After summarising AG Mengozzi's Opinion on the EU-Canada PNR Agreement, it is argued that Article 7 CFREU is interfered with since the PNR Agreement permits the transfer of PNR data to US authorities. Article 8 CFREU is interfered with since personal data is processed in accordance with the Agreement. The interference of both rights can be justified since fighting serious crime has been acknowledged as being a matter of public security. Subsequently, a proportionality assessment is conducted in respect to both rights. The section also analyses the proportionality of the PNR Directive since it is an example of norm-taking from the EU-US Agreement. Last but not least, the section assesses the political actorness of the CJEU in regard to PNR.

3.1 AG Mengozzi on Opinion 1/15 Request for an Opinion submitted by the European Parliament

In September 2016 AG Mengozzi published his opinion on the request for an opinion submitted by the European Parliament (*Opinion 1/15*). The EP had requested the CJEU opinion in 2014 before approving the EU-Canada PNR Agreement. The EP posed two questions to the Court: First, do Articles 82(1)(d) and 87(2)(a) TFEU constitute the correct legal basis for the Council Act concluding the Agreement or

must the act be based on Article 16 TFEU? Second, is the Agreement compatible with the provisions of the Treaties and the Charter of Fundamental Rights? The CJEU has previously held that CJEU's assessments exclusively refer to the measure under scrutiny and do not impact the legality of other measures displaying similar characteristics.[1118] Nonetheless, *Opinion 1/15* will necessarily have implications for the PNR Agreement with the US as well as the PNR Directive due to the striking similarity of the instruments.[1119] Therefore, it is analysed in the following.

The AG assessed first whether the draft agreement is based on the correct legal basis. The choice of the legal basis has 'constitutional significance' as well as 'practical implications'. The former refers to complications in the international legal order in case that the Agreement has to be invalidated at a later stage due to the choice of the wrong legal basis. In regard to 'practical implications', the choice between a Title V and another legal basis (i.e. Article 16 TFEU) has implications for the participation of Denmark, Ireland and the UK. The AG continues by providing examples illustrating that the purpose of the Agreement is both to maintain security as well as data protection. For instance, Article 1(1) of the Agreement mentions that the use of PNR Data is "to ensure security and safety of the public and prescribe the means by which the data is protected."[1120] Furthermore, Article 82(1)(d) TFEU is considered not to be a correct legal basis since the PNR Agreement does not promote (at least not in the first place) cooperation between judicial authorities of the Member States.[1121] Therefore, the correct legal basis should be Article 16 (2) TFEU and Article 87 (2)(a).

The AG also provides an exhaustive explanation of the proportionality of the PNR Agreement. More specifically, he mentions that the Agreement can only be considered as being in line with the Treaties and the Charter if it: (i) lists clearly and precisely the data to be transferred in the annex by excluding sensitive data, (ii) contains in an annex an exhaustive list of crimes covered by the agreement, (iii) identifies clearly who is in charge of processing PNR data; (iv) specifies principles and rules applicable to the databases PNR is compared with in the context of automated processing; (v) lays down objective criteria to facilitate that the number of

[1118] In regard to the review of the legal basis, see: C-94/03 *Commission v Council* of 10 January 2006, para. 50; C-658/11 *Parliament v Council*, of 24 June 2014, para. 48.
[1119] AG Opinion on *Opinion 1/15*, para. 4.
[1120] Para. 70.
[1121] Para. 108.

officials that can access PNR data can be specified; (vi) states reasons for the necessity of a particular data retention period, (vii) mentions that directly identifiable information has to be masked; (viii) stipulates that onward transfer needs to be subject to ex-ante notification to EU DPAs; (ix) an independent authority reviews the respect for private life and data protection; (x) passengers that are not present in Canada can submit an administrative appeal to independent authorities.[1122]

3.2 Interference with Articles 7 and 8 CFREU

3.2.1 Interference with Article 7 CFREU

'Passenger name records' refer to sets of personal data which are generated when persons book, pay and engage in a journey to the US.[1123] The PNR Agreement requires that PNR are made available to DHS "(…) to the extent they are collected and contained in the air carrier's automated reservation/departure control systems (…)."[1124] Thus, the PNR Agreement does not require airlines to collect data they would not do for their own purposes. More specifically, "[t]he number and nature of the fields of information in a PNR will vary [among airlines] depending on the reservation system used during the initial booking."[1125] Rather than requiring collection of data the Agreement obliges airlines to create the PNR 'data dossier' from potentially different airline internal databases.[1126] Due to the foregoing, it can be concluded that the collection of data does not amount to interference under the remit of the Agreement.

The PNR Agreement requires carriers to transfer the PNR data contained in their reservation systems to the Department of Homeland Security. As pointed out on earlier occasions in this thesis, to establish interference persons concerned do not have to suffer any adverse consequences on account of that interference and data does not

[1122] AG Opinion on *Opinion 1/15*, para. 328.
[1123] Annex, 2012 PNR Agreement.
[1124] Preamble, 2012 PNR Agreement.
[1125] *ICAO Guidelines on Passenger Name Record (PNR) Data*, *Doc 9944* of 2010, retrieved 08.01.2017 from: https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf, para. 2.1.8.
[1126] For example, the ICAO guidelines mention that data generated during the booking procedure of an airline ticket (as required under point 2, Annex of PNR Agreement) is often stored in a different database as the information on check-in (as required under point 13, Annex of PNR Agreement).

have to be sensitive.[1127] Thus, the mere fact that public authorities receive data without allowing the individual the opportunity to refute it amounts to an interference with Article 7 CFREU.[1128] Consequently, by stipulating the transfer, access, use, storage and potentially further transfer by public authorities for security purposes, the PNR Agreement triggers an interference with Articles 7 and 8 CFREU. [1129]

Having clarified that interference takes place it is necessary to establish whether the interference is 'particularly serious'. One parameter to assess the seriousness of interference is whether individuals are informed about the data processing.[1130] Under PNR, interference does not happen without the knowledge of the data subject since the individuals are informed about the processing by carriers when buying the airline ticket and the requirements are published on the Federal Register and the DHS website.[1131] Furthermore, ex-post the individual has the chance to request his or her PNR from DHS.[1132] A second parameter to assess the seriousness of interference is the examination on whether it is wide-ranging.[1133] This parameter can be considered to be met since: (i) a wide variety of data –possibly including sensitive data- is transferred to US authorities;[1134] (ii) the transfer has a systemic character since all travellers to the US are covered without exception[1135] and (iii) data is processed "(…) without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions."[1136]

3.2.2 Interference with Article 8 CFREU

In addition to Article 7, Article 8 CFREU has also been interfered with because the transfer of data and subsequent access, to data constitutes 'processing of personal data'.[1137] In addition to that, Article 8 CFREU is interfered with since the PNR

[1127] *Schrems*, para. 87; *DRI*, para. 33; *Österreichischer Rundfunk and Others*, para. 75.
[1128] *DRI*, para. 34. In regard to Article 8 ECHR see also: *Leander v. Sweden*, para 48; *Rotaru v. Romania*, para. 46 and *Weber and Saravia v. Germany*, para. 79.
[1129] AG Opinion on *Opinion 1/15*, para. 170.
[1130] *DRI*, para. 37.
[1131] Article 10, 2012 PNR Agreement.
[1132] Article 11, 2012 PNR Agreement.
[1133] *DRI*, para. 37.
[1134] See in analogy: *Tele2 Sverige*, para. 97.
[1135] Ibid.
[1136] *DRI*, para. 58; see also *Tele2 Sverige*, para. 105; and AG Opinion *on Opinion 1/15*, para. 176.
[1137] *DRI*, para. 29. See also: C-92/09 and C-93/09 *Volker and Markus Schecke and Eifert*, para. 47.

Agreement regulates how data has to be stored, destroyed and possibly further transferred once it has been sent to US authorities.[1138]

3.3 Justification for interference with Articles 7 and 8 CFREU

This section assesses whether data processing under the PNR regime is justified in line with Article 52 (1) CFREU. First, it can be argued that the agreement is 'provided for in law'. Since the Agreement was concluded according to procedures set out in Article 218 TFEU the Agreement qualifies as an 'international agreement' under the Treaties. Both ECtHR and CJEU case law have confirmed that international agreements are automatically incorporated into national law and an are integral part of the EU legal order.[1139]

Second, interference can only be justified if legislation in question respects the essence of the rights that are concerned.[1140] It can be argued that the essence of Article 8 CFREU[1141] is not interfered with because several data protection principles are in place, such as data security provisions which aim to protect personal data against accidental, unlawful or unauthorised destruction, loss, disclosure, alternation, access, processing and use.[1142] Furthermore, mechanisms are in place to allow individuals to access their data (Article 11, PNR), and if necessary to have it rectified (Article 12, PNR). Ultimately, oversight mechanisms are in place (Article 14, PNR).

Whether the essence of Article 7 CFREU is interfered with is more difficult to assess. The 19 data categories transferred to US authorities include a wide variety of personal information such as address, contact details and travel patterns. Furthermore, they may include sensitive data which is not even necessary for the purpose of the agreement.[1143] For instance, SSR data (i.e. data inserted in fields called: 'general

[1138] Articles 5, 8, 16 and 17, 2012 PNR Agreement.
[1139] *Neulinger and Shuruk v. Switzerland*, para.99; *Fernández Martínez v. Spain*, para. 118; See also: C-308/06, *Intertanko and Others*, para. 42 and C-401/12 *Council and Others v Vereniging Milieudefensie and Stichting Stop Luchtverontreiniging Utrecht*, para. 52.
[1140] Article 52(1) CFREU.
[1141] In *DRI* it has been argued that the essence of Article 8 CFREU would be infringed if no data protection or data security principles would be applied to the processing of personal data (*para. 40*).
[1142] Article 5, 2012 PNR Agreement. See: AG Opinion on *Opinion 1/15*, para. 187.
[1143] Opinion 4/2003 of the Article 29 Data Protection Working Party on the Level of Protection ensured in the US for the Transfer of Passengers' Data, *WP 78*, adopted 13 June 2003. The Article 29 WP argues that only the following fields should be processed: "PNR record locator code, date of reservation, date(s) of intended travel, passenger name, other names on PNR, all travel itinerary, identifiers for free tickets, one-way tickets, ticketing field information, ATFQ (Automatic Ticket Fare Quote) data, ticket number, date of ticket issuance, no show history, number of bags, bag tag numbers,

remarks') is concerning, in particular since a special remark on a meal request can reveal information on religious beliefs (e.g. halal food).[1144] In addition to that, OSI (Other Service-Related Information) and information concerning frequent-flyers is not relevant for the purposes pursued by the Agreement especially since it can also reveal sensitive data. For instance, a request for a special airport service could reveal information on health conditions.[1145] Thus, while the data categories include personal data (e.g. name) and non-personal data (e.g. information on baggage) they can also in specific circumstances include sensitive data if passengers or a travel agency on the passenger's behalf fill out the SSR and OSI data fields. Apart from the detailed picture this information reveals about a passenger, information requested does still mainly relate to the circumstances of the journey (e.g. information on tickets, selected route, baggage, frequent-flyer programme etc.).[1146] Furthermore, a number of guarantees are available to ensure that data is gradually depersonalised after a relatively short period of six months.[1147] Therefore, the essence of the right is not interfered with.

Third, as mentioned in articles 1 and 4 of the PNR Agreement, an objective of general interest is pursued within the meaning of Article 52 (1) CFREU namely that of maintaining public security through the fight against terrorism and serious transnational crime.[1148] In the joint review conducted in 2013 the review team stated that the "various ways in which PNR is used follows an approach allowing it to maximize the added value of using PNR for law enforcement purposes."[1149] More specifically, PNR data was used in a number of cases to prevent flying and to conduct more targeted searches once certain passengers arrived in the US.[1150] Furthermore, the added value of PNR data is that it allows authorities to identify passengers that are not

---

go show information, number of bags on each segment, voluntary/involuntary upgrades, historical changes to PNR data with regard to the aforementioned items."

[1144] As noted in: ICAO Guidelines on Passenger Name Record (PNR) Data, *Doc 9944 of 2010*, retrieved 03.08.2016 from: https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf, para. 2.1.10.

[1145] Article 29 Working Party, Opinion 4/2003, op. cit., p. 7.

[1146] AG Opinion on *Opinion 1/15*, para. 186.

[1147] The AG on *DRI* indicated that retention periods under one year seem to be justified (para. 149).

[1148] *DRI*, para. 42.

[1149] Report from the European Commission on the Review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, *COM(2013) 844 final*, p. 8.

[1150] ibid., p. 7-8.

yet suspected of a crime.[1151] Due to the foregoing it can be concluded that the PNR Agreement is indeed a valuable tool in fighting serious crime.[1152]

3.4 Proportionality of interference with Articles 7 and 8 CFREU

Before engaging in the discussion on the PNR Agreement's safeguards against abuse of power, it needs to be assessed whether the PNR Agreement is appropriate and necessary in regard to the legitimate objectives pursued. First it needs to be pointed out that the PNR Agreement is of a reciprocal nature since any analytical information resulting from the PNR data transfer shall be shared with EU and Member State authorities.[1153] In this way, the effects of the Agreement concern both the EU and the US. The Agreement enables authorities to shed light on terrorism and serious crime in the context of international transport and thereby ensures public security in the EU and the US. Furthermore, the indiscriminate nature of the transfer allows law enforcement authorities to identify passengers that have previously not been suspected of being involved in a terrorist network or in serious crime.[1154] Consequently, the Agreement can be considered to be appropriate for attaining the objective pursued. In respect to necessity, the fight against terrorism –however fundamental it may be- cannot in itself justify the indiscriminate nature of data transfer under the PNR Agreement.[1155] Instead limitations to the respect for privacy and data protection must apply only in so far as strictly necessary.[1156]

3.4.1 Indiscriminate transfer and access to data

Four parameters need to be taken into account to examine whether access of competent authorities to data and their subsequent use can be considered to be proportionate. First, transfer and access to data should be strictly limited to the

[1151] AG Opinion on *Opinion 1/15*, para. 205.
[1152] Note that the last joint review took place in 2013. However, in 2015 the Department of Homeland Security Privacy Office conducted an assessment of the functioning of the PNR Agreement. See: United States Department of Homeland Security Privacy Office Report on the use and transfer of passenger name records between the European Union and the United States." Retrieved 12.01.2017 from: https://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf. The report does however not discuss the usefulness of PNR for the purpose of fighting crime.
[1153] Article 18, 2012 PNR Agreement.
[1154] AG Opinion on *Opinion 1/15*, para. 205.
[1155] See in analogy: *Tele2 Sverige*, para. 103.
[1156] See in analogy: *DRI*, para. 52.

purpose of preventing and detecting serious offences.[1157] The PNR Agreement sets out that the US 'collects, uses and processes PNR data for the purposes of preventing, detecting, investigating, and prosecuting' terrorism, related and other crimes punishable by a sentence of imprisonment for three years or more.[1158] Furthermore, on a case-by-case basis data can be used and processed where necessary if ordered by a court.[1159] There are two concerns in relation to these provisions. On the one hand, the article does not mention that data transfer and access is 'strictly' limited to the aim pursued. On the other hand, the Agreement expressly allows further processing if ordered by a court without specifying the purpose for which the data might be used by the court.[1160] Therefore, the agreement can be considered to be not strictly limited to the purpose it pursues.[1161]

Second, the nature of crimes triggering the applicability of the Agreement needs to be precisely defined.[1162] Article 4 of the PNR Agreement provides a relatively precise explanation of what qualifies as a terrorist offence. It also refers to international conventions relating to terrorism and it sets out what counts as crimes relating to terrorism.[1163] The Agreement does however also apply to other crimes that are punishable by a sentence of imprisonment of three years or more and which are transnational. The meaning of 'transnational' is also further specified.[1164] While the Agreement does not explicitly refer to 'serious' crime[1165] it lays down objective criteria in relation to the nature and degree of seriousness of the offences in which cases US authorities are entitled to process PNR data.[1166] Nonetheless, it is concerning that no list containing the specific crimes has been included in this provision.[1167] For

[1157] *DRI*, para. 61; *Tele2 Sverige*, para. 111; *Kennedy v. United Kingdom*, para. 159; *Zakharov v. Russia, para*. 244.
[1158] Article 4, 2012 PNR Agreement.
[1159] Article 4 (2), 2012 PNR Agreement.
[1160] European Commission Legal Service Note for the Attention of Mr Stefano Manservisi Director General DG HOME on the Draft Agreement on the Use of Passenger Name Records (PNR) between the EU and the United States. Retrieved 12.01.2017 from: http://www.statewatch.org/news/2011/jun/eu-usa-pnr-com-ls-opinion-11.pdf
[1161] AG Opinion on *Opinion 1/15*, para. 237.
[1162] *Zakharov v. Russia*, para. 248.
[1163] Article 4 (1) (a), 2012 PNR Agreement.
[1164] Article 4 (1) (b), 2012 PNR Agreement.
[1165] AG Opinion on *Tele2 Sverige*, para. 229 and *DRI*, paras. 61 and 62.
[1166] AG Opinion *on Opinion 1/15*, para. 231.
[1167] The inclusion of a list on specific crimes has already been requested by the EDPS before the 2012 Agreement has been adopted. See: Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security. *Brussels, 09.12.2011*.

instance, the list of crimes annexed to the PNR Directive shows that there is the possibility to define crimes more precisely on the supranational level.[1168] In transatlantic relations the incorporation of such a list would prevent that a party to the Agreement takes a unilateral decisions to criminalise a certain action and thus indirectly extends the scope of the Agreement.

Third, access to data shall be limited to a small number of authorised persons.[1169] Article 3 of the PNR Agreement mentions that PNR data shall be provided to the DHS. Furthermore, Article 5 sets out technical and organisational measures to prevent unauthorised access. For example, all access shall be logged and documented by DHS. Nevertheless, on some occasions, the Agreement makes reference to the United States more generically instead of mentioning DHS. For instance, Article 17 mentions that the "United States may transfer PNR to competent government authorities of third countries." Also in Article 4 it is mentioned that "the United States collects, uses, processes PNR (…)" Furthermore, it can be criticised that no objective criteria are laid down to make known the number of officials that have access to PNR data.[1170] It can thus be concluded that the authority responsible for the processing is not sufficiently limited to a small number of authorised persons.[1171] Whether this vagueness was intentional or not, it is an aspect prone to abuse.

Fourth, the target group liable to interception should be defined by law and limited to what is necessary.[1172] PNR data is exclusively collected from persons travelling to the US. Thus, data subjects take a deliberate decision to subject themselves to the legal requirements of the PNR regime when travelling to a US destination.[1173] In paragraph 59 of the *DRI* judgment, the CJEU criticises that data collection is (amongst others) not sufficiently limited to a *particular geographical zone*.[1174] Reverting to this criticism, it is thus conceivable that PNR data processing is sufficiently limited *ratione personae* due to its restricted geographical scope. Furthermore, the primary purpose of the broad scope of the Agreement is to allow law enforcement authorities to identify individuals which were previously not known to the authorities. Thus, limiting the scope *ratione personae* would render the purpose of

[1168] PNR Directive, Annex II. See also: AG Opinion on *Opinion 1/15*, para. 235.
[1169] *DRI*, para. 62.
[1170] See AG Opinion on *Opinion 1/15*, para. 273.
[1171] See: AG Opinion on *Opinion 1/15*, paras. 246 to 251.
[1172] See: *Liberty and others v. UK*, para. 64 or *Szabó and Vissy v. Hungary,* para. 66 -67.
[1173] See also: AG Opinion on *Opinion 1/15*, para. 242.
[1174] *DRI*, para. 59; emphasis added by author. Reiterated in *Tele2 Sverige*, para. 111.

the agreement meaningless.[1175] In addition to that, although transfer of PNR data is systemic and indiscriminate, it cannot necessarily be regarded as 'pre-emptive' since all data is immediately used by linking it to other databases. In this regard it has been argued that it is a similar control mechanism to physical security controls at airports.[1176] A positive effect of that is that physical controls at airports can be more targeted increasing efficiency and preventing unwarranted suspicion.[1177]

Fifth, access and use of data needs to be conditional upon prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary.[1178] The Agreement does not provide for prior review before data is accessed. However, given the high volume of PNR data that is provided to and accessed by US authorities in the first place, it is for the sake of efficiency as well as resource-wise not feasible to make the transfer of every passenger's data subject to review by a court or an independent administrative body. Therefore, the requirement of ex-ante review of the transfer can be waived as long as sufficient ex-post judicial oversight is guaranteed.[1179]

3.4.2 Data retention period

There are three parameters to assess whether the retention period is proportionate. First, data retention periods shall be strictly limited according to the usefulness of the data for the purposes pursued both in terms of data categories as well as persons concerned.[1180] The data retention period under the 2012 Agreement can reach a maximum of 15 years. However, Article 8 of the Agreement lays down a complex and nuanced retention period in active and dormant databases. First of all, all categories of PNR data will be retained in an active database for five years. However, the data is depersonalised and masked already after six months and it is only accessible by a limited number of specifically authorised officials.[1181] Depersonalisation means that names, contact information, other supplementary information, special service information, special service request and APIS

[1175] See: AG Opinion on *Opinion 1/15*, para. 244.
[1176] Interview with EU Commission official.
[1177] Ibid.
[1178] *DRI*, para. 60; *Szabó and Vissy v. Hungary*, para. 73.
[1179] *Szabó and Vissy v. Hungary*, para. 77 and *Tele2 Sverige*, para. 120.
[1180] *DRI*, para. 63.
[1181] Article 8 (1), 2012 PNR Agreement.

information needs to be masked.[1182] In this way all information that could reveal sensitive and personal information are pseudoymised. Subsequent to the five-year period in an active database, PNR data shall be transferred to a dormant database for a period up to ten years. This dormant database shall be subject to even further controls by restricting the number of authorised personnel, as well as a higher level of supervisory approval being required before access.[1183] Dormant data can be re-personalised if needed for law enforcement operations and in connection to an identifiable case, threat or risk.[1184] While it is difficult to clearly define the notion of 'threat' it is concerning that 'identifiable case, threat or risk' is not explicitly related to the purpose of the Agreement. It has to be noted that the nuanced retention period, applies equally to all persons that fall under the remit of the PNR Agreement. The only differentiation that is made is that data related to a specific investigation can be kept in the active database for an unspecified period of time until the investigation is over. The nuanced data retention period does also not differentiate between the usefulness of certain types of data. For instance, it is not entirely clear why all 19 data sets are treated equally when considering the long storage time.[1185] Therefore, the PNR Agreement does not meet this requirement.

