Department of Law

The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement

Maria Tzanou

Thesis submitted for assessment with a view to obtaining the degree of
Doctor of Laws of the European University Institute

Florence, March 2012

EUROPEAN UNIVERSITY INSTITUTE
Department of Law

The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement

Maria Tzanou

Thesis submitted for assessment with a view to obtaining the degree of
Doctor of Laws of the European University Institute

Examining Board:

Professor Martin Scheinin, European University Institute (EUI Supervisor)
Professor Valsamis Mitsilegas, Queen Mary University of London
Professor Tuomas Ojanen, University of Helsinki
Professor Giovanni Sartor, European University Institute

Summary

This thesis examines the added value of the fundamental right to data protection within the EU legal order when law enforcement measures are at stake. It provides a comprehensive analysis of the concept of data protection, its underlying values and aims, and the approaches to this right. It discusses the current theories and the existing case-law on data protection by identifying their shortcomings. It introduces a new theory on data protection that reconstructs the right and reshapes in a clear and comprehensive manner its understanding.

The thesis tests the added value of the 'reconstructed' right to data protection in the most difficult context: law enforcement and counter-terrorism. Three specific case-studies of data processing in the field of law enforcement are used: 1) the information collection; 2) the information storage; and, 3) the information transfer case. The information collection case discusses the EU Data Retention Directive and addresses the conceptual confusions between the rights to privacy and data protection that surround it, before turning to a substantive fundamental rights assessment of the Directive. The information storage case examines the added value of the fundamental right to data protection in the context of the access of law enforcement authorities to information stored on EU-scale databases such as the second generation Schengen Information System (SIS II), the Visa Information System (VIS) and Eurodac. Finally, the information transfer case discusses the role of the rights to privacy and data protection with regard to the transfer of data from the EU to the US for counter-terrorism purposes. In this context, it addresses the EU-US PNR and TFTP cases.

Contents

Acknowledgements

In my third year of Law at the University of Athens, on the third floor of the University's libraries at Ippokratou's 45, I saw a poster of the European University Institute in Florence. It was old and full of dust, but it made an impression on me. That same evening, after a search on the Internet, I decided to write my PhD thesis at this very place. The how and when was not clear to me, but the decision was taken. Three years later, I was there. The amazing journey had started.

Writing a PhD is very much of a lonely exercise. For the most part, I have thought, worked and written this thesis alone in my room. Yet, it would have been impossible to complete it without these people that have been around me all these four years of solitude. They all have contributed in different ways to this project and I am very much indebted to them.

First, I would like to thank my PhD supervisor Martin Scheinin. I am deeply grateful for his generous support and comments throughout all these years, but above all I am grateful for introducing me to the magic world that has become the topic of this thesis, data protection! I still remember the first report I wrote on data protection, without ever imagining that I would go any further on the issue, and then the discussions we had for almost a year that this should be the subject of my doctoral research. In the end, I did become a 'privacy freak' and that's all thanks to Martin's silent but strong persistence on the issue.

I would further like to thank Marise Cremona, Takis Tridimas and Bruno de Witte for their helpful advice and suggestions that have inspired the writing of this thesis. I am also very grateful to my PhD examiners Tuomas Ojanen, Valsamis Mitsilegas, and Giovanni Sartor that have contributed with their insightful comments to the final version of the research.

I would not have been in position to write a PhD without the funding of IKY, which has also been generous in previous times of my studies, and the European University Institute. I am very thankful to Linda Gilbert for her invaluable help to secure the research grant for my fellowship at NYU and for the funding of my teaching experience in Utrecht. I will never forget our long conversations in her office, Linda has always been one of the most supporting persons I met at the EUI.

Concerning my big step to NYU, I will never forget the help of Lucas Lixinski that showed me how to overcome all the difficulties and above all my personal anxieties. I am also very grateful to Annick Bulckaen that has helped me through numerous administrative questions with kindness and patience and has organised everything until the last moment of the defence of this thesis. Finally, I would like to thank Machteld Nijsten for ordering all the books I asked in my last year of the PhD.

My four months in New York have been an important part of my PhD journey and the people I met there have influenced this work. Professor's Joseph Weiler's four-hour seminar on how to write a PhD really changed my life. It was the starting point to change the focus of my research. I am also indebted to Sam Rascoff for allowing me to attend his course on Intelligence, Counter-Terrorism and the Law at NYU and for providing me with invaluable comments when I presented for the first time my changed research topic at the NYU JSD Forum. Finally, I am very thankful to all the participants of the NYU JSD Forum for their enthusiastic remarks and helpful suggestions at a point that I needed them the most.