Second, any data retention period 'must be based on objective criteria in order to ensure that it is limited to what is strictly necessary'.[1186] The Agreement falls short of this requirement, since it does not explicitly mention that the retention period is necessary for the purposes of the Agreement.[1187] However, in practice, this criterion is difficult to apply since the assessment of what retention period is strictly necessary obviously includes a certain level of discretion as long as necessary evidence for the appropriateness can be provided. Article 8 (6) of the PNR Agreement reflects this concern since it mentions the need to assess the necessity of the 10-year dormant period in the next PNR Agreement evaluation. While it is questionable why the evaluation shall not include an assessment of the five-year active retention period it

[1182] Ibid., Article 8 (2).
[1183] Ibid., Article 8 (3).
[1184] Ibid.
[1185] AG Opinion on *Opinion 1/15*, para. 284.
[1186] *DRI*, para. 64.
[1187] Ibid., para. 63.

shows that policy-makers acknowledge the difficulty in determining a period based on objective criteria.[1188]

One might wonder why data needs to be retained at all for such a long period if it merely serves the purpose of screening for a potential threat when passengers travel to the US. The justification for long retention periods is to detect long-term patterns of suspected criminals.[1189] Respectively, suspicion in some cases only arises when specific travel patterns exist (i.e. by taking unnecessarily expensive routes or flying multiple times to certain countries) or when the journey is booked via specific travel agencies or with specific credit cards. Thus, in some cases the data of suspects needs to be crosschecked with earlier travel patterns in order to corroborate or reject suspicion. This in turn is only possible if data is available over a longer period of time.[1190] Furthermore, the average lifetime of criminal networks and the investigation of those take up several years.[1191] While this is a valid justification for opting for a longer retention period, it is difficult to assess whether this period is also 'objective'.[1192] Especially in respect to terrorism and serious crime it is very difficult to detect overall patterns and as such any time period carries a certain amount of arbitrariness with it.

Third, irreversible destruction of the data at the end of the prescribed data retention period shall be ensured.[1193] The Agreement also falls short of this requirement since nowhere it is specifically mentioned that data shall be irreversible destructed. The reference to destruction is made in Article 8 (4) stipulating that "following the dormant period, data retained must be rendered fully anonymised by deleting all data types which could serve to identify the passenger to whom PNR relate without the possibility of repersonalisation".[1194] This provision only refers to anonymisation and not irreversible deletion. Since 'anonymisation' techniques -such as randomisation or generalisation- is fraught with technical difficulties, full

[1188] While the evaluation of the PNR Agreement is an important safeguard against arbitrariness, the review as such can be criticised. For instance, neither the 2005 nor the 2010 joint review report states reasons for the need to prologue the initial 3.5 years period.
[1189] Interview with EU Commission official.
[1190] Ibid.
[1191] AG Opinion on *Opinion 1/15*, para. 279.
[1192] This period would probably qualify as 'objective' if statistics reveal the usefulness of data after such long time periods in a number of cases. However, this type of statistics is often not publicly available.
[1193] *DRI*, para. 67., *Zakharov v. Russia*, para. 255. See also: *Klass and Others v. Germany*, para. 52 or *Kennedy v. United Kindom*, para 162; *Tele 2 Sverige*, para. 122.
[1194] Article 8 (4), 2012 PNR Agreement.

destruction is not guaranteed.[1195] In addition to that, Article 8 (5) of the PNR Agreement mentions that data related to a specific case or investigation may remain in the active PNR database until the case or investigation is archived.[1196] Thus data that falls into this category is not subject to any specified retention period. The 2015 report of the DHS Privacy Office acknowledges deficiencies on this particular point. The report finds that "during the course of this review, the DHS Privacy Office found that there might be a high percentage of PNRs that are inaccurately linked to a law enforcement event and therefore not depersonalized after six months."[1197] Thus, compliance due to technological capabilities poses another challenge to the PNR Agreement's compliance with data retention safeguards.

3.4.3 Onward transfer of PNR data

Any public security legislation needs to include precautions when data is transferred to third parties.[1198] Furthermore, an adequate level of data protection cannot be circumvented when transferring data to third countries.[1199] If those principles are interpreted *sensu stricto* in relation the PNR Agreement it would be illegitimate to further transfer data under the PNR agreement to a US authority other than DHS and to a third country if the EU did not establish adequacy first or if an independent EU authority has oversight of how data is processed in that third country or institution. In the following the different types of onward transfer are assessed.

Onward transfer is possible for the purposes of the agreement under articles 16 and 17[1200] and has three dimensions. First, US-internal transfer of data to other US agencies is possible if equivalent or comparable safeguards exist in those agencies.[1201] It is concerning that no list has been provided of agencies that are eligible to receive PNR data. Furthermore, since the agencies only have to prove 'comparable' data

[1195] An overview of these shortcomings can be found in: Opinion 05/2014 of the Article 29 Data Protection Working Party on Anonymisation Techniques, *WP216*, adopted on 10 April 2014.
[1196] Article 8 (5), 2012 PNR Agreement.
[1197] United States Department of Homeland Security Privacy Office report on the use and transfer of passenger name records between the European Union and the united states of 26 June 2015. Retrieved 12.01.2017 from:
https://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf
[1198] *Weber and Saravia v. Germany*, para. 95.
[1199] *Schrems*, para. 73.
[1200] Article 16 and 17, 2012 PNR Agreement.
[1201] Ibid., Article 16 (1).

protection safeguards (instead of equal), one could speak of a standard that is a 'derivative of the EU derivate'. While Article 16 ensures that other agencies can only make use of the data for purposes which fall within the ambit of the agreement[1202] the fact that data protection standards might be lower raises the risk of misuse or loss of data.

Second, onward transfer can also concern the sending of data to third countries. Respectively, Article 17 stipulates that apart from *emergency circumstances*, any transfer shall occur pursuant to *express understandings* that data protection standards comparable to those applied to PNR by DHS shall be incorporated.[1203] One concern is that emergency circumstances have not been closely defined leaving it unclear whether it refers to an imminent threat through terrorism or whether it also includes other situations (such as to protect the vital interest of the data subject or others). Furthermore, the third country needs to demonstrate a comparable data protection level by way of 'express understanding' whereas it is not clear what legal status this would have. In addition, Article 17 (4) stipulates that "where DHS is aware that PNR of a citizen or a resident of an EU Member State is transferred, the competent authorities of the concerned Member State shall be informed of the matter at the earliest appropriate opportunity."[1204] While the notification to competent authorities in the Member State of the citizen is a step forward in terms of transparency, it is not clear why it is linked to the condition that DHS *is aware* of a data transfer as there should be no reason for it to not be aware of a transfer.[1205]

The third dimension of onward transfer is a re-transfer of intelligence derived from PNR data to EU law enforcement agencies. It is mentioned that "(…) DHS shall provide competent police, other specialised law enforcement or judicial authorities of the EU Member States and Europol and Eurojust within the remit of their respective mandates, as soon as practicable, relevant, and appropriate, analytical information obtained from PNR in those cases under examination or investigation to prevent, detect, investigate, or prosecute within the European Union terrorist offences and related crimes (…)."[1206] In this way the PNR data exchange between the EU and US goes beyond the exchange of raw data and extends the aim of the agreement to

[1202] Article 16 (1a), 2012 PNR Agreement.
[1203] Ibid., Article 17 (2).
[1204] Ibid., Article 17 (4).
[1205] EDPS Opinion of 9 December 2011, para. 27. The EDPS mentioned that DHS should always be aware of data transfers.
[1206] Ibid., para. IX

exchanging intelligence.

While in the case of the third dimension of onward transfer Member States are directly bound by the EU Charter when processing personal information, there are concerns in regard to the first two dimensions. On the one hand, transfer is only dependent on the DHS assessment. Prior authorisation is neither needed from a judicial authority nor from an independent administrative authority.[1207] On the other hand, the Agreement neither requires that the competent national authority of the Member State of the data subject nor the Commission is notified in advance of the transfer.[1208] Instead it is only mentioned that this shall happen if DHS is aware of the transfer and at the earliest opportunity. The mere *post factum* review cannot ensure a potentially wrong assessment of the level of protection afforded nor restore privacy if needed.[1209]

3.4.4 Remedies

According to the Charter everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[1210] Articles 11 and 12 of the PNR Agreement regulate the rights for access, correction and rectification by mentioning that any individual regardless of nationality, country of origin or place of residence is entitled to request his or her PNR from DHS and/or may seek the correction or rectification (including the possibility of erasure or blocking) of his/her PNR by DHS.[1211] Furthermore, Article 8 (3) CFREU mentions that an independent authority shall monitor compliance with these rights. Respectively, the Agreement establishes an 'oversight authority' which is in charge of monitoring the safeguards included in the Agreement and which is entitled to receive, investigate, respond and redress complaints in relation to non-compliance with the Agreement.[1212] Nevertheless, it is nowhere explicitly spelt out that this authority can receive,

[1207] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU" of 9 December 2011, para. 26. See also: AG Opinion on *Opinion 1/15*, para. 300 and *Tele2 Sverige*, para. 123.
[1208] AG Opinion on *Opinion 1/15*, para. 300.
[1209] AG Opinion on *Opinion 1/15*, para. 302. See also: *Szabó and Vissy v. Hungary*, para. 77.
[1210] Article 8 (2), CFREU.
[1211] Article 11 (1) and 12 (1), 2012 PNR Agreement.
[1212] Article 14 (1), 2012 PNR Agreement.

investigate and respond to complaints lodged by an individual concerning their request for access, correction or rectification of their PNR data. Furthermore, the independence of the oversight authority is questionable.[1213] The PNR Agreement stipulates that oversight over data protection safeguards shall be carried out by the DHS Chief Privacy Officer.[1214] Entrusting the oversight role to a DHS- internal privacy officer is critical since he/she is subject to influence of the responsible minister and thus independence in accordance to Article 8 (3) CFREU is not fully guaranteed.[1215]

The Agreement also mentions the availability of administrative and judicial redress. In regard to the former, Article 13 (4) points to the DHS Traveller Redress Inquiry Program (DHS TRIP). It has been introduced to resolve all travel-related inquiries including those related to the use of PNR. It provides a redress process for individuals who believe that they have been delayed or prohibited from boarding because they were wrongly identified as a threat.[1216] While this simplified administrative procedure is a step in the right direction, there has been criticism in regard to its functioning in practice. Particularly in regard to no-fly lists travellers are often not notified of why they are being denied boarding or are subjected to additional screening.[1217] The fact that remedies should not only be mentioned in the legislation but be effective in practice was also stressed in *DRI*. The CJEU mentioned that the law in question must impose "(…) minimum safeguards so that the persons whose data have been retained have *sufficient* guarantees to *effectively* protect their personal data (…)."[1218]

If administrative remedies have been exhausted, data subjects should in light of Article 47 CFREU be able to access judicial remedies enabling him/her to challenge an adverse decision before national courts.[1219] Every individual can request judicial review under provisions of the Administrative Procedure Act and in accordance with relevant provisions of (i) the Freedom of Information Act, (ii) the Computer Fraud and Abuse Act, (iii) the Electronic Communications Privacy Act and

[1213] See: *Zakharov v. Russia*, para. 278 and 279. See also: Case C-518/07, *Commission v Germany*; Case C-614/10l *Commission v Austria* and Case C-288/12 *Commission v Hungary*.
[1214] Article 14, 2012 PNR Agreement.
[1215] See: AG Opinion on *Opinion 1/15*, para. 315.
[1216] Article 13 (4), 2012 PNR Agreement.
[1217] Ramsey, M. (2014). A Return Flight for Due Process? An Argument for Judicial Oversight of the No-Fly List. Retrieved 12.01.2017 from http://dx.doi.org/10.2139/ssrn.2414659, p. 11
[1218] *DRI*, para. 54 (emphasis added by author); *Schrems*, para. 95.
[1219] *Schrems*, para. 64

(iv) other applicable provisions of US law.[1220] It is however interesting to note that judicial review can only be requested "of any final agency action by DHS" it is thus not clear what happens if data has been shared with other US agencies. Apart from the laws mentioned, it is also worth pointing out that both Article 11 on access for individuals and Article 12 on correction and rectification explicitly mention that any refusal shall inform individuals of the options available under US law for seeking redress. The recently adopted judicial redress act shall also apply to any non-US citizens. However, in the last PNR review its application to the PNR Agreement was not yet entirely clear.[1221]

3.4.5 Data security

An adequate data security strategy needs to account for: (i) the vast quantity of data whose retention is required; (ii) the sensitivity of the data; (iii) the risk of unlawful access to data requiring data integrity and confidentiality.[1222] The 2012 PNR Agreement includes detailed provisions on how to ensure appropriate technical measures and organisational arrangements to protect data.[1223] For example, the Agreement mentions that appropriate use of technology is made to ensure data protection, security, confidentiality and integrity. More specifically, data shall be held in a secure physical environment and encryption mechanisms should exist.[1224] Moreover, the Agreement mentions that after six months data shall be masked and pseudonymised.[1225] Ultimately, breach notifications in case of a privacy incident shall be issued. It is however not clear, what qualifies as a 'significant privacy incident' and which information needs to be contained in a breach notification to the individual.[1226] However, generally the PNR Agreement accounts for the vast quantity of data, the sensitivity of the data and the risk of unlawful access through adequate technological and organisational means.

[1220] Article 13 (3), 2012 PNR Agreement.
[1221] European Commission Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, *SWD(2017) 14 final*, p. 16.
[1222] *DRI*, para. 66; *Tele2 Sverige*, para. 122.
[1223] Article 5, 2012 PNR Agreement.
[1224] Ibid.
[1225] Article 8, 2012 PNR Agreement.
[1226] EDPS Opinion of 9 December 2011 op.cit, para. 21.

In *DRI* the Court ruled that the data security safeguards of the DRD were not adequate because providers can take economic considerations into account when determining the level of data security. The repealed DRD mentioned that "the data shall be subject to *appropriate* technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alternation, or unauthorised or unlawful storage, processing, access or disclosure."[1227] The data security provision in the PNR Agreement is very similar: "DHS shall ensure that *appropriate* technical measures and organisational arrangements are implemented to protect personal data and personal information contained in PNR against accidental, unlawful or unauthorised destruction, loss, disclosure, alteration, access, processing or use."[1228] Given the similarity of the provisions, it can be assumed that the 2012 Agreement does not comply with the standards established by *DRI*. Nevertheless it is necessary to take one major difference into account. In *DRI* the Court focused its reasoning mainly on the nature of traffic and location data when discussing data security standards. Accordingly, the judges criticised the fact that the DRD did not sufficiently take the vast quantity of data and the sensitive nature of that data and into account.[1229] While both under the PNR Agreement and the DRD a vast quantity of data is processed, the data under the DRD (traffic and location data) is considered as a sensitive category of data which is not the case for categories of PNR data. However, as stated earlier, PNR data can include sensitive data which is also a special category of data.

3.5 Applicability of jurisprudence to the PNR Directive

As explained earlier in this chapter, one effect of the EU-US PNR Agreement has been 'norm-internalisation' leading to the adoption of the PNR Directive. Thus, it is necessary to also assess what effect case law could have on the EU internal PNR regime. In regard to the interference with Articles 7 and 8 CFREU and the justification for this interference the same findings apply as those stated above in sections 3.2 and 3.3. Although the substance of the PNR Directive is similar to the PNR Agreement it is still necessary to assess proportionality separately. First of all

[1227] Article 7 (b), DRD.
[1228] Article 5 (1), 2012 PNR Agreement.
[1229] *DRI*, para. 66.

this is due to the fact that an "assessment depends on all the circumstances of the case, such as the nature, scope duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by national law."[1230] Second, since the EU internal PNR regime is an EU Directive instead of an international Agreement, it is not only bound by the Charter but also by EU secondary law. The proportionality assessment also needs to take into account that in contrast to the PNR Agreement no compromise with a non-EU country was necessary.[1231]

3.5.1 Proportionality of interference with Articles 7 and 8 CFREU

(i) Indiscriminate transfer and access to data

First, transfer and access to data should be strictly limited to the purpose of preventing and detecting serious offences.[1232] The Directive sets out that the purpose of PNR data processing is the prevention, detection, investigation and prosecution of terrorist offences and serious crime.[1233] Article 6 further specifies the purpose by mentioning three instances in which processing is allowed: (i) carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities or by Europol in regard to terrorism or serious crime; (ii) responding to requests from the competent authorities to provide and process PNR data in specific cases when necessary to address terrorism and serious crime; (iii) analysing PNR data for the purpose of updating or creating new criteria to be used in the assessments to identify any persons who may be involved in a terrorist offence or serious crime.[1234] All of these points support the overarching purpose of preventing, detecting, investigating and prosecuting terrorism and serious crime.

Second, the Directive also precisely defines the nature of the crimes covered.[1235] A detailed account is provided in regard to the meaning of terrorism by

[1230] *Kennedy v. United Kingdom*, para. 153.
[1231] AG Opinion on *Opinion 1/15*, para. 7.
[1232] *DRI,* para. 61; *Tele2 Sverige*, para. 111.
[1233] Article 1 (2), PNR Directive.
[1234] Ibid., Article 6.
[1235] *Zakharov v. Russia*, para. 248; *DRI*, para. 61.

referring to Articles 1 to 4 of Framework Decision 2002/475/JHA.[1236] Furthermore, a list of offences qualifying as 'serious crime' is annexed to the Directive.[1237]

Third, access to data shall be limited to a small number of authorised persons.[1238] The PNR Directive requires Member States to sets up Passenger Information Units (PIUs) which are in charge of "collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities."[1239] Furthermore, PIUs are in charge of exchanging both PNR data and the results of processing those data with the PIUs of other Member States and with Europol in accordance with Articles 9 and 10.[1240] Thus, PIUs have the authority to both access data in the first place and to transfer data to authorities within the Member State or to other Member States. While this shows that the Directive clearly designates PIUs as bodies in charge of accessing PNR data, the Directive leaves the composition of PIUs very broad since Member States can decide to designate an authority. For example, it could either be an already existing authority in charge of fighting terrorism and serious crime or it could be a newly established body. In both cases it is also not clearly stated that the size of PIU's needs to be strictly limited to what is necessary for the purpose of complying with the Directive. While this may be justified to account for the differences in the Member States' criminal justice systems, the differences may make some PNR regimes more vulnerable to risks of abuse than others.

Fourth, the Directive defines the target group liable to interception[1241] by mentioning that PNR data is collected from passengers of extra-EU flights.[1242] Nevertheless, it is at the Member State's discretion to also apply the Directive to all or selected intra-EU flights. This means that the *ratione personae* scope potentially extends to all passengers landing on EU soil. While this implies a massive scope which goes even beyond the one of the EU-US PNR Agreement, it has been argued earlier that the purpose of the broad scope of PNR regimes is to allow law enforcement authorities to identify individuals who were previously not known to the authorities. Thus, limiting the scope *ratione personae* to suspects or only to a

[1236] Article 3 (8), PNR Directive.
[1237] Annex II, PNR Directive.
[1238] *DRI*, para. 62.
[1239] Article 4 (2) (a), PNR Directive.
[1240] Ibid., Article 4 (2) (b).
[1241] *Liberty and others v. UK*, para. 64 or *Szabó and Vissy v. Hungary*, para. 66 -67.
[1242] Article 1 (1) (a), 2012 PNR Directive.

particular region would render the purpose of the agreement meaningless in this respect.[1243]

Fifth, according to case law, access and use of data needs to be dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary.[1244] As stated earlier it is possible to wave the requirement of ex-ante review as long as sufficient ex-post judicial oversight is guaranteed.[1245] Due to the considerably high amount of transfers and access this seems to apply in this case.

(ii) Retention period

As mentioned before there are three parameters to assess the retention period. First, data retention periods shall be strictly limited according to the usefulness of the data for the purposes pursued.[1246] The data retention period under the PNR Directive is five years in total while depersonalisation of all data that could reveal the identity of a passenger is required after six months.[1247] The information to be depersonalised is explicitly mentioned in the form of an exhaustive list and seems to cover all categories from Annex I that could indeed reveal a person's identity.[1248] The 5-year retention period does not differentiate between the usefulness of the different PNR data categories nor between the persons concerned.[1249] Nevertheless, additional safeguards have been added since disclosure of depersonalised data can only be permitted if approved by a judicial authority or a national authority competent under national law.[1250] While this adds an additional safeguard, the Directive does not specifically point out *to whom* data shall be disclosed.

Second, the CJEU also held that any data retention period 'must be based on objective criteria in order to ensure that it is limited to what is strictly necessary'.[1251] The Directive falls short of this requirement, since it does not explicitly mention that the retention period is necessary for the objectives pursued in the Directive.[1252]

[1243] See: AG Opinion on *Opinion 1/15*, para. 244.
[1244] DRI, para. 60; *Szabó and Vissy v. Hungary*, para. 73.
[1245] *Szabó and Vissy v. Hungary*, para. 77 and case law cited.
[1246] *DRI*, para. 63; AG Opinion on *Tele 2 Sverige,* para. 242.
[1247] Article 12 (1) and (2), PNR Directive.
[1248] Note that it covers frequent flyer information in Article 12 (2) (d) which was not included in the EU-Canada PNR Agreement and explicitly criticised by the AG in his Opinion on *Opinion 1/15*.
[1249] *DRI*, para. 63.
[1250] Article 12 (3) (b), PNR Directive.
[1251] *DRI,* para. 64. AG Opinion on *Tele2 Sverige*, para. 242.

Third, irreversible destruction of the data at the end of the prescribed data retention period has to be provided for.[1253] The Directive mentions that all PNR data has to be permanently deleted after the expiry of the maximum retention period of five years.[1254] Nevertheless, this requirement does not apply where specific PNR data has been transferred to competent authorities in the context of specific cases for fighting terrorism and serious crime.[1255] In those situations retention has to be regulated by national law. While it can be argued that handling of data during national criminal procedures goes beyond the competences of the EU, it has to be acknowledged that EU action on PNR triggered interference with Article 7 and 8 CFREU. Therefore, establishing core guarantees such as the irreversible destruction of data cannot be left to Member States alone.[1256]

(iii) Onward transfer of PNR data

Under the PNR Directive onward transfer of PNR data has four dimensions. First, within a Member States onward transfer happens between PIUs and 'competent authorities'.[1257] Article 6 (2) (a) of the Directive mentions that PIUs shall be in charge of assessing all PNR data in order to detect passengers who need to be further examined by competent authorities. Thus it is clear that PIUs are tasked with filtering out targeted data for competent authorities. Nevertheless, when mentioning the circumstances in which PIUs can transfer data to competent authorities it is mentioned that PIUs *shall transfer data received from air carriers or the results of* those data to the competent authorities.[1258] It is not clear why this provision keeps onward transfer to competent authorities so broad without explicitly mentioning that it should be restricted to specific cases where a suspicion exists or where appropriate actions for fighting serious crime and terrorism need to be taken. This does not meet the standard of the *DRI* judgement mentioning that objective criteria should exist by which to determine the limits of the access of the competent national authorities to the

[1252] AG Opinion on *Opinion 1/15*, para. 280.
[1253] *DRI*, para. 67; *Zakharov v. Russia*, para. 255; *Klass and Others v. Germany*, para. 52 or *Kennedy v. United Kingdom*, para 162; AG Opinion on *Tele 2 Sverige*, para. 243.
[1254] Article 12 (4) of the PNR Directive.
[1255] ibid.
[1256] AG Opinion on *DRI*, para. 120.
[1257] Article 4 (2) (a), PNR Directive. Competent authorities are those authorities in charge of fighting terrorism and serious crime and shall be determined in each Member State.
[1258] Ibid.

data and their subsequent use.[1259]

Second, the Directive also regulates the transfer between Member States. On the one hand, PIUs shall be in a position to exchange and request PNR data among themselves. For example if one PIU identifies a suspicious person via PNR data all other PIUs shall be informed so that they can take appropriate actions in case the person travels to another Member State. [1260] Furthermore, PIUs can request data elements from other PIUs if it is duly reasoned.[1261] The Directive requires independent review of such data exchange only after data is depersonalised after six months. However, all such requests should be subject to authorisation by a judicial or independent administrative authority in case it is transferred to other authorities. On the other hand the competent authority of one Member State shall also be in a position to request data from a PIU in another Member State in emergency cases.[1262] In this case, the competent authority shall still channel their request through the PIU of its Member State.

Third, the Directive also regulates the onward transfer to Europol by stipulating that it can request data from PIUs on a case-by-case basis if the data lies within its competences and is necessary for the performance of its tasks.[1263] While it is mentioned that Europol needs to notify its data protection officer of each exchange[1264] it is not mentioned that PIUs can either refuse to transfer data to Europol or that it should depend on authorisation by a judicial or independent administrative authority. It is surprising that such a safeguard mechanism exists in respect to requests by national competent authorities (at least after the initial 6 months) but not in regard to Europol.[1265]

The fourth dimension is the onward transfer to third countries. Member States can transfer either PNR data or the results of processing to third countries on a case-by-case basis. There are several safeguards in regard to the transfer. First of all, it is explicitly mentioned that transfer can only take place for the purposes of the Directive.[1266] Second, transfer has to comply with Decision 2008/977/JHA which

[1259] *DRI*, paras. 60 and 61. See also: EPDS Opinion 5/2015, para. 42.
[1260] Article 9 (1), PNR Directive.
[1261] Ibid., Article 9 (2).
[1262] Ibid., Article 9 (3).
[1263] Ibid., Article 10 (1).
[1264] Ibid., Article 10 (3).
[1265] For national competent authorities, see Article 9 (2) PNR Directive.
[1266] Article 11 (1) (b), PNR Directive.

among others mentions that the third country shall have an adequate level of protection.[1267] Third, the transfer shall happen with the consent of the Member State from which the data originates[1268] and in case this is not possible due to exceptional circumstances ex-post verification shall take place.[1269] Fourth, after an initial six months the transfer has to be authorised by a judicial authority or an independent administrative authority.[1270] While these safeguards have to be positively acknowledged, it can be criticised that it is not specified which Member State authority can conduct the onward transfer (i.e. the PIUs or competent authorities).

In sum, several safeguards are included in respect to onward transfer of PNR data on national, EU and international levels. However, it is concerning that in some cases the nature and purpose of PNR data to be transferred is not sufficiently specified. Furthermore, prior authorisation is not always needed from either a judicial authority or from an independent authority.[1271] While in exceptional situations the lack of ex-ante authorisation can be justified if sufficient ex-post review measures are present, no or only mere *post factum* review in some of the instances mentioned above might not be able to ensure a potentially wrong assessment of the level of protection afforded nor restore privacy if needed.[1272]

(iv) Remedies

In accordance with Article 8 (2) CFREU, the Directive specifies that each passenger shall have the same right to protection of their personal data, rights of access, rectification, erasure and restriction.[1273] The Directive further refers to the provisions of Framework Decision 2008/977/JHA as well as its implementing measures in national law in regard to the availability of these rights.[1274] Passengers are entitled to send a request to access, rectification or erasure to the data protection officer in the PIU of each Member State who function as a single point of contact for all processing of PNR data.[1275]

[1267] Article 11 (1) (a) PNR Directive and Article 13 (1) (d) Framework Decision 2008/977/JHA
[1268] Article 13 (1) (c) Framework Decision 2008/977/JHA
[1269] Article 11 (2), PNR Directive.
[1270] Ibid., Article 11 (1) (d).
[1271] EDPS opinion of 9 December 2011, para. 26. See also: *DRI*, para. 62. See also: AG Opinion on *Opinion 1/15*, para. 300.
[1272] AG Opinion on *Opinion 1/15*, para. 302. See also: *Szabó and Vissy v. Hungary*, para. 77.
[1273] Article 13 (1), PNR Directive.
[1274] Framework Decision 2008/977/JHA, Articles 17 and 18.
[1275] Article 5 (3), PNR Directive.

In accordance with Article 8 (3) CFREU and relevant case law[1276] the Directive also stipulates that a national supervisory authority -as specified in Framework Decision 2008/977/JHA- shall monitor compliance with data subject rights.[1277] Each national supervisory authority shall receive and investigate complaints lodged by individuals, verify the lawfulness of data processing, and advise data subjects on the exercise of their rights under the Directive.[1278] Furthermore, the Framework Decision also specifies that national supervisory authorities shall have access to all relevant information, shall be able to order the blocking, erasure or destruction of data and shall have the power to engage in legal proceedings.[1279] Ultimately, in light of Article 47 CFREU data subjects shall also be able to access judicial remedies enabling him/her to challenge an adverse decision before national courts.[1280] The Directive regulates judicial remedies as well as compensation by reference to Framework Decision 2008/977/JHA.[1281]

It can be concluded that the Directive in accordance with Framework Decision 2008/977/JHA offers sufficient safeguards for individuals in respect to the rights to access, rectification and erasure, the right to lodge a claim before a national supervisory authority and to access judicial remedies.

(v) Data security

It is stipulated that the PIUs shall implement "appropriate technical and organisational measures and procedures to ensure a high level of security appropriate to the risks represented by the processing and the nature of the PNR data."[1282] The Directive also includes some other provisions on data security for instance when discussing depersonalisation of data after six months or when discussing data protection principles in general.[1283] In accordance with CJEU jurisprudence, the Directive also states that storage of data shall take place in a secure location within the territory of the EU.[1284] Ultimately, the Directive also makes explicit references to the DPD and the 2008 Framework Decision which both contain detailed provisions on data security.

[1276] *Tele2 Sverige*, para. 123.
[1277] Article 15 (1), PNR Directive.
[1278] Ibid., Article 15 (3).
[1279] Article 25 (2), Framework Decision 2008/977/JHA
[1280] *Schrems*, para. 64
[1281] Article 13 (1), PNR Directive.
[1282] Ibid., Article 13 (7).
[1283] Ibid., Article 13 (6).
[1284] Ibid., Article 6 (8).

For example, the PNR Directive explicitly refers to Article 22 of the 2008 Framework Decision which establishes that the controller and the processor shall take into account "(…) the state of the art and the cost of their implementation, [and] such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."[1285]

4. The PNR Agreement and 'political actorness' of the CJEU

As outlined in the previous section relevant ECtHR and CJEU jurisprudence is at least partially applicable to the EU-US PNR Agreement. This raises the question as to whether and under which circumstances the CJEU can exhibit political actorness in relation to further regulation of PNR. First of all, the fact that the EU-Canada PNR Agreement is currently under scrutiny by the CJEU already demonstrates a certain degree of political actorness of the CJEU since it is in a position to influence developments on PNR. A factor facilitating the EP's decision to question the Canada PNR Agreement was obviously timing as the *DRI* judgement was published just in time when the EP was asked to consent to the PNR Canada Agreement.[1286] Moreover, the EP mentioned that the reason for referring the matter to the CJEU is not solely the uncertainty about whether the findings of the *DRI* judgment might also apply to other existing instruments but also to obtain guidance on the legitimacy of potential future PNR regimes. Respectively, a MEP mentioned: "Russia, Mexico, Korea and other countries with weaker data protection rules are collecting passenger flight information and might want to negotiate their own agreements soon. It should be clear that any agreement, present or future, must be compatible with EU treaties and fundamental rights and must not be used as a means to lower European data protection standards via the back door."[1287] This statement provides an indication of how for instance the EP can exploit the CJEU's findings in steering future legislative initiatives. Nevertheless, the political actorness of the CJEU is limited which has been demonstrated with the recently adopted PNR Directive. While the EP stressed during the negotiation phase that the findings of *DRI* need to be accounted for, the adopted

[1285] Article 22 (1) Framework Decision and Article 13 (2) PNR Directive.
[1286] Interview with EU Commission official.
[1287] "MEPs refer EU-Canada air passenger data deal to the EU Court of Justice" retrieved 12.01.2017 from: http://www.europarl.europa.eu/news/en/news-room/20141121IPR79818/MEPs-refer-EU-Canada-air-passenger-data-deal-to-the-EU-Court-of-Justice

text still does not comply with CJEU-generated principles. It can thus be argued that political actorness depends heavily on the acceptance of court-generated principles by political actors.

Turning to the question how likely it is that the EU-US PNR Agreement will be affected obviously depends on the CJEU's deliberations when providing its judgment on the Canada Agreement. In contrast to what has been found in regard to the SWIFT Agreement (see Chapter 6 above) the Commission would be under much higher pressure to terminate/amend the EU-US PNR Agreement due to the almost identical purpose and similar nature of the two agreements. Furthermore, it would be difficult to justify upholding the EU-US PNR Agreement if subsequent regimes with other countries were based on different conditions.

Conclusion

The aim of this chapter was to assess how the EU institutional framework shaped data protection and privacy in regard to the EU-US PNR Agreement. Hypothesis two (*i.e. the EU institutional framework enables EU legislative actors to pursue strategic preferences in the legislation-making process and thereby influences the way privacy and data protection is shaped in the public security context*) has been confirmed since the EU institutional framework fostered strategic preference formation of institutional actors which influenced the way data protection and privacy was framed in the context of the PNR Agreement. Five key observations have been made in this respect. First, the EU Commission emerged as the key driver of the initial negotiations due to transnationalism, the exclusion of the EP and by framing PNR as a data protection matter. Second, the EP exploited the cross-pillar nature of PNR to instrumentalise the CJEU for its strategic purposes and thereby triggered the annulment of the first PNR Agreement. Third, after the annulment of the first Agreement, the EP continued attempting to influence the way privacy and data protection was shaped through venue shopping. Fourth, when the EP got the right to retroactively vote on the second PNR Agreement, the EP's sensitivity to failure shaped privacy and data protection in a sense that the EP accepted policy outcomes with lower standards than it originally postulated. Fifth, it has also been illustrated that norm-taking played a role in initiating the development of an EU internal PNR regime. While norm-taking is not

considered a strategic preference *per se*, it has been shown that after the norm taking took place, strategic preferences were formed.

The chapter also analysed and confirmed Hypothesis 3 (*i.e. the transitional nature of the EU institutional framework contributed to the CJEU's evolution from a 'legal basis arbiter' to a political actor in its own right that increasingly determines substantial aspects relating to privacy and data protection in the public security context*). It has been shown that while pre-Lisbon the CJEU's role was limited to ruling on the legal basis of the PNR Agreement, post-Lisbon CJEU principles have had an impact on data protection and privacy in relation to the EU-US PNR Agreement. By applying the framework established in Chapter 3 it was shown that the Agreement infringes Articles 7 and 8 CFREU. First, transfer and access to data is not strictly limited to the purpose of preventing and detecting serious offences since on a case-by-case basis data can be used and processed where necessary if ordered by a court. Second, the nature of crime giving rise to the agreement is not precisely defined and only the degree of seriousness of the offences in which cases US authorities are entitled to process PNR data is mentioned. Third, the authority responsible for accessing and processing PNR data is not sufficiently limited since the Agreement does not consistently refer to one designated authority. Fourth, the data retention period is not sufficiently limited. While a nuanced data retention period exists the Agreement fails to differentiate between the usefulness of certain types of data. Furthermore, the retention period is not limited based on objective criteria and irreversible destruction of the data is not explicitly required. Fifth, safeguards in relation to onward transfer are limited to a *post factum* review which might not be sufficient in all cases. Sixth, the Agreement fails to define the competences of the data protection oversight body and does not sufficiently ensure its independence. Furthermore, the effectiveness of administrative and judicial remedies can be doubted. In regard to the PNR Directive, requirements are stricter in than the case of the PNR Agreement but some aspects still raise concerns. Last but not least, it has also been shown that the CJEU has been given the opportunity to exercise political actorness in regard to determining privacy and data protection in the PNR context. However, it is rather a conditional political actorness since the PNR Directive still does not live up to all CJEU-generated principles.

PART III – CONCLUDING REMARKS AND FUTURE PERSPECTIVES

CHAPTER 7 – CONCLUSION

1. Summary of findings

As highlighted in the introduction, there are two dynamics which can be understood as the wider context in which the research of this thesis took place.[1288] On the one hand, the omnipresence of personal data in the digital age has transformed the *modus operandi* of public security bodies, raising concerns about a nation's ability to conduct mass surveillance. On the other hand, this new modus operandi gains legitimisation from real threats as well as threat perceptions. Thus, reconciling privacy and data protection with public security concerns is highly context dependent and fluctuating depending on events and related discourse. While bearing in mind this wider context, the aim of this thesis was to understand how the EU institutional framework shapes data protection and privacy in regard to data retention and access measures. Three case studies were scrutinised for that purpose: the Data Retention Directive and the PNR and SWIFT regimes. In Chapter 2, three hypotheses in accordance to NI were presented in an attempt to answer the overarching research question. In the following, conclusions in respect to each hypothesis will be drawn.

Hypothesis 1: 'Privacy and Data Protection in AFSJ' is an institutional framework in transition implying that both established as well as new institutional features co-exist and commonly determine how data protection and privacy is shaped in relation to public security.

The thesis has confirmed the first hypothesis since the institutional framework is marked by incremental transformation where some aspects exhibit features of 'old paths' while others exhibit new structures. Turning points or so-called 'critical junctures' and institution-internal uncertainties have contributed to the transitional character of the institutional framework while path-dependence led to the stickiness to the institutional status quo. Two key 'critical junctures' have been identified which in many respects triggered change: the entry into force of the Lisbon Treaty and the adoption of the CFREU. It is also relevant to assess the underlying causes for

[1288] Chapter 1, sections 5.1 and 5.2.

institutional change. While more generally it can be argued that the Treaty of Lisbon and the adoption of CFREU are the outcome of European integration, in the particular case of privacy and data protection in AFSJ the role of events and processes should not be underestimated in triggering institutional change. For example, the attacks on 9/11 and the Snowden revelations had a particular impact on determining the paths of EU-US relations and led to a political prioritisation at EU level. In addition, technological change and the transnational nature of data flows and its implications for data protection and privacy are underlying factors that led to change.

Chapter 2 of this thesis provided insights into the meaning of the term 'institution' and/or 'institutional framework' in accordance with NI. These terms refer to the 'operating framework' that organises actions of institutional actors into predictable and reliable patterns. In the context of the thesis, the legal framework that structures privacy and data protection for public security purposes is considered to be the relevant 'institutional framework'. Respectively, a holistic view has been taken by including constitutional rules on privacy and data protection; secondary legislation laying down more practice-oriented rules; procedural rules applicable to legislation-making when data protection and privacy for public security purposes is at stake; and CJEU and ECtHR case law.

In a further step, Chapter 3 examined the institutional framework on privacy and data protection in AFSJ from a HI perspective. On a constitutional level, a particularity of the institutional framework is the fact that both the ECHR and CFREU play a role in shaping privacy and data protection in the public security context. However, while the ECHR only recognises the right to privacy as a fundamental right, the CFREU distinguishes between the right to privacy and the right to data protection. It has been demonstrated that there are multiple interpretations aiming to explain the deviation from the constitutional path laid down by the ECHR such as the drafters' attempt to provide more legitimacy to the EU data protection framework; the attempt to address problems that emerged due to technological developments; the attempt to extend the application of data protection principles to former third pillar areas and to international relations; and the fact that the EU could not easily accede to other international instruments such as the Council of Europe Convention 108. It has also been shown that by granting data protection the status of a fundamental right, CFREU – in theory- represents a significant deviation from institutional traditions developed mainly by the ECHR and respective jurisprudence. However -in practice- by entering

into judicial dialogue with the ECtHR, the CJEU adheres to the ECtHR conceptualisation of privacy and its correlation to data protection. Consequently, CFREU's constitutional innovation was to date not able to function as critical juncture and path-dependence can be observed in respect to the conceptualisation of privacy, data protection and their correlation. This could change however in the future. For instance, in *Tele2 Sverige* the Court for the first time mentioned explicitly that the two rights are distinct but without explaining this in further detail.

Although the conceptualisation of privacy and data protection is to date path-dependent, it has been illustrated that the entry into force of CFREU provided the CJEU with an opportunity to emerge as the primary actor in shaping data protection and privacy in the public security context. Respectively, the thesis first established a toolkit illustrating how recent CJEU case law – by being founded on ECtHR principles– assesses the legality of data processing measures in light of privacy and data protection.[1289] In a second step it is shown that while ECtHR jurisprudence continues to play a role, the CJEU seems to be the new trendsetter due to institutional reasons such as the integrationist bias of CJEU jurisprudence and the more agile structure of CJEU offering more and speedier venues for litigation. The changing relevance of ECtHR and CJEU jurisprudence has been illustrated with the recent ECtHR's reference to CJEU case law in *Zakahrov v. Russia*. From a HI perspective, a slow transition to a new paradigm can be detected where the growing importance of CJEU jurisprudence vis-à-vis ECtHR jurisprudence deviates from existing paths.