Florence is an amazing place to write a PhD. For me, Florence has always been home and I will remember it like that. Great friends, such as Laura and Janine have contributed to making my living in Florence so memorable. Laura has been an amazing flatmate and I have always enjoyed our incredibly long discussions. Janine with her beautiful smile is by far the nicest and kindest person I met at the EUI. She would always make my day when I saw her. My friends from back home have also been there for me. Dimitris that made sure I arrived well in Florence by singing to me all the way through the ferry trip, Vassilis with his shocking questions about my future, and Theodora with her incredible sense of humour.

I am indebted to my family for the abundant support that they had given me throughout all these years. I would especially like to thank my brother, Giannis, who, with Dora, has been there for me every single day, ready to hear my problems, but also to make me laugh. I miss him very much but when we manage to be together, it is explosive as always.

Raúl has been the most amazing part of my PhD journey. It is impossible to thank him enough for all he has done for me. He believed in me, he supported me through every moment, he helped me with every possible small or big question on my thesis. From how to put the footnotes and handle thousands of problems with Word, to our extremely stimulating conversations on how I should proceed with substantive

issues, it was always Raúl. It was because of him that I realised what I wanted to do with my research after quite some years of insecurities. It was because of him that I managed to go through anxieties and stress, chicken poxes, minor problems that looked huge and big problems that looked impossible. You are there, always calm, patient, smiling, encouraging, loving, supporting... I am thankful for every moment with you... Te quiero.

My greatest thanks go to my parents, Christos and Foteini, for being the ones behind not only every step of my PhD but also every step of my life. I never thanked them enough for all they have done for me, for all the incredible support they have given me. Without them it would have been impossible. This work is dedicated to them as the smallest sign of my gratitude.

Introduction

"Καὶ μὴν καὶ τῶν πόνων πλείστας ἀναπαύλας τῇ γνώμῃ ἐπορισάμεθα, ἀγῶσι μέν γε καὶ θυσίαις διετησίοις νομίζοντες, ἰδίαις δὲ κατασκευαῖς εὐπρεπέσιν, ὧν καθ'ήμέραν ἡ τέρψις τὸ λυπηρὸν ἐκπλήσσει."[1]

1.1 Subject Matter and Aims

The entry into force of the Lisbon Treaty on December 1, 2009 marked a historic moment for data protection: the right was elevated to the status of a fundamental right within the EU legal order, alongside the right to privacy. This thesis has a specific purpose: it seeks to examine the added value of data protection as a fundamental right in the context of law enforcement.

Data protection is understood, normally, as referring to a set of rules that aim to protect the rights, freedoms and interests of individuals, when information related to them ('personal data') is being processed (collected, stored, exchanged, altered, deleted). Data protection has always been linked to privacy, in such a way that it is very difficult in certain circumstances to assess its very concept, its purposes and its underlying values without referring to privacy.

A large body of laws pertains already to data protection, however there are numerous uncertainties concerning the right's capabilities to resolve problems and provide for an effective protection. In this respect, this research project investigates how data protection can operate as a fully-fledged fundamental right next to the right to privacy. It attempts to bring clarity on the concept of data protection, its underlying values and aims, and the approaches to this right. It discusses the current theories and the existing case-law on data protection by identifying their shortcomings. It elaborates a new theory on data protection that reshapes in a clear and comprehensive manner the understanding of the right, and can guide courts and legislators on data protection issues in the field of law enforcement.

Having introduced a new theory on data protection, the thesis goes on to test the added value of the right in the most difficult context: law enforcement and

[1] Thoukidides, Pericle's Epitaph speech, para 38. "Further, we provide plenty of means for the mind to refresh itself from business. We celebrate games and sacrifices all the year round, and the elegance of our private establishments forms a daily source of pleasure and helps to banish the spleen."

counter-terrorism.[2] Three specific case-studies of data processing in the field of law enforcement are used: 1) the information collection; 2) the information storage; and, 3) the information transfer case. The analysis will focus on four specific EU counter-terrorism measures: the Data Retention Directive (the information collection case), the exchange of information through three EU large-scale databases the second generation Schengen Information System (SIS II), the Visa Information System (VIS), and EURODAC (the information storage case), and, the EU-US PNR and TFTP Agreements (the information transfer case). This does not mean that each of the counter-terrorism measures discussed involves necessarily one category or type of processing. On the contrary, processing of personal data is a very broad term that refers to any operation carried out on the data (from collection, storage, processing, alteration, exchange, transfer, to erasure, deletion, etc). In this respect, all the above measures involve different types of processing. For instance, the Data Retention Directive may be discussed for the purposes of the present thesis under the heading of 'information collection' case-study, but besides collection of personal data it involves their storage, processing, retention, and transfer to the relevant authorities. It should be clarified, therefore, that this categorisation of the specific counter- terrorism measures addressed under certain case-studies that describe different instances of processing is not aimed to be in any way absolutist or categorical.