Transition towards a new path has also been detected in respect to privacy and data protection in AFSJ as laid down by the treaties and secondary legislation. It has been shown that although over the years AFSJ matters were increasingly regulated on EU level until the adoption of the Treaty of Lisbon the institutional framework for AFSJ was complex and fragmented. In this environment data protection and privacy were mainly regulated in regard to specific sectors and thus multiple data protection regimes co-existed in an autonomous manner. The lack of consistency can be ascribed to the inherent paradox of AFSJ cooperation on EU level. On the one hand, Member States consider public security to be a matter at the heart of national sovereignty. On the other hand, Member States increasingly realised that EU integration of some aspects such as free movement cannot be seen in isolation from security. Finally, the

[1289] Details on this toolkit are further explained under Hypothesis 3 below.

adoption of the Lisbon Treaty can be regarded as a 'critical juncture' in the sense that it harmonised many of the previously fragmented areas. While even after Lisbon the autonomous data protection regimes still continue to exist, the adoption of the Police and Criminal Justice Directive at least establishes EU-wide standards when data is processed for law enforcement and public security purposes. This shows that existing complexities are the results of a previously established path while at the same time the Lisbon Treaty resulted in a new, more unified approach.

The external dimension of AFSJ is also an example of the incremental transition towards a new path. Chapter 3 explained that the Lisbon Treaty contributed to a more consistent approach to the external relations of AFSJ. This is also evident in regard to EU-US relations where a paradigm change over time can be observed. While EU-US relations on public security matters began to institutionalise shortly after 9/11 the initial phase of this cooperation was marked by US supremacy and it can even been argued that the EU had a reactive and norm-taking role. However, several 'critical junctures' resulted partially in more 'actorness' of the EU: (i) the adoption of the Lisbon Treaty resulted in more consistency in EU external relations, allowing the EU to be more assertive in negotiations; (ii) the Snowden revelations led to more reluctance among EU institutional actors to uncritically tolerate public security practices that interfere with the rights to privacy and data protection and (iii) the increasing role of the CJEU in determining how privacy and data protection ought to be treated in the public security context had a direct impact on the relationship.

In sum, the core argument under Hypothesis 1 was that privacy and data protection in AFSJ is a transitional institutional framework as reflected in constitutional, competence-related and legislative modifications. This transitional nature can be traced back to multiple dynamics but this thesis treated European integration in form of the Lisbon Treaty and the adoption of the CFREU as the two key drivers.

Hypothesis 2: The EU institutional framework enables EU legislative actors to pursue strategic preferences in the legislation-making process and thereby influences the way privacy and data protection is shaped in the public security context.

In regard to the overarching research question how the EU institutional framework shapes data protection and privacy in respect to the data retention and access regimes, the thesis analysed the way stakeholders interacted with the institutional framework in the policy formation stage and in the further stages of the DRD, the PNR and SWIFT regimes. Seven aspects have been identified revealing that strategic preferences have guided the behaviours of legislative actors confirming Hypothesis 2. Each of those aspects are summarised below.

(i) Cross-pillarisation and power struggles

Due to the shift from pre- to post-Lisbon procedures, a core dynamic in relation to all three regimes is *cross-pillarisation* and corresponding *power struggles*. As has been shown in Chapter 2 as well as the case study chapters, the term refers to the institutional complexity of AFSJ measures and the corresponding questions it raises about what constitutes an appropriate legal basis and what are the adequate decision-making procedures. Policy actors have in all three cases exploited the blurriness of the EU pillar structure in order to pursue strategic preferences.

In respect to the DRD it has been shown that policy-making actors exploited cross-pillarisation to increase their influence in the legislation-making procedure. Data retention has an internal market dimension by harmonising legal requirements imposed on service providers in the EU. However, the ultimate aim of any data retention measure is to make retained data available to competent authorities if requested for the investigation, detection or prosecution of serious crime. This ambiguity obviously invited actors to advocate for the legal basis that grants them more benefits. The Council advocated for a framework decision excluding the EP from the legislation-making process and thereby speeding up the process and circumventing opposition. Contrarily, the Commission preferred a directive in order to maximise its own influence in potential follow-up processes and to increase democratic accountability and transparency. Determining the legal basis was not only crucial for the power allocation among legislative actors but determines the legal

safeguards applicable to privacy and data protection as during the negotiations for the DRD no data protection instrument existed in the third pillar.

In regard to the SWIFT Agreement it has been shown that the institutional framework encouraged power struggles for more legislative influence between the EP and the Council which led to a revision of the SWIFT Agreement and thus to the re-shaping of privacy and data protection. The first SWIFT Agreement was adopted after only four months of EU-US negotiations and just one day before the adoption of the Lisbon Treaty, which would have granted the EP co-decision rights. As a consequence the Agreement was heavily criticised for two reasons. First, the provisions on safeguarding the rights to privacy and data protection were considered insufficient. Second, the EP was deliberately excluded from the policy-making process and was not granted access to relevant documentation. In this context the EP exploited the legislative framework to maximise its future influence on shaping data protection and privacy. First, it instrumentalised the CJEU by demanding access to all relevant TFTP information held by the Council in *Council v. In't Veld.* Second, the EP made use of its retroactive right to vote on the SWIFT Agreement in 2010 to reject the Agreement which can be considered to be a demonstration of power vis-à-vis other policy-making actors but at the same time had a positive impact on the protection of the rights to privacy and data protection.

In respect to the PNR Agreement, the EP exploited the cross-pillar nature of PNR and instrumentalised the CJEU for strategic purposes and thereby triggered the annulment of the first PNR Agreement. It has been described how the EP took legal actions both against the Agreement and the Commission's Adequacy Decision shortly after it had been adopted. Among others the EP argued that the first pillar is not the correct legal basis because the Decision's aim is not the establishment and functioning of the internal market but to make data processing of personal data lawful in line with US legislation. Furthermore, the EP also argued that the Agreement infringes the right to protection of personal data. The CJEU only reacted to the EP's plea on the legal basis and decided that a third pillar legal basis would have been the correct one. Since this deprived the EP of its co-legislative rights the annulment plea can be regarded as a warning at all costs to the Council and the Commission to not exclude the EP in the future. While it has been argued that normative considerations were the key driver of the EPs actions, the fact that the annulment resulted in a lower

level of protection of individuals' rights to privacy and data protection contradicts this assumption.

(ii) Legislation-making procedures and sensitivity to failure

The co-decision procedure was introduced with the Maastricht Treaty (1992) but only with the entry into force of the Lisbon Treaty the co-decision procedure –which was renamed to ordinary legislative procedure-[1290] was applied to former third pillar topics. Given the EP's strong opposition to all three data retention and access regimes it seemed logical that privacy and data protection standards would improve as soon as the EP had a say in the legislation-making procedure. Nevertheless, this expectations was not fully met and the EP frequently agreed to measures which it criticised sharply on previous occasions. It has been demonstrated that the legislation-making procedure (especially the fast-track procedure) contributed to strategic preference formation and sensitivity to failure which ultimately determined policy outcomes.

In respect to the DRD, it has been shown that under the fast-track procedure – an expedited version of co-decision- expected positive outcomes in respect to safeguards on privacy and data protection did not materialise. Since the fast-track procedure leaves more room for informal discussions than the traditional co-decision procedure it facilitates 'political horse trading' and in the case of the DRD to lower than expected data protection and privacy safeguards. The two majority parties were able to side-line the rapporteur and the LIBE committee by reaching a deal with the Council under the fast-track procedure. This behaviour does not reflect the usual critical stance of the EP and the rationale for this behaviour can be explained with 'sensitivity to failure', long term strategic considerations or simply shared beliefs.

In regard to PNR, the EP got the right to retroactively vote on the second PNR Agreement. Against expectations, the EP's sensitivity to failure led to lower privacy and data protection safeguards. It has been shown that the EP set out several data protection principles that should be included in the new Agreement. However, the EP ultimately accepted the Agreement although not all of those principles had been taken on board. In Chapter 6 it has been argued that after becoming a co-legislator and thus sharing legislative responsibility the EP became more *sensitive to failure.* This is linked to the EP having an integrationist bias implying that deviation from the original

[1290] Article 294 TFEU (ex-Article 251).

mandate is always considered more favourably than maintaining the status quo.

(iii) Transgovernmentalism

Another relevant strategy revealing power maximization techniques is transgovernmentalism. The idea of transgovernmentalism refers to a mode of governance where sub-national actors intensively interact with each other, sometimes by circumventing their own national governments and in order to gain power. The term 'sub-national actors' can refer to a wide range of actors who are below the level of heads of state and government, such as ministerial officials or law enforcement agencies. Originally, transnationalism was applied to assess the interaction between sub-national actors within the EU in the AFSJ field.[1291] Nevertheless, this thesis applies transgovernmentalism by analysing how actors such as the European Commission or the European Parliament build strategic transatlantic networks in order to enhance their chances to achieve their strategic preferences in the EU context.

In regard to the SWIFT Agreement, the institutional framework fostered strategic transgovernmentalism between EU and US actors which played a role in shaping privacy and data protection both when the first and the second Agreement were adopted. It has been shown that the US was in a stronger position than the EU due to the TFTP programme originating in the US and due to the fragmented EU legal framework. In this context the involved actors framed negotiations in two ways. First, the US built strategic alliances on an informal basis with actors from the Council and the Commission by establishing forums such as the High-Level Political Dialogue on Border and Transportation Security and the High-Level Contact Group on data protection. It has been shown that these channels of informal cooperation excluded the EP and contributed to a mutual understanding between the Commission/Council and US actors on how privacy and data protection should be shaped. The second aspect was lobbying efforts towards the EP. When the US administration became aware of the possible rejection of the Interim Agreement efforts were made to pressure the EP into acceptance of the Agreement. After those efforts failed the US changed its 'strategy of deterrence' into a 'strategy of inclusion'.

[1291] Lavenex, S. (2009). Transgovernmentalism in the Area of Freedom, Security and Justice. In: Tömmel, I. & Verdun, A. (eds.) *Innovative Governance in the European Union. The Politics of Multilevel Policymaking*, Boulder: Lynne Rienner.

This contributed to the Parliament's more uncritical acceptance of the second SWIFT Agreement even though the provisions on privacy and data protection did not match the EP's original expectations.

In respect to the PNR Agreement, the EU Commission emerged as the key actor in the initial negotiations due to intensive transnational cooperation. The Commission led initial discussions with the US where it stressed full solidarity with the US policies on the prevention and combat of terrorism and with the need to find practicable solutions on PNR transfers. By signing a joint statement -without the Council's approval- right after the first round of negotiations, the Commission revealed its ambitions to remain the main negotiator on the matter. The Commission also managed to exclude the EP from participating in the initial negotiations. For example, the Commission neither shared updates on the progress of the negotiations with the Parliament nor did it take the EP's concerns into consideration. Ultimately, by framing PNR transfer as a data protection matter the Commission further carved out competences from the Council and the EP. The Commission was a key actor in negotiating the adequacy decision between the EU and the US which is foreseen under the Article 25 (6) DPD. It has to be noted that this exclusive role did not remain undisputed. The responsible EP rapporteur threatened the Commission to instrumentalise the CJEU if it did not allow a greater role for the EP in the negotiations.

(iv) Other aspects revealing strategic preferences

Besides the three main institutional variables, there are at least three other institutional dynamics that can be detected when analysing the three data retention and access regimes.

First, if a significant event takes place some policy actors are able to exploit the consequences of the event in order to make their strategic preferences seem to be a collectively superior outcome. Policy formation depends on the intersection of three different streams (the problem, policy and politics streams). When the three streams intersect, i.e. when a problem is recognized while simultaneously a solution is available, and the political climate is providing the right context for change, a *window of opportunity* emerges enabling policy change.[1292] In respect to the DRD many

[1292] See: Kingdon J. W. (1995) *Agendas, Alternatives and Public Policies*. London: Longman.

scholars regarded the London and Madrid bombings as the main driver of the adoption of the DRD. However it has been illustrated how the ambition of introducing data retention measures had already developed in the 1990s. The two before-mentioned terror events were merely a 'window of opportunity' legitimizing the initiative. The public security concerns arising from the bombings allowed the Council to make use of an AFSJ-related institutional particularity which grants Member States the right of initiative on AFSJ policy matters in case where the proposal is put forward by a quarter of the Member States.[1293] In this way, the DRD's appearance on the agenda is an outcome of the Council's long-term objective to regulate data retention on the EU level rather than being exclusively the reaction to terror events.

Second, venue shopping takes place when policy actors explore all formal and informal (even unusual or innovative) venues to maximize their influence in the legislation-making process. After the annulment of the first PNR Agreement, the EP continued attempting to influence the way privacy and data protection was shaped through venue shopping. By stressing the principle of loyal cooperation between the EU institutional players the EP President urged the Council and Commission to keep the Parliament informed about any new developments and to take its views into account. Furthermore, the EP requested full co-decision rights on PNR with the help of the 'passerelle' clause. Ultimately, since no instrument on data protection in the third pillar yet existed, the EP continued to provide guidelines and opinions on how the PNR Agreement should safeguard data protection. It has to be noted though that none of these attempts have been successful.

Third, strategic preference formation also determines the willingness to initiate regulatory debates. In the case of the SWIFT Agreement, the fact that the TFTP was initially carried out in secret meant that safeguards on rights to privacy and data protection were non-existent. This can partially be ascribed to the lack of sincere cooperation between EU institutional actors. It has been shown that the ECB had been informed about the data transfers to the US since the TFTP's beginning in 2001 because it belonged to the SWIFT supervisory committee. The non-disclosure of the data transfers to the US conflicts with the principle of sincere cooperation as stipulated in Article 13 (1) and (2) TEU. The ECB explained non-disclosure with the

[1293] Article 76 (b) TEU (former Article 34 (2) TEU).

fact that its mandate in the supervisory committee was restricted to detecting and advising on risks to financial stability and the integrity of financial infrastructures. This shows that that ECB was subject to a different institutional framework impacting its preference formation when deciding not to act or initiate discussions on future legislation with other EU institutional actors.

Ultimately, it has been illustrated that norm-taking played a role in initiating legislative discussions in respect to the PNR regime. Right from the beginning of the PNR negotiations, particularly the Council and the Commission were persuaded of the usefulness of PNR data for public security purposes. Furthermore, the Commission scented the opportunity for actorness by stating that the EU's approach cannot be limited to responding to the initiatives of others. In subsequent years, the Commission's ambition was to develop an internal PNR regime which failed however due to institutional changes triggered by the Lisbon Treaty and due to the opposition of the EP. Only through the threats posed by 'foreign terrorist fighters' did a window of opportunity allow the adoption of the PNR Directive in 2016. While norm-taking is not a strategic preference *per se*, it has been shown that after the norm-taking took place, strategic preferences were formed at EU level.

Hypothesis 3: The transitional nature of the EU institutional framework contributed to the CJEU's evolution from a 'legal basis arbiter' to a political actor in its own right that increasingly determines substantial aspects relating to privacy and data protection in the public security context.

It has been shown that pre-Lisbon the CJEU's role in respect to the case studies was confined to ruling on the legal basis and in one case on access to information. In this way the CJEU was primarily a 'legal basis arbiter' determining power allocations between policy makers whilst they shaped privacy and data protection in relation to the data retention and access regimes. The changes of the institutional framework in the post-Lisbon era provided the CJEU with the necessary tools to increasingly litigate on substantive terms and thus proactively shape data protection and privacy in the public security context. For example, spill-over judgments emerged giving the CJEU the opportunity to further develop previously established principles; CJEU decisions have been instrumentalised in legislative debates and have been used to support the mandate of legislative actors; and the integration bias of judgments reveal

the overarching direction 'political actorness' is taking. Nevertheless, the extent of political actorness is not unconditional. Several aspects have been detected which limit the extent of political actorness in the policymaking process. For example, path-dependence to previous ECtHR and CJEU case law limits the degree of novelty applied by the Court. Furthermore, timing and related institutional and behavioural constraints limit the *de facto* effects of CJEU's decisions. Ultimately, also strategic preferences of policy makers are decisive in a sense that they can either further encourage that court-generated principles are reflected in legislation or they can limit the influence thereof. Consequently, referring back to the continuum between the constrained and dynamic view on Courts described in Chapter 2, the findings of the thesis can be described as a 'conditional dynamic' view.[1294]

(i) CJEU's role as a 'legal basis arbiter'

In regard to all three case studies the CJEU played an important role as a 'legal basis arbiter' before the entry into force of the Lisbon Treaty. Furthermore, the Court was instrumentalised by legislators with a view to allocate and rectify competences during the legislation-making process.

In respect to the PNR Agreement, pre-Lisbon the CJEU was instrumentalised by the EP since it asked the CJEU to rule on the first PNR Agreement. It has been shown that although the EP put arguments on the substance of the Agreement to the CJEU, the Court decided to only rule on the legal basis without making any reference to the PNR Agreement's impact on fundamental rights. The Court held that the first pillar was the wrong legal basis for both the Commission's adequacy decision and the subsequent Council decision legitimising the transfer of PNR data to US authorities. The CJEU claimed that the PNR regime entails elements that concern the functioning of the internal market by harmonizing requirements for airline companies. However, the primary concern of the regime is to protect public security by combatting terrorism. Hence, the Court annulled both acts, implying that any re-negotiation needed to take place under third pillar procedures. The CJEU ruling created a *lacuna legis* in regard to the protection on privacy and data protection since at the time of annulment no EU legal instrument on data protection in the third pillar existed. The CJEU's reluctance to extend its reasoning beyond legal basis considerations could be

[1294] See Chapter 2, section 2.6.3.

related to the fact that the CJEU felt that in the absence of fundamental rights enshrined in the EU legal order, it would interfere disproportionality with EU policy decisions involving third countries.[1295]

Based on the Court's findings in respect to the PNR Agreement, Ireland challenged the legal basis of the DRD. Here, the Court came to a different conclusion by rejecting the argument that the instrument had to be based on the third pillar. Instead the Court argued that the minimum harmonisation approach adopted by the legislator implies that the Directive exclusively harmonises practices taking place under the first pillar. All data processing that relates to the activities of law enforcement authorities is beyond the remit of the Directive. The CJEU's arguments seem appropriate when purely focusing on the reach of the Directive. However, it nonetheless fails to take the DRD's purpose and its wider implications into account. In terms of implications, the CJEU's DRD judgment has contributed to further legislative development since the EP had for the first time legislative influence in regard to an instrument which has third pillar implications. In this way the CJEU shaped privacy and data protection in the public security context since it prevented the emergence of a *lacuna legis* as was the case in regard to the PNR Agreement. The CJEU seemed to prefer the first pillar legal basis to claim authority on potential future requests dealing with proportionality, especially in light of the upcoming Lisbon Treaty.

In respect to the SWIFT Agreement the CJEU did not play a role in regard to determining the legal basis of the instrument. Instead, the Court contributed to the power allocation between the legislative actors with its ruling on access to information. The Dutch MEP Sophie in't Veld sought access to a Council document containing an opinion of the Council's legal service on the legal basis of the SWIFT Agreement. The Council refused access since it claimed that secrecy in respect to the negotiations between the Council and US counterparts outweighed the public interest of disclosure. The Court rejected the Council's arguments by stressing that the existence of a disagreement between the EP and the Council on the powers of the

[1295] For example on one occasion, the AG contemplated that when ruling on international agreements it must be borne in mind that those agreements are the outcome of international negotiations with a third country which in in the absence of a satisfactory agreement, may reject to conclude the agreement and prefer to find unilateral solutions. (AG Opinion on *Opinion 1/15*, para.7). This shows that the CJEU is well aware of the delicate nature of international agreements. However, in this particular case the AG also concedes that this does not mean that "(…) the Court must lower the degree of vigilance which it has shown in relation to respect for the fundamental rights protected in EU law." (para. 8).

institutional actors does not justify secrecy for the sake of credibility in negotiations for an international agreement. The judgment can be considered to follow the trend set by previous 'access to information' rulings.[1296] In this way the CJEU seems to encourage openness and transparency in international negotiations. However, above all, ruling in favour of transparency also re-balances the institutional power allocation between the EP and the Council.

(ii) CJEU and political actorness post-Lisbon

After the entry into force of the Lisbon Treaty the importance of legal basis considerations ceased due to the abolition of the pillar structure. Furthermore, the extended competences granted to the CJEU and the adoption of CFREU resulted in a shifting role of the CJEU on privacy and data protection in AFSJ. In order to analyse 'political actorness' of the CJEU the thesis adopted a two-fold approach. The first step consisted of analysing the legality of the measure in accordance to the framework established in Chapter 3. This helped in understanding whether there is any room for 'political actorness'. The second step involved the assessment of whether CJEU-generated principles do or have the potential to influence the way privacy and data protection is shaped in the respective policy field. In the following both steps are summarised.

Chapter 3 established a framework to analyse the legality of the DRD, the SWIFT and PNR Agreement by laying down three criteria. First, it needs to be assessed whether the measure is accessible, foreseeable and respects the essence of the rights to privacy and data protection. Second, proportionality in terms of necessity with regard to legitimate objectives pursued needs to be analysed. Third, it needs to be analysed whether the measure is proportionate in terms of laying down sufficient safeguards against the abuse of power. Under this point various parameters are discussed such as scope of application, grounds for access to data, oversight on access to data, remedies, data retention period, data security and onward transfer.

The assessment of the DRD mainly focused on assessing and critiquing *DRI* and *Tele2 Sverige* but also took other relevant cases into account. It has been shown that the DRD did not meet the criteria established by CJEU and ECtHR jurisprudence

[1296] T-331/11, *Besselink v Council of Europe* of 12 September 2013.

in multiple ways: (i) the purpose and scope of data retention was not sufficiently limited; (ii) no objective criterion existed by which to determine the limits of access to the retained data; (iii) access to retained data was not subject to prior review by a court or an independent authority; (iv) the data retention period was not sufficiently limited because no differentiation is made between the different types of data and their usefulness; and (iv) no stringent rules on data security were in place. It has also been demonstrated that the CJEU applies a path-dependent conceptualisation of privacy and data protection whilst having a strong stance on safeguards applicable to Articles 7 and 8 CFREU in the context of data retention.

In respect to the SWIFT Agreement it has been demonstrated that in light of recent case law, some aspects of the SWIFT Agreement are disproportionate. For example, the Agreement does not strictly limit the persons who are eligible to access and use data under the SWIFT Agreement. This is because the agreement only mentions that persons who investigate terrorism or its financing can access data without specifically determining the organisations that can access data. Further, the SWIFT Agreement falls short of the requirement that an independent administrative authority or a court needs to review access since the law enforcement authority Europol is entrusted with this task. Another aspect is that the Agreement does not sufficiently limit the retention period of non-extracted personal data since no requirement to depersonalise data exists.

In respect to the PNR Agreement several arguments have been put forward showing that the Agreement is not proportionate in light of Articles 7 and 8 CFREU. For instance, the nature of crimes giving rise to the Agreement is not precisely defined and instead only the degree of seriousness of the offences entitling US authorities to process PNR data is mentioned. A further example is that the Agreement fails to define the competences of the data protection oversight body and does not sufficiently ensure its independence. In regard to the PNR Directive, requirements are stricter than the case of the PNR Agreement but some aspects still raise concerns such as the fact that the scope of PIUs who are in charge of accessing PNR data are not sufficiently limited.

Having illustrated how none of the measures pass the legality assessment, the second step of the analysis was to analyse whether CJEU-generated principles which do or can influence the way privacy and data protection is shaped in regard to SWIFT, PNR

or DRD. In regard to the DRD, it has been argued that the CJEU's annulment of the DRD can be interpreted as example of 'political actorness' for three reasons. First, the judgment left the crucial question on whether indiscriminate data retention can at all be proportionate unanswered which resulted in a lack of legal certainty on the political level. The uncertainty of the judgment triggered a spill-over effect on similar data retention and access regimes on the EU level by having triggered follow-up cases such as *Opinion 1/15* and *Tele2 Sverige*. A second aspect indicating the CJEU's actorness is the fact that the judgement was used by legislative actors as strategic tool. For example, the EP used the findings of *DRI* in the negotiations of the PNR Directive and it has already been indicated that any future PNR regime needs to comply with the CJEU-generated principles. Ultimately, political actorness can be detected since the nature of the judgment reveals an integrationist bias. By making more specific safeguards a pre-condition for proportionality of any potential future measure the CJEU indirectly required stronger harmonisation at EU level.

In regard to the SWIFT Agreement it has been shown that the EP requested shortly after the *DRI* judgement its legal service to elaborate on the impact of the judgment on the SWIFT Agreement and as shown earlier case law has implications for the legality of the SWIFT Agreement. However, no further action has been taken by political actors due to institutional reasons. On the one hand, requesting an opinion on an agreement can only happen either before the adoption of the agreement (as was the case for the EU-Canada PNR Agreement) or within two months after adoption. On the other hand, the Commission's willingness to take action was also limited due to institutional memory relating to the difficulty to reach the current Agreement. To conclude, it has been shown that timing and institutional memory are relevant factors in limiting the degree to which a judgment can directly shape the strategic preferences of policy makers in respect to related policy areas.

In regard to PNR, it has been shown that the timing was favourable since the EP's consent to the EU-Canada PNR Agreement coincided with the aftermath of the *DRI* judgment. It remains to be seen which conclusion the CJEU will reach in respect to the legality of the Agreement. If the CJEU follows the AG by declaring the Agreement void the next question will be how far these findings will translate into real changes of the EU-US PNR Agreement and potentially even the PNR Directive. As established in the thesis, the EU-US PNR Agreement and the PNR Directive do not comply with existing jurisprudence showing that CJEU generated principles only

influenced subsequent legislation to a limited extent. However, if the CJEU invalidates the EU-Canada PNR Agreement the pressure to reconsider the EU-US Agreement is potentially much higher not least due to the danger of follow-up requests to the CJEU.

2. Relevance and future perspectives

As summarised in the previous section, this thesis focused on analysing the evolution of data protection and privacy in the public security context and on how EU institutional actors exercised influence within this transitional context. The core of the research focused on three regimes that emerged in the past but which have been continuously modified and which are still controversial at present. The added value of the approach chosen in this thesis lies in its interdisciplinary and holistic nature. By applying New Institutionalism the thesis went beyond a legal assessment on how privacy and data protection is or ought to be safeguarded. Instead the thesis also analysed the wider constitutional and legislative landscape as well as the behaviours of EU institutional stakeholders involved in all stages of the policy-making cycle. In this way the importance of political factors in determining, interpreting and applying the law has been illustrated. This has ultimately helped to unravel and understand the complexities involved in reconciling the rights to privacy and data protection with public security considerations.

The holistic nature of the thesis' approach might be beneficial for other research. For example, it can be applied to study similar regimes such as the EU-Canada and EU-Australia PNR Agreements or the future EU PNR Agreements with third countries. It could also be applied to study other regimes which fall under the AFSJ umbrella, such as migration databases (e.g. SIS II, VIS, EURODAC). Respectively, the approach should add value to the existing academic debate by providing a holistic account of how legal and political factors shape privacy and data protection in the case of migration databases. In this way, it could make a contribution by uniting literature from political science and legal research camps.

The findings of this thesis can also help to identify possible future trends in relation to privacy and data protection in the public security context. The thesis has shown that **'**privacy and data protection in AFSJ' is an institutional framework in evolution

wherein new and old features coexist. It can be expected that rather than ongoing transformation and volatility the changes that have already occurred will further 'institutionalise' in the near future leading to more institutional stability or 'normalisation'. On the one hand this is due to the fact that CFREU and new legislation are more cautiously designed to factor in underlying disruptions such as technological change and the transformative nature of public security threats. On the other hand this is due to pragmatic considerations. Since major transformations as evident in respect to privacy and data protection in AFSJ take multiple years to be planned and to ultimately materialise it is unlikely that the institutional framework will be subject to major changes soon.

Therefore, evaluating the future of privacy and data protection in the public security context will focus mainly on how actors will interact with the new institutional framework. As pointed out earlier, the abolition of the pillar structure reduces the leeway granted to EU institutional actors to exploit institutional intricacy to pursue strategic interests whilst choosing or disputing the legal basis of an instrument. Therefore, post-Lisbon it will be more important to assess strategic preference formation and tools (such as *transnationalism* or *sensitivity to failure*) during the ordinary or fast track legislation-making procedure or to study why certain initiatives are politically prioritised (e.g. due to *window of opportunity* or *norm-taking*). The previous aspects might be worth testing when future initiatives emerge or when the current regimes are amended. However, as soon as full legislative powers were granted to the EP, the mandates of the EP, the Commission and the Council converged at the expense of a vivid discussion on how to safeguard privacy and data protection. In this context, it could be argued that the CJEU superseded the European Parliament in being the 'champion of privacy and data protection'. Thus in the near future the new competences as well as the more antagonistic approach of the CJEU will render it even more important in shaping data protection and privacy in the public security context. Respectively, in the following some ideas are provided on where CJEU input might be crucial in the future.

First, the CJEU ought to clarify the correlation between privacy and data protection. Traditionally the CJEU has followed ECtHR jurisprudence by adopting the inherency approach and thus has not taken the constitutionalisation of data

protection in CFREU into account.[1297] In *Tele2 Sverige* the CJEU has for the first time explicitly expressed the distinctiveness of Articles 7 and 8 CFREU.[1298] However, the proportionality assessment still does not acknowledge this distinction. The reason for the CJEU's hesitations is at least partially related to the complex interaction between CJEU and ECtHR jurisprudence. Maintaining consistency between the two legal orders is crucial for legal certainty of Member States falling within the remit of both jurisdictions and for the continuous legitimacy of both courts.[1299] At the same time however, it is crucial to elaborate more extensively on the conceptual correlation particularly since the statement in *Tele2 Sverige* stands in contrast to previous CJEU conceptualisations.

Second, the CJEU should also elaborate more extensively on the implications of declaring that public security is a fundamental right stipulated in Article 6 CFREU.[1300] This statement was made in *DRI* and stands in contrast to earlier interpretations of both Article 6 CFREU and its ECHR equivalent Article 5 which only stress the liberty dimension of the articles. While substantially deviating from earlier interpretations, the Court did not analyse this point further. Instead it subsequently treats public security only as a legitimate ground for limiting Articles 7 and 8 CFREU. This raises the question as to whether a proportionality assessment balancing Article 6 CFREU with Articles 7 and 8 CFREU would result in a different conclusion favouring arguments advocating for safeguarding Article 6 CFREU? This aspect might be an interesting subject for future CJEU litigation as well as future research in general.

Third, post-Lisbon the discussion is likely to shift from the question on "which pillar is the adequate legal basis?" to the question of whether a measure falls at all under EU law. While *Tele2 Sverige* clarified that retention and access of traffic and location data for public security purposes falls under the remit of the e-privacy Directive this might be different for other data categories.[1301] This loophole has to be

[1297] Chapter 3, section 2.5.
[1298] *Tele2 Sverige*, para. 129.
[1299] Chapter 3, section 2.5.
[1300] *DRI*, para. 42.
[1301] If the GDPR or the Directive do not apply to national processing, the latter must still respect the essence of Articles 7 and 8 CFREU which essentially extends the level of protection where EU does not apply (see: C-300/11 *ZZ v Secretary of State for the Home Department* of 4 June 2013 where the CJEU held that provisions of the Charter also apply in cases where national (or state) security is concerned.) However, the fact that national measures are not subject to CJEU oversight could limit the effectiveness of this safeguard.

considered particularly in the context of the current political environment where discourse in some EU Member State governments is marked by security concerns and anti-EU sentiments.

Fourth, future developments in respect to EU-US relations will also be subject to further CJEU intervention. Most relevantly for this thesis, *Opinion 1/15* is still outstanding. If the CJEU follows the AG Opinion this would most likely imply yet another re-negotiation of the EU-US PNR Agreement to introduce currently lacking safeguards.[1302] In addition, the new Privacy Shield has been challenged in front of the Irish High Court and depending on the outcome further amendments to the Shield might be necessary.[1303] These two cases demonstrate the increasing importance of the CJEU in upholding European values -including human rights- in EU external relations. Article 21 (1) TEU stresses that EU international relations shall be guided by principles that have inspired the EU's own creation including the rule of law and fundamental rights. However, as illustrated in this thesis, transatlantic cooperation mechanisms do not always live up to those EU values. In this context, the CJEU is faced with the challenging task of ensuring that the rights of EU citizens and residents are protected in line with CFREU while simultaneously acknowledging that international agreements are the outcome of a compromise between the EU and another jurisdiction. While recent case law has put a particular emphasis on the former consideration, it will be interesting to analyse how far upcoming jurisprudence will translate into substantial changes on the legislative level. The current political climate and the strong security bias of the Trump administration might prevent the incorporation of CJEU-generated principles in legislative outcomes. For instance, recently an Executive Order was enacted which arguably has negative implications on data protection safeguards for EU citizens that have been established laboriously over the last two decades and particularly as a result of recent CJEU rulings.[1304] In this context, EU legislators might increasingly move away from a principle-based to a 'realpolitik' approach.

[1302] While *Opinion 1/15* refers to the EU-Canada Agreement, it would most likely imply renegotiations of the EU-US Agreement (see Chapter 6, sections 3 and 4).
[1303] *Data Protection Commissioner v. Facebook Ireland Limited & Maxmilian Schrems*, 2016/4809P.
[1304] Executive Order Enhancing Public Safety in the Interior of the United States of 25th of January, sec. 14. While this Executive Order does not directly invalidate any arrangements under SWIFT, PNR, the Umbrella Agreement or the Privacy Shield, it represents a shift in how the US authorities deal with personal information collected on non-citizens.

While the four points above provide an idea on where CJEU inputs might be most crucial in the near future, other relevant questions on how to interpret EU law might arise once the GDPR and the Police and Criminal Justice Data Protection Directive become operational in 2018. To conclude on a positive note, the future of privacy and data protection in the public security context will probably be more stable from an institutional and legislative perspective than it has been before the Treaty of Lisbon has been adopted. At the same time, many questions regarding the interpretation of the new institutional framework are still open showing that privacy and data protection in the public security context remains an exciting topic to research.

Annex

1. List of cases

1.1 European Court of Human Rights cases (alphabetical order)

Amann v. Switzerland, Application no. 27798/95, judgment of 16 February 2000

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application no. 62540/00, judgment of 28 June 2007

Bosphorus v Ireland, Application no 45036/98 of 30 June 2005

B. v. France, Application no. 13343/87, judgment of 25 March 1992

Burghartz v. Switzerland, Series A No 280-B, p. 28, judgment of 22 February 1994

Christine Goodwin v. the United Kingdom, Application no. 28957/95, judgment of 11 July 2002

Cossey v. the United Kingdom, Application no. 10843/84, judgment of 27 September 1990

Evans v. United Kingdom, Application No. 6339/05, judgment of 10 April 2007

Fernández Martínez v. Spain, Application no. 56030/07 of 12 June 2014

Friedl v. Austria, Application no. 15225/89, judgment of 31 January 1995

Gaskin v. the United Kingdom, Application no. 10454/83, judgment of 7 July 1989

Guerra and others v. Italy, Application no. 14967/89, judgment of 19 February 1998

Huvig v. France, Application no. 11105/84, judgment of 24 April 1990

Kennedy v. the United Kingdom, Application no. 26839/05, judgment of 18 May 2010

Klass and others v. Germany, Application no. 5029/71, judgment of 6 September 1978.

Kopp v. Switzerland Application no. 23224/94, judgment of 25 March 1998

Kruslin v. France, Application no. 11801/85, judgment of 24 April 1990

L. L. v. France, Application no. 7508/02, judgment of 10 October 2006

Leander v. Sweden, Application no. 9248/81, judgment of 26 March 1987

Liberty and others v. the United Kingdom, Application no. 58234/00, judgment of 1 July 2008

Matthews v UK Application No. 24833/94 of 18 February 1999

M. S. v. Sweden, Application no. 20837/92, judgment of 27 August 1997

Malone v. the United Kingdom, Application no. 8691/79, judgment of 2 August 1984

McGinley and Egan v. the United Kingdom, Application nos. 21825/93 and 23414/94, judgment of 9 June 1998

McMichael v. the United Kingdom, Application no. 16424/90, judgment of 24 February 1995

Murray v. the United Kingdom, Application no. 14310/88, judgment of 28 October 1994

Niemietz v. Germany, Application no. 13710/88 of 16 September 1992.

Neulinger and Shuruk v. Switzerland, Application no. 41615/07 of 6 July 2010

Odièvre v. France Application No. 42326/98, judgment of 13 February 2003

P G and J H v United Kingdom, Application No. 44787/98, judgment of 25 September 2001

Peck v United Kingdom, Application No 44647/98, judgment of 28 January 2003

Perry v. the United Kingdom, Application no. 63737/00, judgment of 17 July 2002

Pretty v. United Kingdom, Application No. 2346/02, judgment of 29 April 2002

Rees v. the United Kingdom, Application no. 9532/81, judgment of 17 October 1986

Rotaru v. Romania, Application no. 28341/954, judgment of 4 May 2000

Schüssel v. Austria, Application No. 42409/98, judgment of 21 February 2002

Segerstedt-Wiberg and others v. Sweden, Application no. 62332/00, judgment of 6 June 2006

Stjerna v. Finland, Series A No 299-B, p. 60, judgment of 25 November 1994

Szabó and Vissy v. Hungary, Application no. 37138/14, judgment of 12 January 2016

Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands, Application no. 39315/06, judgment of 22 November 2012

Von Hannover v Germany, Application no. 59320/00, judgment of 24 June 2004

Weber and Saravia v. Germany, Application no. 54934/00, 29 June 2006

Z. v. Finland, Application no. 22009/93, judgment of 25 February 1997

Zakharov v. Russia, Application no. 47143/06, judgment of 4 December 2015

1.2 Court of Justice of the European Union cases/opinions and Court of First Instance cases (chronological order)

C-22/70 *Commission v. Council* judgment of 31 March 1971

C-181/73 *Haegeman v. Belgium* judgment of 30 April 1974

C-5/88 *Hubert Wachauf v Bundesamt für Ernährung und Forstwirtschaft* judgment of 13 July 1989

C-5/88 *Wachauf* judgment of 13 July 1989

C-227/88 *Hoechst,* judgment of 21 September 1989

Opinion 2/94 *on the Accession by the Community to the European Convention for the Protection of Human Rights and Fundamental Freedoms* judgment of 28 March 1996

C-368/95 *Familiapress*, judgment of 26 June 1997

C-185/95 *Baustahlgewebe*, judgment of 17 December 1998

C-292/97 *Karlson and others* judgment of 13 April 2000

C-94/00 *Roquette Frères*, judgement of 22 October 2002

C-187/01 and C-385/01 *Gözütok and Brügge* judgment of 11 February 2003

C-465/00, *Rechnungshof v Österreichischer Rundfunk and Others*, judgment of 20 May 2003

C-101/01 *Lindqvist* judgment of 6 November 2003

C-105/03 *Pupino* judgment of 16 June 2005

C-176/03 *Commission v Council* judgment of 13 September 2005

T-315/01 *Yassin Abdullah Kadi v Council of the European Union and European Commission,* judgment of 21 September 2005

C-344/04 *International Air Transport Association, European Low Fares Airline Association /Department for Transport*, judgment of 10 January 2006

C-94/03 *Commission v Council* judgment of 10 January 2006

C-503/03 *Commission v. Spain* judgment of 31 January 2006

Opinion 1/2003 *Competence of the Community to conclude the new Lugano Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters* judgment of 7 February 2006

Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the*

European Union and Commission of the European Communities judgment of 30 May 2006

C-317/04 and C-318/04 *European Parliament v Council*, judgment of 30 May 2006

T-228/02 *Modjahedines* judgment of 12 December 2006

C-440/05 *Commission v Council* judgment of 23 October 2007

C-91/05 *Commission v. Council*, judgment of 20 May 2008

C-275/06, *Productores de Música de Espana Promusicae vs. Telefónica de Espana*, judgment of 29 January 2008

C-308/06 *Intertanko and Others* judgment of 3 June 2008

C-402/05 P and C-415/05 *P Kadi and Al Barakaat International Foundation v Council and Commission* judgment of 3 September 2008

C-301/06 *Ireland v. Parliament and Council*, judgment of 10 February 2009

C-518/07, *Commission v. Germany*, judgment of 9 March 2010

C-400/10 *PPU J. McB. v L. E.* judgment of 5 October 2010

C-92/09 and C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, judgment of 9 November 2010

C-145/09 *Land Baden-Württemberg v Panagiotis Tsakouridis* judgment of 23 November 2010

C-208/09 *Ilonka Sayn-Wittgenstein v Landeshauptmann von Wien* judgment of 22 December 2010

C-256/11 *Murat Dereci and Others v Bundesministerium für Inneres* judgment of 15 November 2011

C-614/10 *Commission v. Austria* judgment of 16 October 2012

C-614/10 *Commission v Austria* judgment of 16 October 2012

C-539/10 P and C-550/10 P *Al-Aqsa v Council* judgment of 15 November 2012

C-300/11 *ZZ v Secretary of State for the Home Department* judgment of 4 June 2013

T-331/11 *Besselink v Council of Europe* judgment of 12 September 2013

C-473/12 *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others* judgment of 7 November 2013

C-288/12 *Commission v. Hungary* judgment of 8 April 2014

C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others v. Ireland*

judgment of 8 April 2014

Case C-131/12 *Google Spain SL, Google, Inc. v Agencia Española de Protección de Datos, Mario Costeja González* judgment of 13th May 2014

C-148/13 to C-150/13 *A and Others v Staatssecretaris van Veiligheid en Justitie* judgment of 2 December 2014

C-401/12 *Council and Others v Vereniging Milieudefensie and Stichting Stop Luchtverontreiniging Utrecht* judgment of 3 January 2015

C-362/14 *Maximillian Schrems v Data Protection Commissioner* judgment of 6 October 2015

C-601/15 *J. N. v Staatssecretaris van Veiligheid en Justitie, j*udgment of the Court (Grand Chamber) of 15 February 2016

C-203/15 and C-698/15 *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis* judgment of 21 December 2016

1.3 Other cases (alphabetical order)

Data Protection Commissioner v. Facebook Ireland Limited & Maxmilian Schrems, 2016/4809P of the Irish High Court, pending.

Decision 1 BvR 256/08 of the German Constitutional Court of 02 March 2010

Decision No. 1258 of the Constitutional Court of Romania of 8 October 2009

Decision 216/14 of the Supreme Court of Cyprus of 27 October 2015

Decision 8/2014 Bulgarian Constitutional Court Decision of 12 March 2015

Decision No 1258 of the Romanian Constitutional Court of 08 October 2009

Decision Pl. ÚS 24/10 of the Czech Constitutional Court of 22 March 2011

Secretary of State for the Home Department v. David Davis and others, [2015] EWCA Civ 1185

United States v. Powell, 379 U.S. 48, 57-58 (1964)

2. Legislation, Protocols, Conventions

African Charter on Human and Peoples' Rights (1981)

Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States

Department of Homeland Security, Bureau of Customs and Border Protection, *CE/USA/en 1*.