Having set the subject-matter of the present thesis, it has to be explained *why* this research is undertaken. First, there has been no comprehensive legal analysis, up to this point, reflecting on the evaluation of this (new) fundamental right and how it interrelates with privacy in the field of law enforcement. Second, the present thesis differs from the traditional counter-terrorism legal studies that normally tend to undertake a positivist analysis of specific counter-terrorism measures against fundamental rights, such as the rights to privacy and data protection in order to assess whether a non-permissible infringement has taken place. Such a statement should be qualified. It is true that this thesis necessarily conducts a counter-terrorism study. Unlike normal counter- terrorism studies, however, it seeks to examine *primarily* not whether EU counter-terrorism measures fall behind the EU standards of data protection, but what is the *practical significance* and *normative importance* of the

[2] On terrorism and counter-terrorism *see* among others Hanspeter Neuhold, *International Terrorism. Definitions, Challenges and Responses*, INTERNATIONAL TERRORISM : A EUROPEAN RESPONSE TO A GLOBAL THREAT? 23 (Dieter Mahncke & Jörg Monar, 2006).

newly recognised fundamental right to data protection in the field of counter-terrorism. The *practical significance* of the constitutional entrenchment of data protection entails an examination of what this fundamental right can offer in practice to legislators, courts, and individuals. This is essentially closely interconnected to the *normative importance* of the right, which, in this thesis will be discussed separately, focusing mainly on the normative value of a right to data protection next to the right to privacy. This means, in essence, that a substantive assessment on the basis of the right to data protection of the specific counter-terrorism measures discussed will be provided to the extent that this is instrumental to the research to attempt a reply to the following questions: Does the right to data protection add something to the protection of the individual in the context of law enforcement? If not, can this right be constructed in order to have an added value? How can this be possible?

One further clarification is needed here. My intention is not to focus on the distinction between privacy and data protection by engaging into a purely theoretical (but limited practically) discussion on whether data protection can be conceived as a separate, or an autonomous fundamental right, or an aspect of privacy. Data protection, in general, falls under the privacy umbrella and pursues privacy objectives in any case. The question is what pattern should be followed so that the two rights combined can provide for the highest protection in the context of counter-terrorism measures.

1.2 Limitations

The research has certain limitations that should be stated. First, it does not address all the EU measures that involve processing of personal data for counter-terrorism purposes, but it only focuses on the four particular case-studies mentioned above (the Data Retention Directive, SIS II, VIS, EURODAC, PNR and TFTP). This excludes an analysis of legal instruments such as the Prüm Decision,[3] or the 'Swedish' framework decision[4] that aim to speed up and simplify the exchange of different types

[3] 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 L 210/1 of 6.8.2008.
[4] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union OJ L386/89 of 29.12.2006.

of information between the Member States. Also, the Europol and Eurojust databases and their possibilities of information exchange are not subject of this research. This is because, as explained above, the core research question of this thesis is the assessment of the added value of data protection as a fundamental right in the context of law enforcement. Therefore, a comprehensive study on a fundamental rights assessment of all EU counter-terrorism measures involving information processing is out of its purposes. Furthermore, this research-line has been profoundly developed by other authors.[5]

The research is also limited *'ratione temporis'*. Several of the EU counter-terrorism measures addressed at the present thesis are currently being (or they will be) repealed, amended or renegotiated (for instance, the EU-US PNR Agreement). Others, such as SIS II and VIS have not become fully operational yet. The Commission's proposals on the establishment of an EU PNR and an EU TFTS are still in a very early stage. The Data Retention Directive has been currently challenged through the preliminary ruling procedure before the Court of Justice. Finally, on the top of all these, the Commission introduced recently a proposal for a new data protection legal framework. Many developments are still to appear, but the present research necessarily describes the situation as it is until the end of January 2012.