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, *OJ 2010 L 195/7*.

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program *OJ 2010 L 8/11*

Agreement between the United States of America and Eurojust of 6 November 2006.

Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security *OJ 2012 L 215*.

Agreement on extradition between the European Union and the United States of America, *OJ 2003 L181.*

Agreement on mutual legal assistance between the European Union and the United States of America, *OJ 2003 L 181.*

Agreement on the Cooperation between Europol and the United States of America of 6 December 2001.

American Convention on Human Rights (1969)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981.

Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2002, L-63/1.

Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States Department of Homeland Security, Bureau of Customs and Border Protection, *OJ 2004 L183/83*.

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of second generation Schengen Information System, *OJ 2007, L-205/63*

Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) (Annexed Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), *OJ 2007 L 204*.

Council Decision 2006/729/CFSP/JHA of 16 October 2006 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (annexed Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security) *OJ 2006 L 298*.

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime *OJ 2008 L 210.*

Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, *L-121/37.*

Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program. *OJ 2010 L 195/3*

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ 2008 L350/60*.

Council Decision of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security*, OJ 2012 L 215.*

Council Framework Decision of 13 June 2002 on combating terrorism, *OJ L 164/3*.

Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States, *OJ 2002 L 190/1*.

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. *OJ 2016 L 119*

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters, *OJ 2014 L 130*.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime *OJ 2016 L 119.*

Directive 2006/24/EC 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 2006, L 105

Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, *OJ 2008 L 348*.

Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of the individuals with regard to the processing of personal data and on the free movement of such data, *OJ 1995, L-281/31*.

European Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, *OJ 2004 L 235.*

European Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, *C (2016) 4176 final*.

Hessisches Datenschutzgesetz, 7 October 1970.

International Covenant on Civil and Political Rights (1966).

Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the undertakings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of passenger name record (PNR) data, and Reply by the Council Presidency and the Commission to the letter from the USA's Department of Homeland Security, *OJ 2006 C 259*.

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 2016, L 119*.

Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, *OJ 2011 L 55.*

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ 2001 L 8*.

Treaty on the Functioning of the European Union, Annex 36: Declaration on Article 218 of the Treaty on the Functioning of the European Union concerning the negotiation and conclusion of international agreements by Member States relating to the area of freedom, security and justice.

United Kingdom Regulation of Investigatory Powers Act 2000.

United States Executive Order 13,224, 66 Fed. Reg. 49,079.

United States Executive Order Enhancing Public Safety in the Interior of the United States of 25th of January.

United States Foreign Intelligence Surveillance Act (FISA), PUBLIC LAW 95-511—OCT. 25, 1978, Sec. 110.

United States Judicial Redress Act of 2015: Public Law 114–126—FEB. 24, 2016

United States PATRIOT ACT: Pub. L. No. 107-56, 115 Stat. 272 (2001), codified in 50 U.S.C.

US Presidential Policy Directive 28 (PPD-28) of 17 January 2017, sec. 2, fn.5.

United States Aviation and Transportation Security Act 2001 implemented by the US Bureau of Border and Customs Protection (CBP)), Public Law 107-71, 107th Congress.

3. Policy Documents, Recommendations, Opinions

Belgian Data Protection Authority Opinion on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas. *Opinion No. 37 / 2006 of 27 September 2006.*

Belgian proposal for Third Pillar legislation Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions. Retrieved 09.01.2017 from: http://www.statewatch.org/news/2002/aug/05datafd.htm

Council of Europe Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, *European Treaty Series - No. 181*.

Council of Europe Guide on Article 5 of the Convention Right to Liberty and Security, retrieved 04.01.2017 from http://www.echr.coe.int/documents/guide_art_5_eng.pdf

European Commission and the U.S. Treasury Department Joint Report regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *COM(2013) 843 final.*

European Commission and the U.S. Treasury Department Joint Review Report of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *COM(2014) 513 final.*

European Commission Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, *SWD(2017) 14 final.*

European Commission and the U.S. Treasury Department joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), 8-9 February 2010, Brussels, 7.4.2010.

European Commission Communication on 'Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach' *COM(2003) 826 final*.

European Commission Communication on Consequences of the entry into force of the Treaty of Lisbon for ongoing inter-institutional decision-making procedures, *COM(2009) 665 final*.

European Commission Communication to the Council and the European Parliament-Towards enhancing access to information by law enforcement agencies, *COM(2004) 429 final*.

European Commission Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Delivering an area of freedom, security and justice for Europe's citizens - Action Plan Implementing the Stockholm Programme, *COM (2010) 0171 final*.

European Commission Communication to the European Parliament and the Council - A European terrorist finance tracking system (EU TFTS), *COM(2013) 842 final*.

European Commission Communication to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows, *COM(2013) 846 final*.

European Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Delivering and area of freedom, security and justice for European's citizens – Action Plan implementing the Stockholm Programme, *COM(2010) 171 final*.

European Commission Legal Service Note for the Attention of Mr Stefano Manservisi Director General DG HOME on the Draft Agreement on the Use of Passenger Name Records (PNR) between the EU and the United States. Retrieved 12.01.2017 from: http://www.statewatch.org/news/2011/jun/eu-usa-pnr-com-ls-opinion-11.pdf

European Commission Proposal for a Council Decision on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, *COM (2016)0237 final.*

European Commission Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection,

investigation and prosecution of terrorist offences and serious crime, *COM (2011) 32 final.*

European Commission Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, *COM (2005) 438 final*.

European Commission Proposal for a Framework Decision on the use of Passenger Name Record for law enforcement purposes of 6 November 2007, *COM(2007) 654 final*.

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), *COM(2017) 10 final*.

European Commission Report on the Review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, *COM(2013) 844 final.*

European Commission Report to the Council and the European Parliament - Evaluation report on the Data Retention Directive (Directive 2006/24/EC) (2011), *COM(2011) 225 final.*

European Commission second report on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime; *COM(2011)0032*.

European Commission staff working paper on the joint review of the implementation by the U.S. Bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC of 14 May 2004, (redacted version, 12.12.2005), *COM (2005) final*.

European Commission/US Customs Talks on PNR Transmission, Joint Statement. *Brussels, 17/18 February*, para. 2. Retrieved 11.01.17 from http://ec.europa.eu/justice/policies/privacy/docs/adequacy/declaration_en.pdf

European Council and European Commission action plan on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice - Text adopted by the Justice and Home Affairs Council, *C 19/01* of 3 December 1998.

European Council Answers to questionnaire on traffic data retention, *Council Doc. 14107/02*. Retrieved 09.01.2017 from: http://www.statewatch.org/news/2003/jan/12eudatret.htm

European Council Committee on Aviation - New legal requirements by the US on 'Advanced Passenger Information System' (APIS) and 'Passenger Name Records' (PNR); *Council Doc. 6051/03*.

European Council Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001, *SN 140/01.*

European Council Conclusions of the European Council, *Council doc. EUCO 79/14* of the 27 June 2014

European Council Declaration on Combatting Terrorism of 25 March 2004. Retrieved from http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf

European Council Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism of 28 April 2004, *Council nr. 8958/04*.

European Council Exchange of Views on the Position of the Member States. Discussion by Working Party on Aviation on 28 January 2003 on New Legal Requirements by US on 'Advanced Passenger Information System' (APIS) and 'Passenger Name Records' (PNR), *Council Doc. 6051/03*.

European Council Justice and Home Affairs Council Conclusions of 20 September 2001, *SN 3926/6/01*.

European Council Justice and Home Affairs Council Meeting of 1-2 December 2005, *Council Doc. 14390/05*.

European Council Laeken Presidency Conclusions of the Laeken meeting of 14 and 15 December 2001.

European Council of Justice and Home Affairs on Interception of telecommunications of 16 November 1993, *Council doc. 10090/93.*

European Council Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, *Council doc. 5618/2/09 REV 2*.

European Council Report on European Union Priorities and Objectives for External Relations in the Field of Justice and Home Affairs. *Council doc. 7653/00,* Brussels, 6 June 2000.

European Council Report on the European Union Priorities and Objectives for External Relations in the Field of Justice and Home Affairs, *Council Doc. 7653/00*.

European Council Report on the State of Play regarding Declarations made in accordance with Article 24(5) TEU - Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), *Council doc 5311/1/09*, 19 March 2009.

European Council Resolution of 17 January 1995 on the lawful interception of telecommunications, *OJ 1996 C 329/01.*

European Council, Draft Charter of Fundamental Rights of the European Union, Text of the explanations relating to the complete text of the Charter, *CHARTE 4473/00*.

European Council, Explanations Relating to the Charter Of Fundamental Rights, *OJ 2007 C 303/17.*

European Council, Stockholm Programme of 2 December 2009, *Council doc. 17024/09.*

European Council, Tampere European Council Presidency Conclusions of 15 and 16 October 1999.

European Council, The Hague Programme of 13 December 2004, *Council doc. 16054/04.*

European Data Protection Supervisor first reaction to the Court of Justice judgment of 30 May 2006. Retrieved 11.01.2017 from https://secure.edps.europa.eu

European Parliament Committee on Civil Liberties, Justice and Home Affairs Draft Recommendation of 01 February 2012 on the Draft Council decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security; *17433/2011–C7-0511/2011– 2011/0382(NLE).*

European Parliament Committee on Civil Liberties, Justice and Home Affairs Transatlantic Dialogue of 14 May 2007. Retrieved 11.01.2017 from http://www.statewatch.org/news/2007/may/ep-us-pnr-chertoff.pdf

European Parliament Debate about the Agreement between the EU and the USA on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme, *CRE 10/02/2010*.

European Parliament Debate on data retention of 13 December 2005. Retrieved 09.01.2017 from http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20051213&secondRef=ITEM-055&format=XML&language=EN

European Parliament Legal Service on LIBE - Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others* - Directive 2006/24/EC on data retention - Consequences of the judgment, *SJ-0890/H.*

European Parliament Legal Service on the EU-US Umbrella agreement concerning the protection of personal data and cooperation between law enforcement authorities in the EU and the US. *SJ-0784/15 D(2015)57806 AC/DM/apg*, of 14 January 2016.

European Parliament Motion for a Resolution further to the Commission statement pursuant to Rule 37(2) of the Rules of Procedure by Jorge Salvador Hernández Mollar on behalf of the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs on transfer of personal data by airlines in the case of transatlantic flights**,** *B5-0187/2003*.

European Parliament Motion for a Resolution of 5 May 2010 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing. *B7-0038/2009*.

European Parliament Press Release on US Secretary of Homeland Security Michael Chertoff debates data protection with MEPs. Retrieved 11.01.2017 from http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20070514IPR06625&language=SV

European Parliament Report of 19 July 2006 with a Proposal for a European Parliament recommendation to the Council on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime, including organised crime, *A6-0252/2006*.

European Parliament Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), 2001/2098(INI) *final.*

European Parliament Report on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *COM(2011)0032 – C7-0039/2011-2011/0023(COD*).

European Parliament Resolution of 11 February 2015 on anti-terrorism measures. *2015/2530(RSP)*.

European Parliament Resolution of 11 February 2015 on anti-terrorism measures. *2015/2530(RSP)*. See also: European Council "Follow-up to the statement of the Members of the European Council of 12 February 2015 on counter-terrorism: Report on implementation of measures Report on implementation of measures by the EU Counter-Terrorism Coordinator", *Council Doc. 9422/1/15.*

European Parliament Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, *2013/2188(INI)*.

European Parliament Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, *P7_TA(2014)0230*.

European Parliament Resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance; *2013/2831(RSP)*.

European Parliament Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy, *2013/2682(RSP).*

European Parliament Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, *P7_TA(2010)0144*.

European Parliament Resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorize the opening of negotiations for an Agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing, *Eur. Parl. Doc. 0129*.

European Parliament Resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues, *P6_TA(2007)0039*.

European Parliament Resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues of 14 February 2007, *B6-0042/2007/P6_TA PROV(2007) 0039*.

European Parliament Resolution on transfer of personal data by airlines in the case of transatlantic flights, *P5_TA(2003)0097*.

European Parliament, Letter from ALDE MEPs to the Council and the Commission. Retrieved 11.01.2017 from http://www.statewatch.org/news/2007/sep/eu-pnr-alde-info-request.pdf

European Parliament, Letters from Josep Borrell Fontelles (former EP President) to Mr. José Manuel Barroso (former Commission President) and to Wolfgang Schüssel (former President of the European Council). *09.06.2006*, Brussels, retrieved 11.01.17 from: http://www.statewatch.org/news/2006/jun/eu-usa-pnr-borrell-letter2.pdf and http://www.statewatch.org/news/2006/jun/eu-usa-pnr-borrell-letter1.pdf.

European Union and United States New Transatlantic Agenda, signed at EU-US summit in Madrid on 3 December 1995.

European Union- United States of America Summit, 12 June 2008 - Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection of 12 June 2008, *Council doc. 9831/08*.

International Civil Aviation Organization Guidelines on Passenger Name Record (PNR) Data, *Doc 9944* of 2010.

National Bank of Belgium and the central banks co-operating in the oversight of SWIFT Memoranda of Understanding (MoU).

Opinion of the Article 29 Data Protection Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy, adopted on 13 April 2016.

Opinion of the Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

Opinion of the Article 29 Data Protection Working Party, WP 78, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data adopted 13 June 2003

Opinion of the Article 29 Data Protection Working Party, WP216, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014

Opinion of the Article 29 Data Protection Working Party,WP168, on the Future of Privacy-Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data. Adopted on 1 December 2009.

Opinion of the Article 29 WP, Opinion 6/2002 of 24 October 2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, *11647/02/EN WP 66*

Opinion of the European Data Protection Supervisor of 1 February 2007 on the role of the European Central Bank in the SWIFT case.

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU" of 9 December 2011

Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security. Brussels, 09.12.2011

Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II), *OJ 2010 C355/10*.

Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *Opinion 5/2015*.

Organisation for Economic Cooperation and Development *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980 and updated in 2013.

Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes — 'SWIFT', *OJ 2007 C 166/18*.

Recommendation of the Article 29 WP, Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights, *5143/99/EN WP26*.

United Nation High Commissioner for Human Rights Report on the right to privacy in the digital age of 30 June 2014, *A/HRC/27/37*.

United Nations Guidelines Concerning Computerized Personal Data Files.

United Nations Report of Special Rapporteur (United Nations, General Assembly) on the promotion and protection of human rights and fundamental freedoms while countering terrorism of 23 September 2014, *A/69/397*.

United States Department of Homeland Security Privacy Office Report on the use and transfer of passenger name records between the European Union and the united states of 26 June 2015. Retrieved 12.01.2017 from: https://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf

United States Department of Homeland Security Privacy Office Report on the use and transfer of passenger name records between the European Union and the United States." Retrieved 12.01.2017 from: https://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf

United States Department of Treasury, Testimony of Stuart Levey before the House Financial Services Subcommittee on Oversight and Investigations, Retrieved 10.01.2017 from Legal Document Centre for Compliance matters, www.swift.com.

United States Privacy Office of the Department of Homeland Security. Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union *(2008) 38*.

United States Terrorist Finance Tracking Program Redress Procedures for Seeking Access, Rectification, Erasure, or Blocking. Retrieved from: https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/Revised%20Redress%20Procedures%20for%20Web%20Posting%20(8-8-11).pdf

4. Online and print news articles

A Nation Challenged: Money Trail, U.S. makes Inroads in Isolating Funds of Terror Groups, retrieved 10.01.2017 from http://www.nytimes.com/2001/11/05/world/nation-challenged-money-trail-us-makes-inroads-isolating-funds-terror-groups.html

Bank Data Sifted in Secret by U.S. to Block Terror, published in New York Times 23 June 2006.

Clinton Presses European Parliament to Back Terror Data Deal, retrieved 10.01.2017 from: http://www.eubusiness.com/news-eu/us-attacks-banks.2l5.

Einigung in Brüssel. EU besiegelt umstrittenes Bankdaten-Abkommen, retrieved 10.01.2017 from http://www.spiegel.de/politik/ausland/0,1518,664264,00.html

EU-US PNR: Council to ignore Parliament and go ahead with "deal", retrieved 11.01.2017 from http://www.statewatch.org/news/2004/may/06eu-us-nr-deal.htm

Hacker dringen in Zahlungssystem Swift ein'. Retrieved 10.01.2017 from: http://www.spiegel.de/wirtschaft/service/swift-hacker-sind-zahlungssystem-eingedrungen-a-1089390.html

How US Customs bounced the European Commission into a quick decision, retrieved 11.01.17 from http://www.statewatch.org/news/2003/mar/02usdata2.htm

MEPs refer EU-Canada air passenger data deal to the EU Court of Justice, retrieved 12.01.2017 from: http://www.europarl.europa.eu/news/en/news-room/20141121IPR79818/MEPs-refer-EU-Canada-air-passenger-data-deal-to-the-EU-Court-of-Justice

Mass Surveillance, EU Citizens and The State'. Lecture delivered by MEP Claude Moraes at Annual Lecture of the Centre for Research Into Surveillance and Privacy (CRISP), 17 June 2014, London School of Economics & Political Science.

MEPs say 'no' to SWIFT, retrieved 10.01.2017 from http://www.euractiv.com/justice/meps-swift-news-258160

New Offer to Save EU-US Data Deal, retrieved 10.01.2017 from: http://www.politico.eu/article/new-offer-to-save-eu-us-data-deal/

Prime Minister Condemns SWIFT Data Transfers to U.S. as "Illegal", Retrieved from: http://www.privacyinternational.org/article.shtml.cmd[347]x-347-543789.

Surveillance judgment is a victory for democracy, retrieved 28.01.2017 from: http://www.independent.ie/opinion/analysis/surveillance-judgment-is-a-victory-for-democracy-30172786.html

Vom 'Europa der verschiedenen Geschwindigkeiten', retrieved 04.02.2017 from: http://www.tagesschau.de/ausland/eu-merkel-101.html

5. Bibliography

Achen, H.C. (2006) Institutional realism and bargaining models In: Thomson, R., Stokman, F.N., Achen, C.H. and König, T. (eds) *The European Union Decides*. Cambridge University Press.

Acosta, D. (2009). The good, the bad and the ugly in EU migration law: is the European Parliament becoming bad and ugly? *European Journal of Migration and Law*, vol. 11.

Alston, P. & Weiler, J.H.H. (1998) An Even Closer Union in Need of a Human Rights Policy, *European Journal of International Law*, vol. 9, pp. 658- 723.

Alter, K. (1998) Who are the 'Masters of the Treaty'? European governments and the European Court of Justice. *International Organization*, vol. 52 (1), pp. 121-47.

Alter, K. (2001) Establishing the Supremacy of European Law: The Making of an International Rule of Law in Europe. Oxford University Press.

Alter, K. (2009) The European Court's political power across time and space, *Revue Francaise de Science Politique*, vol. 59, pp. 1-24.

Amicelle, A. (2011) The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the "SWIFT Affair", *Research Questions No. 36, May 2011*, Centre d'études et de recherches internationales, SciencePo.

Anderson, D. & Eeckhout, P. (2011) Series Editors' Foreword. In: Peers, S. (2011). *Justice and Home Affairs Law*, OUP.

Anderson, D. & Murphy, C. (2011). The Charter of Fundamental Rights: History and Prospects in Post-Lisbon Europe. *EUI Working Paper LAW 2011/08*

Arendt, H. (1958). *The Human Condition*. University of Chicago Press.

Argomaniz, J. (2009) When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms. *Journal of European Integration*, vol. 31 (1), pp. 119-136.

Armstrong, K.A. (1998) Legal Integration: theorizing the legal dimension of European Integration, *Journal of Common Market Studies*, vol. 36 (2), pp. 155-74.

Balzacq, T. (2005). The Three Faces of Securitisation: Political Agency, Audience and Context, *European Journal of International Relations,* vol. 11 (2), pp. 171 -201.

Barros, X. (2012) The external dimension of EU counter-terrorism: the challenges of the European Parliament in front of the European Court of Justice, *European Security*, vol. 21 (4), pp. 518-536.

Beckman, J. (2015) *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*. Roudledge.

Bell, S. (2002) Institutionalism. In: Summers, J. (Ed.), *Government, Politics, Power And Policy In Australia*, Pearson Education Australia, pp. 363-380.

Bendel, P., Parkes, R. and Ette, A. (2011) *The Europeanisation of Control: Venues and Outcomes of EU Justice and Home Affairs Cooperation*. Lit Verlag.

Bendiek, A. (2006). Cross-pillar security regime building in the European Union: Effects of the European Security Strategy of December 2003. *European Integration Online Papers*

Bennett, C. (1992) *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press.

Bennett, C. & Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective.* MIT Press 2006.

Beyer, P. (2005). Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. *European Law Journal*, vol. 11 (3), pp. 365–375.

Bignami, F. (2006). Protecting Privacy Against the Police in the European Union: The Data Retention Directive. *GW Law School Law and Legal Theory Paper No. 2013-43.*

Bognetti, G. (2003) The Concept of Human Dignity in European and US Constitutionalism. In: Nolte, G. (ed.) *EU and US Constitutionalism*. Cambridge University Press.

Böhm, F. (2012) *Information Sharing and Data Protection in the Area of Freedom Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU level*. Springer.

Bradley, A. (2013) Introduction: The need for both national and international protection of human rights – the European challenge. In: Flogaitis, S; Zwart, T; and Fraser, J. (eds), *The European Court of Human Rights and its Discontents*. Edward Elgar.

Bretherton, C. & Vogler, J. (2006). *The European Union as a Global Actor*, Routledge

Brouwer, E. (2008) *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*. Martinus Nijhoff Publishers.

Brown, I. (2010). Data protection: the new technical and political environment. *Computers & Law*, vol. 21 (1).

Bulmer, Simon J. (1998) New institutionalism and the governance of the Single European Market, *Journal of European Public Policy*, vol. 5 (3), pp. 365 – 386.

Burley, A.M. and Mattli, W. (1993) Europe before the Court: a political theory of legal integration. *International Organization*, vol. 47 (1), pp. 41-76.

Buzan, B. et al. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers

Bygrave, L. A. (2014). *Data Privacy Law: An international Perspective*, Oxford University Press.

Bygrave, L.A. (2001). The Place of Privacy in Data Protection Law. *UNSW Law Journal*, vol. 24 (1), p. 277 – 283.

Campbell, J. (1995) Institutional Analysis and the Role of Ideas in Political Economy. *Paper at Harvard University.*

Cannataci, J. & Mifsud-Bonnici, J. (2005). Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty. *Information and Communications Technology Law*, vol. 14 (5).

Canon, B.C. (1983) Defining the Dimensions of Judicial Activism, Judicature, vol. 66 (6)

Carruba, C. J., Gabel, M. and Hankla, C. (2008). Judicial behavior under political constraints: evidence from the European Court of Justice. *The American Political Science Review,* vol. 102 (04), pp. 435-54.

Carruba, C. J., Gabel, M. and Hankla, C. (2012). Understanding the Role of the European Court of Justice in European Integration. *The American Political Science Review*, vol. 106 (1), pp. 214-223.

Christiansen, T., Jørgensen, K.E. and Wiener, A. (2001) *The Social Construction of Europe*. Sage Publications.

Colangelo, A. J. (2014). What Is Extraterritorial Jurisdiction? *Cornell Law Review,* vol. 99 (6).

Collier, D. and Collier, R. (1991) *Shaping the Political Arena*. Princeton University Press

Conant, L.J. (2002). *Justice Contained, Law and Politics in the European Union*, Cornell University Press.

Connorton, P. (2007). Tracking Terrorist Finance through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide. *Fordham Law Review*, vol. 76 (1), pp. 283-322.

Cook, K. S. and Levi, M. (1990). *The Limits of Rationality*. University of Chicago Press

Coppel, J. and O'Neill (1992) The European Court of Justice: Taking Rights Seriously? *Common Market Law Review*, vol. 29.

Costa, J.P. (2011) On the legitimacy of the European Court of Human Rights' judgments. *European Constitutional Law Review*, vol. 7.

Costello, C. (2006) The *Bosphorus* Ruling of the European Court of Human Rights: Fundamental Rights and Blurred Boundaries in Europe. *Human Rights Law Review,* vol. 6 (1)

Cowles, M.G. and Curtis, S. (2004) Developments in European Integration Theory: The EU as "Other". In Cowles, M.G. and Dinan, D. (eds) *Developments in the European Union*. Palgrave, pp. 296-309.

Cremona, M. (2006). External relations of the EU and the member states: Competence, mixed agreements, international responsibility, and effects of international law. *EUI Working Papers Law No. 2006/22*

Cremona, M. (2008) EU External Action in the JHA Domain: A Legal Perspective. *EUI Working Papers, LAW No. 2008/24.*

Cremona, M. (2011a). Coherence in European Union Foreign Relations law. In Koutrakos, P. (ed.). *European Foreign Policy: Legal and Political Perspectives*. Edward Elgar.

Cremona, M. (2011b). Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement. Institute for European Integration Research. *Working Paper No. 04/2011*, p. 19.

Cuijpers, C. (2007). A Private Law Approach to Privacy; Mandatory Law Obliged? SCRIPT-ed, vol. 4 (4), pp. 304 – 318.

Dawson, M., De Witte, B. and Muir, E. (2013) *Judicial Activism at the European Court of Justice*. Edward Elgar.

De Burca, G. (2011a) The Evolution of EU Human Rights Law. In Craig, P. and De Burca, G. (eds) *The Evolution of EU Law*. OUP.

De Burca, G. (2011b). The Road not taken: The European Union as a Global Human Rights Actor, *American Journal of International Law*, vol. 105.

De Búrca, G. (2013). After the EU Charter of Fundamental Rights: The Court of Justice as a human rights adjudicator. *Maastricht Journal of European and Comparative Law*, vol. 20 (2).

De Capitani, E. (2010) The Evolving Role of the European Parliament in AFSJ. In: Monar, J. (ed.). *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice*. College of Europe Studies, Peter Lang.

De Goede, M. (2012). *Speculative Security*. Minneapolis: University of Minnesota Press.

De Hert and Gutwirth, S. (2009) Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth, S. et al. (eds.) Reinventing Data Protection? Springer

De Hert, P & De Schutter, B. (2008). International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift. In Martenczuk, B. & Van Tiehl, S. (2008). *Justice, Liberty, Security. New Challenges for EU External Relations*. Brussels University Press.

De Hert, P. & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In Claes, E., Duff, A. & Gutwirth, S. (eds.) *Privacy and the criminal law*. Intersentia.

De Hert, P. & Papakonstantinou, V. (2009) The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for. *Computer Law & Security Review*, vol. 25 (5), pp. 403–414.

De Hert, P. and Papakonstantinou, V. (2015) Data Protection: The EU Institutions' Battle over Data Processing vs. Individual Rights'. In Trauner, F. and Ripoll Servent,

A. (eds) *Policy Change in the Area of Freedom, Security and Justice: How EU Institutions Matter*. Routledge.

De Hert, P., Papakonstantinou, V. and Riehle, C. (2008) Data protection in the third pillar: cautious pessimism. In: Maik, M. (ed.). *Crime, rights and the EU: The future of police and judicial cooperation*. Justice.

Delany, H. & Carolan, E. (2008) *The Right to Privacy – A Doctrinal and Comparative Analysis*. Thomson Round Hall

De Simone, C. (2010) Putting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive, *German Law Journal*, vol. 11.

De Vries, K. et al. (2011) The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)' In: Gutwirth, G. et al (eds) *Computer, Privacy and Data Protection: An Element of Choice*. Springer.

De Witte, B. (1991) *Community Law and National Constitutional Values.* Legal Issues of European Integration.

De Witte, B. (1999) 'The Past and Future Role of the European Court of Justice in the Protection of Human Rights' in Alston, P. (ed) *The EU and Human Rights*. OUP.

De Witte, B. (2008). Too Much Constitutional Law in the European Union's Foreign Relations? In: Cremona, M. and De Witte, B. (eds.) *EU Foreign Relations Law*. Hart Publishing.

DeLanda, M. (2006) *A New Philosophy of Society: Assemblage Theory and Social Complexity*. Continuum.

Deleuze, G., & Parnet, C. (2007) *Dialogues II*. Columbia University Press.

Douglas-Scott, S. (2011). The European Union and Human Rights After the Treaty of Lisbon. *Human Rights Law Review*, vol 11.

Downing, M. (1992) *The Military Revolution and Political Change: Origins of Democracy and Autocracy in Early Modern Europe*. Princeton, University Press.

Durica, J. (2013) Directive on the Retention of Data on Electronic Communication in the Rulings of the Constitutional Courts of EU Member States and Efforts for its Renewed Implementation. *The Lawyer Quarterly*, vol. 3(2).

Eckes, C. & Konstadinides, T. (eds.) (2011) *Crime within the Area of Freedom, Security and Justice*. Cambridge University Press.

Eeckhout, P. (2011*) EU External Relations L*aw. Oxford EU Law Library.

Elsig, M. (2002) *The EU's Common Commercial Policy: Institutions, Interests and Ideas*. Ashgate.

Epp, C.R. (1998) *The Rights Revolution: Lawyers, Activists, and Supreme Courts in Comparative Perspective*. University of Chicago Press.

Eriksson, J. & Rhinard, M. (2009) The Internal External Security Nexus: Notes on an Emerging Research Agenda *Cooperation and Conflict*, vol. 44 (3) pp. 243–267.

Fabbrini, F. (2015) The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court, *iCourts Working Paper Series*, no. 15.

Fabbrini, F. & Larik, J. (2016). The Past, Present, and Future of the Relation between the European Court of Human Rights. *Yearbook of European Law,* pp. 1-35.

Fahey, E. (2013). Law and Governance as Checks and Balances in Transatlantic Security: Rights, Redress and Remedies in EU-US Passenger Name Records and the Terrorist Finance Tracking Program. *Yearbook of European Law*, vol. 32 (1), pp. 368-388.

Fahey, E. (2015) Of One Shotters and Repeat-Hitters: A Retrospective on the Role of the European Parliament in the EU-US PNR Litigation. In Davies, B. and Nicola, F. (forthcoming) *EU Law Stories*, Cambridge University Press. Available at SSRN https://ssrn.com/abstract=2605793.

Farrell, H. and Heritier, A. (2003). Formal and Informal Institutions under Co-decsion: Continuous Constitution-Building in Europe. *Governance: An International Journal of Policy, Administration and Institutions*, vol. 16(4), p. 577-600.

Frederickson, H.G. (2006) Whatever Happened to Public Administration? Governance, Governance Everywhere. In: Ferlie, E., Lynn, L.E., and Pollitt, C. (eds) *Oxford Handbook of Public Management.* Oxford University Press.

Friedewald, M. et al. (2010). Privacy, data protection and emerging sciences and technologies: towards a common framework. *Innovation -The European Journal of Social Science Research,* vol. 23 (1).

Galetta, A. & De Hert, P. (2014) Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance. *Utrecht Law Review*. 10(1), pp.55–75.

Garland, D. (1996). The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society. *British Journal of Criminology*, vol. 36, pp. 445-71.

Gebhard, C. (2011). Coherence. In: Hill, C. & Smith, M. (eds.). *International Relations and the European Union*. Oxford University Press.

Gilmore, W. (2003). The Twin Towers and the Third Pillar: Some Security Agenda Developments. *EUI Working Paper LAW No. 2003/7*.

Gilmore, W. Fletcher, M., Lööf, R. & (2008). *EU Criminal Law and Justice.* Elgar European Law. Edward Elgar Publishing.

Gilmore, G. and Rijpma, J. (2007). Joined cases C-317/04 and C-318/04. *Common Market Law Review*, vol. 44 (4), pp. 1081-1099.

Goold, J. (2009) Surveillance and the Political Value of Privacy. *Amsterdam Law Forum*.

Gourevitch, P. (1986) *Politics In Hard Times*. Cornell University Press.

Greenleaf, G. (2012). Global data privacy in a networked world. In: Brown, I. (ed) *Research Handbook on Governance of the Internet*. Edward Elgar.

Granger, M. & Irion, K. (2014) The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection. *European Law Review,* vol. 39 (4), pp. 835-850.

Guild, E. & Carrera, S. (2014). The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive. *CEPS Paper in Liberty and Security* No. 65/May 2014.

Guiraudon, V. (2000) European Integration and Migration Policy: Vertical Policy Making as Venue Shopping, *Journal of Common Market Studies*, vol. 38 (2), pp. 241-271.

Haas, E. B. (1958) *The Uniting of Europe*. Stanford University Press. Reprinted 2004 by University of Notre Dame Press.

Haas, E.B. (1961). European Integration: The European and Universal Process, *International Organization*, vol. 4, pp. 607–46.

Haas, E.B (2001). Does Constructivism Subsume Neofunctionalism? In: Christiansen, T. et al. (eds) *The Social Construction of Europe*. Sage, pp. 22-31.

Habermas, J. (1989). The structural transformation of the public sphere. MIT Press.

Hall, P. A. & Taylor R. (1996) Political Science and the Three New Institutionalisms, *MPIFG Discussion Paper 96/6.*

Hall, P.A. (2007). Preference Formation as a Political Process: The Case of the Monetary Union in Europe. In: Katznelson, I. & Weingast, B. (eds). *Preferences and Situations: Points of Intersection between Historical and Rational Choice Institutionalism*. Sage Foundation.

Hartley, T. (1998) *The Foundations of European Community Law*. Oxford University Press.

Hatzis, N. (2005). Giving Privacy is Due: Private Activities of Public Figures in von Hannover v Germany. *The King's College Law Journal*, vol. 16 (1), pp. 143-157.

Hatzopoulos, V. (2008). With or without you...Judging politically in the area of freedom, security and justice", *European Law Review*, vol. 33 (1), pp. 44-65.

Hay, C. (2008) Constructivist institutionalism. In: Rockman, B, Rhodes, R. & Binder, S. (eds). *The Oxford Handbook of Political Institutions*, pp.56- 74. Oxford University Press.

Hayes, M. (2001). *The Limits of Policy Change: Incrementalism, World View and the Rule of Law.* Washington, Georgetown University Press.

Héritier, A. and Reh, C. (2009). Co-decision transformed: Informal Politics, Power Shifts and Institutional Change in the European Parliament. *Paper at UACES Conference on Exchanging Ideas on Europe*, 3-5 September.

Hijmans, H. (2006) The European data protection supervisor: The institutions of the EC controlled by an independent authority. *Common Market Law Review*, vol. 43.

Hijmans, H. (2016). *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU*. Springer.

Hijmans, H. & Scirocco, A. (2009) 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help?' *Common Market Law Review*, vol 46 (5), pp. 1485–1525.

Hillion, C. and Wessel, R.A. (2009) Competence Distribution in EU External Relations after ECOWAS: Clarification or Continued Fuzziness?' *Common Market Law Review*, vol. 46.

Hix, S., Kreppel, A. and Noury, A. (2003) 'The party system in the European Parliament: collusive or competitive?' *Journal of Common Market Studies,* vol. 41(3), pp. 309–31.

Hogan, J. (2006) Remoulding the Critical Junctures Approach. *Canadian Journal of Political Science*, vol. 39 (3), pp. 657-79.

Höpner, M. and Schäfer, A. (2012) Embeddedness and regional integration: waiting for Polanyi in a Hayekian setting, *International Organization*, vol. 66 (3), pp. 429-55.

Hörl, B., Warntjen, A. and Wonka, A. (2005). Built on quicksand? A decade of procedural spatial models on EU legislative decision-making. *Journal of European Public Policy, vol.* 12(3): pp. 592–606.

Huysmans, J. (2000) The European Union and the Securitization of Migration. *Journal of Common Market Studies*, vol. 38, pp. 751–777.

Jenson, J. (1989) Paradigms and Political Discourse: Protective Legislation in France and the United States Before 1914. *Canadian Journal of Political Science,* vol. 22 (2), pp. 235-258.

Jones, C & Hayes, B. (2013). The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy. IN: *SECILE – Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness*. A Project co-funded by the European Union within the 7th Framework Programme – SECURITY theme.

Katznelson, P. & Weingeist , B. (2005) *Preferences and Situations. Points of Intersection Between Historical and Rational Choice Institutionalism*. Russell Sage Foundation.

Kaunert, C. (2010), Towards supranational governance in EU counter-terrorism? - The role of the Commission and the Council Secretariat' , *Central European Journal of International & Security Studies*, vol. 4 (1) , pp. 8-31.

Kaunert, C., Léonard, S. & MacKenzie, A. (2012) The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT, *European Security*, vol. 21 (4), pp. 474-496.

Kingdon J. W. (1995) *Agendas, Alternatives and Public Policies*. London: Longman.

Kmiec, K. (2004) The Origin and Current Meanings of Judicial Activism. *California Law Review*, vol. 92.

Kohler-Koch, B. and Eising, R. (1999) *The Transformation of Governance in the European Union*, Routledge;

Konstadinides, T. (2014) Mass Surveillance and Data Protection in EU Law: The Data Retention Directive Saga. In: Bergström, M. and Jonsson Cornell, A. (eds.) *European Police and Criminal Law Co-Operation*. Hart Publishing, pp. 69 – 84.

Konstakopoulou, D. (2010) An Open and Secure Europe? Fixity and Fissures in the Area of Freedom, Security and Justice After Lisbon and Stockholm, *European Security*, vol. 19 (2), pp. 151-167.

Kosta, E. (2013) The Way to Luxembourg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection. *SCRIPT-ed*, vol. 10(3).

Kosta, E.. Coudert, F. & Dumortier, J. (2007) Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive, *International Review of Law, Computers & Technology*, vol. 21 (3), pp. 347-362.

Krasner, S. (1984) Approaches to the State: Alternative Conceptions and Historical Dynamics. *Comparative Politics*, vol. 16 (2), pp. 223–46.

Krasner, S. (1988) Sovereignty: An Institutional Perspective, *Comparative Political Studies,* vol. 21, pp. 66-94.

Krenn, C. (2015) 'Autonomy and Effectiveness as Common Concerns: A Path to ECHR Accession After Opinion 2/13, *German Law Journal*, vol. 16.

Kreppel, A. and Hix, S. (2003). From "grand coalition" to left–right confrontation: explaining the shifting structure of party competition in the European Parliament', *Comparative Political Studies,* vol. 36(1–2), pp. 75–96.

Krisch, N. (2010) *Beyond Constitutionalism*. Oxford University Press.

Krommendijk, J. (2015). The use of ECtHR case law by the CJEU after Lisbon: The View of the Luxembourg insiders. *Maastricht Faculty of Law Working Paper 2015/6*

Kuijper, J. (2008). The Opinion on the Lugano Convention and the Implied External Relations Powers of the European Community. In: Martenczuk and van Thiel (eds) *Justice, Liberty, Security: New Challenges for EU External Relations*. VUB Press.

Kuijper, P. J. (2014). The Case Law of the Court of Justice of the EU and the Allocation of External Relations Powers. Whither the Traditional Role of the Executive in EU Foreign Relations? In: Cremona, M. & Thies, A. (eds.). *The European Court of Justice and External Relations Law. Constitutional Challenges*. Hart Publishing.

Labayle, M. (2013). The New Commission's Role in Freedom, Security and Justice in the Post-Lisbon Context. New Era or Missed Opportunity? In: Chang, M. & Monar, J. (eds.) *The European Commission in the Post-Lisbon Era of Crises.* College of Europe Studies No.16

Larsson, O. and Naurin, D. (2016). Judicial independence and political uncertainty: How the risk of override impacts on the Court of Justice of the EU. *International Organization*, vol. 70 (2), pp. 377-408.

Lavenex, S. (2004) EU external governance in 'wider Europe'. *Journal of European Public Policy*, vol. 11(4), pp. 680-700.

Lavranos, N. (2008). Towards a Solange-Method between International Courts and Tribunals? In: Broude, T. & Shany, Y. (eds.) *The shifting Allocation of Authority in International Law: Considering Souvereignty, Supremacy and Substiarity*. Hart Publishing.

Lewis, J. (2005) The Janus face of Brussels: socialization and everyday decision making in the European union, *International Organization*, vol. 59 (4), pp. 937–72.

Lindblom, C. (1959). The Science of Muddling Through. *Public Administration Review*, vo. 19 (2), pp. 79-88.

Loughlin, M. (2010). What is Constitutionalisation? In: Dobner, P. and Loughlin. M. (eds.) *The Twilight of Constitutionalism?* Oxford University Press, pp. 47-72.

Ludlow, N. P. (2006) De-commissioning the empty chair crisis: The community institutions and the crisis of 1965-6. In: Wallace, H., Winand, P. and Palayret, J.M., (eds.) *Visions, Votes and Vetoes: the Empty Chair Crisis and the Luxembourg Compromise Forty Years On*. Peter Lang.

Lynsky, O. (2015) *The Foundations of EU Data Protection Law*. Oxford University Press.

MacKenzie, A. (2011). A US Driven Security Agenda? EU Actorness in Counter-Terrorism Co-operation with the US. Paper presented at *EUSA Twelfth Biennial International Conference Boston*, *Massachusetts*.

Mahoney, J. & Thelen, K. (2010) A Theory of Gradual Institutional Change. In: Mahoney, J. & Thelen, K. (eds.) *Explaining Institutional Change: Ambiguity, Agency, and Power*. Cambridge University Press.

Manners, I. (2002) Normative Power Europe: A Contradiction in Terms? *Journal of Common Market Studies*, vol. 40, pp. 235–258.

Manners, I. (2006). Normative power Europe reconsidered: beyond the crossroads. *Journal of European Public Polic*y, vol. 13(2), pp. 182–99.

Mansbridge, J. (1990). *Beyond Self-Interest*. University of Chicago Press.

Maras, M. (2011). While the European Union was Sleeping, the Data Retention Directive Was Passed: The Political Consequences of Mandatory Data Retention. *Hamburg Review of Social Sciences*, vol. 6 (1), pp. 1-30.

March, J. & Olsen, J. (1984) The New Institutionalism: Organizational Factors in Political Life. *The American Political Science Review*, vol. 78 (3), pp. 734-749.

March, J.G. and Olsen, J. (1998). The Institutional Dynamics of International Political Orders. *International Organizations*, vol. 52 (4), pp. 943-969.

Marin, L. and Spena, A. (2016) Introduction: The Criminalization of Migration and European Dis(Integration), *European Journal of Migration and Law,* vol. 18 (2), pp. 147-156.

Martenczuk, B. (2008) Visa Policy and EU External Relations. In: Martenczuk and van Thiel (eds) *Justice, Liberty, Security: New Challenges for EU External Relations*. VUB Press.

Martinsen, D. (2015) An Ever More Powerful Court? The Political Constraints of Legal Integration in the European Union, Oxford Scholarship Online

McCann, M. (1994) *Rights at Work: Pay Equity, Reform and the Politics of Legal Mobilization*, University of Chicago Press.

McCullagh, K. (2009). Protecting 'privacy' through control of 'personal' data processing: A flawed approach. *International Review of Law, Computers and Technology*, vol. 23 (1-2), p. 47–58.

McHarg, A. (1999). Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights. *The Modern Law Review*, vol. 62(5), pp. 671-696.

Milward, A.S. (2000) *The European Rescue of the Nation-State*. Routledge

Milward, A.S. & Lynch, F. M. B. (1993) *The Frontiers of National Sovereignty: History and Theory 1945–1992*. Routledge

Missiroli, A. (2001). European Security Policy: The Challenge of Coherence. *European Foreign Affairs Review*, vol. 6 (2), pp. 177-96.

Mitsilegas, V. (2003) The New EU-US Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data. *European Foreign Affairs Review*, vol. 8, pp. 151-36.

Mitsilegas, V. (2009) *EU Criminal Law.* Hart Publishing.

Mitsilegas, V. (2014). Transatlantic counterterrorism cooperation and European Values. The elusive quest for coherence. In: Curtin, D. & Fahey, E. (eds.). *A Transatlantic Community of Law Legal Perspectives on the Relationship between the EU and US Legal Orders*. Cambridge University Press.

Mitsilegas, V. (2015). The Transformation of Privacy in an Era of Pre-emptive Surveillance. *Tilburg Law Review*, vol 20 (2015), pp. 35-57.

Mitsilegas, V. (2016) EU Criminal Law after Lisbon. Rights, Trust and The Transformation of Justice in Europe. Hart Publishing.

Monar, J. (2006) Cooperation in the Justice and Home Affairs Domain: Characteristics, Constraints and Progress, *Journal of European Integration*, vol. 28 (5), pp. 495-509.

Monar, J. (2010). The Institutional Dimension of the AFSJ. In Monar, J. (ed.). *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice*. College of Europe Studies, Peter Lang.

Monar, J. (2010a). The Institutional Framework of AFSJ – Specific Challenges and Dynamics of Change. In: Monar, J. (ed.). *The Institutional Dimension of the European Union's Area of Freedom Security and Justice.* College of Europe Studies, No. 11.

Monar., J. (2010b). Editorial Comment. The Rejection of the EU–US SWIFT Interim Agreement by the European Parliament: A Historic Vote and Its Implications. *European Foreign Affairs Review*, vol. 15.

Moore, G. (1965) Cramming more components onto integrated circuits. *Electronics Magazine*, vol. 38 (8).

Moravcsik, A. (1993) Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach. *Journal of Common Market Studies*, vol. 31, pp. 473–524.

Moravcsik, A. (1998), *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht.* Cornell University Press.

Moravcsik, A. & Schimmelfennig, F. (2009). Liberal Intergovernmentalism. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. Oxford University Press.

Muir, E. (2013). The Court of Justice: a fundamental rights institution among others. In: Dawson, M., De Witte, B. and Muir, E. (eds.) Judicial Activism at the European Court of Justice. Edward Elgar.

Murphy, C. (2010) Romanian Constitutional Court, Decision No. 1258 of 8 October 2009, *Common Market Law Review*, vol. 47, pp. 933 – 941.

Niemann, A. & Schmitter, P. (2009). Neofunctionalism. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. Oxford University Press

North, D. (1990) *Institutions, Institutional Change and Economic Performance.* Cambridge University Press.

Nowak, T. (2010). Of garbage cans and rulings: judgments of the European Court of Justice in the EU legislative process, *West European Politics*, vol. 33(4), pp. 753-69.

O'Neill, M. (2010) The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar, *Journal of Contemporary European Research*, vol 6 (2), pp. 211 – 235.

Ostrom, E. (1990). *Governing the Commons*. Cambridge University Press.

Papakonstantinou, V. & De Hert, P. (2009). The PNR Agreement and Transatlantic Anti-Terrorism Co-operation: No Firm Human Rights Framework on either Side of the Atlantic. *Common Market Law Review*, vol. 46 (1), pp. 885-919.

Pawlak, P. (2009a) *Made in the USA? The Influence of the US on the EU's Data Protection Regime.* Centre of European Policy Studies, Liberty and Security in Europe, Justice and Home Affairs section.

Pawlak, P. (2009b) Network Politics in Transatlantic Homeland Security Cooperation, *Perspectives on European Politics and Society*, vol. 10 (4), pp. 560-581.

Peers, S. (2011) Mission Accomplished? EU Justice And Home Affairs Law after the Treaty of Lisbon. *Common Market Law Review* vol. 48, pp. 661–693.

Peers, S. (2012) EU *Justice and Home Affairs Law*. Oxford University Press.

Peers, S. et al (2014) *The EU Charter of Fundamental Rights: A Commentary*. Hart Publishing.

Peters, G & Pierre, J. (2009). Governance Approaches. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. Oxford University Press.

Peters, G. (2000) Governance and comparative politics. In: Pierre, J. (ed.), *Debating Governance*, Oxford University Press, pp. 36–53.

Peterson, J. & Shackleton, M. (2012). The EU's institutions: an overview. In: Peterson, J. & Shackleton, M. (eds.) *The institutions of the European Union*. Oxford University Press, pp. 1-19.

Peterson, J. and Bamberg, E. (1999) *Decision-making in the European Union*. Palgrave.

Peterson, P. (2009). Policy Networks. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. OUP.

Pfisterer, V. (2010). The Second SWIFT Agreement between the European Union and the United States of America – An Overview. *German Law Journal*, vol. 11, pp.1173-1190.

Pierson, P. (1994) *Dismantling the Welfare State?* Cambridge University Press.

Pierson, P. (2000) Increasing Returns, Path Dependence and the Study of Politics. *The American Political Science Review*, vol. 94 (2), pp. 251-267.

Pollack, M. (2014) Theorising EU Policy-Making. In: Wallace, H., Wallace, W. & Pollack, M. (2014). Policy-making in the European Union. Seventh Edition. OUP

Pollack, M. A. (2009). The New lnstitutionalisms and European Integration. In: Wiener, A. & Diez, T. (eds.). *European Integration Theory*. OUP.

Pollack, M.A. (2003) The Engines of European Integration, Delegation, Agency and Agenda Setting in the EU. Oxford University Press.

Poullet, Y. (2009) Data Protection Legislation: What is at Stake for Our Society and for Democracy, *Computer Law and Society Review*, vol. 25.

Ramsey, M. (2014). A Return Flight for Due Process? An Argument for Judicial Oversight of the No-Fly List. Retrieved 12.01.2017 from http://dx.doi.org/10.2139/ssrn.2414659

Rasmussen, A. (2008). Time Choices in bicameral bargaining: Evidence from the Co-Decision Legislative Procedure of the European Union. *Paper at 4th Pan-European Conference on EU Politics,* Riga.

Rasmussen, M. (2013) Rewriting the history of European public law: the new contribution of historians. *American University International Law Review*, vol. 28 (5), pp. 1187-223.

Rauhofer, J. (2006) Just because you're paranoid, doesn't mean they're not after you: Legislative developments in relation to the mandatory retention of communications data in the European Union. *SCRIPT-ED*, vol. 3 (4).

Rees, W. and Aldrich, R. (2005). Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence? *International Affairs*, vol. 81 (5), pp. 390-406.

Reh, C. et al. (2011) The Informal Politics of Legislation: Explaining Secluded Decision Making in the European Union, *Comparative Political Studies*, vol. 46 (9).

Reh. C., Héritier, A., Bressanelli, E., & Koop, C. (2005) The Informal Politics of Legislation: Explaining Secluded Decision-Making in the European Union. *Paper at the APSA Annual Convention, 2-5 September*, Washington.

Reyners, J. (2015). Is there a fourth institutionalism? Ideas, Institutions, and the Explanation of Policy Change. In: Hogan, J. & Howlett, M. (eds.) *Policy Paradigms in Theory and Practice Discourses, Ideas and Anomalies in Public Policy Dynamics*. Palgrave.

Richards, A. (2014) Conceptualizing Terrorism. Studies in *Conflict & Terrorism*, vol. 37 (3).

Rieker, P. (2006). *Europeanization of National Security Identity: The EU and the Changing Security Identities of the Nordic States*. Routledge.

Ripoll Servent, A. (2006). Setting priorities: functional and substantive dimensions of irregular immigration and data protection under co-decision. *Journal of Contemporary European Research*, vol. 5 (2), pp. 225-242.

Ripoll Servent, A. (2013) Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision. *Journal of European Public Policy*, vol. 20(7).

Risse, T. (2009). Social Constructivism and European Integration. In: Wiener, A. & Diez, T. (eds.) *European Integration Theory*. OUP

Rosas, A. (2007) The European Court of Justice in Context: Forms and Patterns of Judicial Dialogue. *European Journal of Legal Studies*, vol. 1.

Rosenbach, M. and Stark, H. (2015). *Der NSA Komplex. Edward Snowden und der Weg in die totale Überwachung*, Spiegel Buchverlag.

Rosenberg, G.N. (2008) The Hollow Hope: Can Courts Bring About Social Change?, University of Chicago Press.

Rouvoy, A. & Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth, S. et al. (eds.) Reinventing Data Protection? Springer

Ruiter, R. & Neuhold, C. (2012). Why is Fast Track the Way to Go? Justifications for Early Agreement in the Co-Decision Procedure and Their Effects. *European Law Journal*, vol. 18 (4), pp. 536-554.

Ryngaert, C. (2015). *Jurisdiction in International Law*. Oxford Scholarly Authorities on International Law.

Sandholtz, W. (1993) Choosing Union: Monetary Politics and Maastricht. *International Organization*, vol. 47 (1), pp. 1-39.

Santolli, J. (2008). Note: The Terrorism Financing Tracking Program: Illuminating the Shortcomings of The European Union's Antiquated Data Privacy Directive. *The George Washington International Law Review*, vol. 40, pp. 553-582.

Santos Vara, J. (2013). The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon. *Centre for the Law of EU External Relations (CLEER) Working Papers 2013/2*, pp. 1-31.

Scherb, K. (1996). Comment, Administrative Subpoenas for Private Financial Records: What Protection for Privacy Does the Fourth Amendment Afford? *Wis. L. Rev*, vol. 1075, pp. 1076-85.

Schieffer, M. (2008) Readmission and Repatriation of Illegal Residents. In: Martenczuk and van Thiel (eds) *Justice, Liberty, Security: New Challenges for EU External Relations*. VUB Press.

Schimmelfennig, F. (2007). Competition and Community: Constitutional Courts, Rethorical Action, and the Institutionalization of Human Rights in the European Union. In: Rittberger, B. & Schimmelfennig, F. (eds.). *The Constitutionalisation of the European Union*. Routledge.

Schimmelfennig, F. and Sedelmeier,U. (2004) Governance by Conditionality: EU Rule Transfer to the Candidate Countries of Central and Eastern Europe, *Journal of European Public Policy*, vol. 11 (4), pp. 669–687.

Schmidt, V. A. (2008): Discursive Institutionalism: The Explanatory Power of Ideas and Discourse. *Annual Review of Political Science*, vol. 11, pp. 303-36.

Servent, A. (2014) The Role of the European Parliament in international negotiations after Lisbon. *Journal of European Public Policy*, vol. 21 (4), pp. 568-586.

Servent, A. & MacKenzie, A. (2012). The European Parliament as a 'NormTaker'? EU-US Relations after the SWIFT Agreement. *European Foreign Affairs Review*, vol. 17, pp. 71–86.

Servent, A. & MacKenzie, Al (2011). Is the EP Still a Data Protection Champion? The Case of SWIFT. *Perspectives on European Politics and Society*, vol. 12 (4), pp. 390-406.

Shapiro, M. (2002). Judicial Jurisprudence. In: Shapiro, M. & Stone Sweet, A. (2002). *On Law, Politics & Judicialization*. Oxford University Press

Shea, C. (2008). A Need for Swift Change: The Struggles between the European Union's Desire for Privacy in International Financial Transactions and the United States' Need for Security from Terrorists as evidenced by the SWIFT Scandal. *Journal of High Technology Law*, vol. 8 (1), pp. 143-168.

Shepsle, K. &Weingast, B. (1987) The Institutional Foundations of Committee Power, *American Political Science Review,* vol. 81 pp. 85–104.

Simitis, S. (2009) Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung. *Neue Juristische Wochenzeitschrift 25*, pp. 1782-1786

Sion-Tzidkiyahu, M. (2008) Opt-Outs in the Lisbon treaty: What direction for Europe à la Carte. *European Journal of Law Reform*, vol.10 (4).

Skocpol, T. (1979) *States and Social Revolutions*. Cambridge University Press.

Smith, H. (2002) *European Union Foreign Policy: What it is and what it does*. Pluto Press.

Smith, K. (2003). *European Union foreign policy in a changing world*. Cambridge: Polity Press.

Smith, K. (2009) The Justice and Home Affairs Policy Universe: Some Directions for Further Research', *Journal of European Integration,* vol. 31 (1), pp. 1–7.

Smith, M. E. (2004). *Europe's Foreign and Security Policy: The institutionalisation of cooperation*, Cambridge University Press.

Solingen, E. and Ozyurt, S. (2006). 'Mare Nostrum? The Sources, Logic, and Dilemmas of the Euro-Mediterranean Partnership'. In: Adler, E. et al. (eds) *The Convergence of Civilizations: Constructing a Mediterranean Region. Toronto*. University of Toronto Press.

Solove, D. (2004) *The Digital Person: Technology and Privacy in the Information Age*. New York University Press.

Solove, D. (2008). *Understanding Privacy*. Harvard University Press.

Stetter, S. (2004). Cross-pillar politics: functional unity and institutional fragmentation of EU foreign policies. *Journal of European Public Policy,* vo.11 (4), pp. 720–39.

Stone Sweet, A. (1998) Constitutional Dialogues in the European Community. In: Slaughter, A. Stone Sweet, A. & Weiler, J. (eds.) *European Courts and National Courts*. Hart Publishing.

Stone Sweet, A. (2000) *Governing with Judges: Constitutional Politics in Europe*, Oxford University Press.

Stone Sweet, A. (2003) European Integration and the Legal System. In: Börzel, T. and Cichowski, R.A. (eds.) *The State of the European Union: Law, Politics, and Society*. Oxford University Press.

Stone Sweet, A. and Brunell, T. (2012). The European Court of Justice, state noncompliance, and the politics of override. *American Political Science Review,* vol. 106 (1), pp. 204-13.

Storgaard, L. H. (2015) Composing Europe's Fundamental Rights Area: A Case for Discursive Pluralism. *Cambridge Yearbook of European Legal Studies*, vol. 17.

Streeck, W. & Thelen, K. (2005) Introduction: Institutional Change in Advanced Political Economies. In: Streeck, W. & Thelen, K. (eds.) *Institutional Change in Advanced Political Economies*. Oxford University Press.

Sweet Stone, A. (2002) Path Dependence, Precedent, and Judicial Power. In: Stone Sweet, A. & Shapiro, M. (eds.). *On Law, Politics, & Judicialization*, Oxford University Press.

Szyszczak, E. (2006) Experimental Governance: The Open Method of Coordination. *European Law Journal*, vol. 12 (4), pp. 486–502.

Thelen, K. and Steinmo, S. (1992). Historical Institutionalism in Comparative Politics. In: Steinmo et al. (eds). *Structuring Politics*, p. 2.

Tiefenbrun, S. (2002) A Semiotic Approach to a Legal Definition of Terrorism. *ILSA Journal of International & Comparative Law*, vol. 9, p. 357.

Trauner, F. (2005). *External aspects of internal security: A research agenda*. EU-Consent Project.

Trauner, F. & Carrapico, H. (2012) The External Dimension of EU Justice and Home Affairs after the Lisbon Treaty: Analysing the Dynamics of Expansion and Diversification'. *European Foreign Affairs Review*, vol.17, Special Issue, pp. 1–18.

Trauner, F. & Ripoll Servent, A. (2016) The Communitarization of the Area of Freedom, Security and Justice: Why Institutional Change does not Translate into Policy Change. *Journal of Common Market Studies*, pp. 1–16.

Tsebelis et al. (2001) Legislative procedures in the European Union: An empirical analysis. *British Journal of Political Science*, vol. 31, pp. 573–99.

Tsebelis, G. (1990). *Nested Games: Rational Choice in Comparative Politics*. University of California Press.

Tsebelis G. (1994) The power of the European Parliament as a conditional agenda setter. *American Political Science Review*, vol. 88, pp. 129–42;

Tzanou M. (2013) Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, vol. 3(2), pp. 88-99.

Uçarer, E. M. (2013) Area of Freedom, Security, and Justice. In: Cini, M. & Perez-Solorzano Barragán, N. (eds.) *European Union Politics*. Oxford University Press.

Van Alsenoy B. and Koekkoek M. (2015) Extra-Territorial Reach of the EU's Right to Be Forgotten. *ICRI Research Paper 20.*

Van Elsuwege, P. (2014). The Potential for Inter-Institutional Conflicts before the Court of Justice: Impact of the Lisbon Treaty. In: Cremona, M. & Thies, A. (eds.). *The European Court of Justice and External Relations Law*. Hart Publishing.

Vanhoonacker, S. (2011) The Institutional Framework. In: Hill, C & Smith, M. (eds.) *International Relations and the European Union*. Oxford University Press, pp. 76-100.

Warren, S. & Brandeis, L, (1890). The Right to Privacy, *Harvard Law Review* vol. 4(5).

Whitman, J. (2002). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal*, vol. 113.

W. R. (1994) Institutions and Organizations: Towards a Theoretical Synthesis. In: Scott, W.R. & Meyer, J. et al. (1994) *Institutional Environments and Organizations: Structural Complexity and Individualism*, Sage, pp. 55–80.

Wacks, R. (2000). *Law, Morality, and the Private Domain*. Hong Kong University Press.

Wæver, O. (1995) Identity, Integration and Security: Solving the Sovereignty Puzzle in EU Studies. *Journal of International Affairs*, vol. 48 (2), pp. 46-86.

Walden, I. (2011) Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. Queen Mary School of Law Legal Research Paper, No. 74/2011. Retrieved 25.05.2016 from: http://ssrn.com/abstract=1781067.

Walden, I. (2015) The right to privacy and its future. Retrieved 26.04.16 from: https://issuu.com/vpmarketing/docs/synergy_57_online_5e0911c1a89c2a

Walker, N. (2004) *Europe's Area of Freedom, Security and Justice*. Oxford University Press.

Walker, N. (2011) In Search of the Area of Freedom, Security and Justice: A Constitutional Odyssey. In: Walker, N. (ed.) *Europe's Area of Freedom Security and Justice*. Academy of European Law/European University Institute.

Weiler, J. (1991) The Transformation of Europe, *Yale Law Journal*, 100, pp. 2403-83.

Weiler, J. (2001) The Transformation of Europe. *Yale Law Journal,* vol. 100 (8), pp. 2403-2483.

Weingast, B. and Marshall, W. (1988) The Industrial Organization of Congress, *Journal of Political Economy*, vol. 96 (1), pp. 132–163.

Weir, M. and Skocpol, T. (1985) State Structures and the Possibilities for 'Keynesian' Responses to the Great Depression in Sweden, Britain and the United States. In Evans, P. et al. (eds.) *Bringing the State Back In*. Cambridge University Press, pp. 107–163.

Wessel, R. A. (2010) Cross-Pillar Mixity: Combining Competences in the Conclusion of EU International Agreements. In: Hillion, C. and Koutrakos, P. (eds.) *Mixed Agreements in EU Law Revisited*. Hart Publishing.

Wessel, R., Marin, L. & Matera, C. (2011). The External Dimension of the EU's Area of Freedom, Security and Justice. In: Eckes, C & Konstadinidis, T. (eds.) *Crime within the Area of Freedom, Security and Justice*. Cambridge University Press.

Wiener, A. & Diez, T. (2009) Introducing the Mosaic of Integration Theory. In: Wiener, A. & Diez, T. (eds.) *European Integration Theory*. OUP.

Wittgenstein, L. (1958). *Philosophical Investigations*, paras. 66-67. G.E.M. Anscombe trans.

Wolff, N. & Mounier, G. (2009) The External Dimension of Justice and Home Affairs: A Different Security Agenda for the EU? *Journal of European Integration*, Vol. 31 (1), pp. 9-23.

Wolff, S. (2012) *The Mediterranean Dimension of EU Internal Security*. Palgrave.

Wolff, S., Goudappel, F. and De Zwaan, J. W. (2011) *Freedom, Security and Justice After Lisbon and Stockholm*. T.M.C. Asser Press.