1.3 Sources

The research employs mainly legal documents of the EU. The analysis of EU primary law, EU secondary legislation such as Regulations, Directives, Council Decisions, international agreements and decisions of European courts (mainly the Court of Justice of the EU, but also national constitutional courts) is at the centre of the present thesis. Due attention is been given also to Opinions of the European Data Protection Supervisor and of the Article 29 Data Protection that have a particular importance in the context of counter-terrorism. The Recommendations and the Reports of the European Parliament, as well as the Working Documents of the Article 29 Working Party and the various Commission Communications constitute a further

[5] *See* for instance, *inter alia,* FRANZISKA BOEHM, INFORMATION SHARING AND DATA PROTECTION IN THE AREA OF FREEDOM, SECURITY AND JUSTICE TOWARDS HARMONISED DATA PROTECTION PRINCIPLES FOR INFORMATION EXCHANGE AT EU-LEVEL (2012).

important part of the research. Furthermore, EU policy documents are utilised but to a more limited extent as they are normally intended to set the general political framework of EU policies.

Data protection has generated an abundant literature mainly coming from legal scholars, political scientists, and information scientists. The legal and political science literature, commentaries, studies, case-notes and reports constitute a particularly important source for the present analysis. It goes without saying that a *selection procedure* must be employed. According to this, pieces of research most close to the focus of the present thesis are preferred.

1.4 Terminology

The thesis uses a number of terms that require further clarification. These include 'data protection', 'privacy', 'personal data', 'information', 'processing', 'data subject', 'data controller', 'data protection principles', 'fair information principles' and 'law enforcement authorities'. As the analysis focuses on a specific legal framework, the EU, the different terms are most commonly understood by reference to this legal order.

'Data protection' comes from the German '*Datenschutz*'. It denotes normally a set of legal rules that protects the interests of individuals, whose personal data are collected, stored, disseminated, destructed, or otherwise processed. 'Privacy' has a different meaning from 'data protection' in this thesis. 'Privacy' is understood as the general right that refers to the respect of the private and family life, home and correspondence, as it is laid down in Article 8 ECHR and Article 7 EUCFR.

'Personal data' refers to any information related to an identified or an identifiable natural person. Often this thesis uses the term 'information' instead of the most accurate 'personal data'. Nevertheless, their notions should be regarded as synonymous for the purposes of this analysis.

'Processing' is any operation or set of operations performed upon personal data normally by automatic means. The notion, as understood in EU law, is very broad and it includes the collection, recording, organisation, storage, retrieval, use, disclosure, dissemination, combination, combination, erasure, destruction of personal data, etc. The broad understanding of the term is also endorsed in the present thesis.

'Data subject' is the identified natural person to whom the information is linked. Data protection law normally grants the 'data subject' certain rights concerning his/her data. The present thesis uses sometimes the term 'individual' to denote the 'data subject'.

The term 'data controller' denotes the natural or legal person, public authority, agency or any other body that alone or jointly with others determines the purposes and means of the processing of personal data. Data protection law normally imposes certain obligations on the 'data controller'.

'Data protection principles' are understood as the set of rules that govern the processing of personal data. The 'data protection principles' are considered the core of data protection law. The term 'data protection principles' is used interchangeably with the term 'fair information principles' in this thesis.

The research project uses numerous times the term 'law enforcement': 'law enforcement purposes', 'law enforcement authorities', 'law enforcement context', etc. 'Law enforcement authorities' are to be understood as the authorities responsible for the prevention, detection and investigation of criminal offences. The notion is used broadly here and comprises the judicial, police and intelligence agencies involved in crime prevention and investigation.

1.5 Outline

This thesis contains seven chapters, an introduction and conclusions. It is divided into two Parts. Part I lays down the theoretical foundations of the research and provides a general overview of the EU data protection legal framework and the EU counter-terrorism policies. Part II discusses three data processing cases-studies under four different EU counter-terrorism measures: the Data Retention Directive, the EU large-scale databases, PNR and TFTP.

Chapter 1 sets out the theoretical framework of the thesis. It explains the concepts of privacy and data protection and the differences between the two rights. It analyses the underlying values of data protection, and the approaches to this right. It discusses the current theories on data protection and identifies their shortcomings. It provides a new theory on data protection that reconstructs the fundamental right. It examines how European courts perceive data protection.

Chapter 2 provides an overview of the current EU data protection legal framework, with a focus on the changes introduced by the Lisbon Treaty. It takes a closer look at primary and secondary EU law concerning data protection and points out its shortcomings. It lays down the case-law of the Court of Justice in the EU on data protection and describes in detail the legal framework covering police and judicial cooperation in criminal matters.

Chapter 3 presents the EU's counter-terrorism strategy and its particularities. It examines the EU's counter-terrorism cooperation and identifies its milestones. It discusses the limitations of the EU's counter-terrorism strategy and explains why information sharing is considered the main contribution of the EU in the fight against terrorism.

Chapter 4 deals with the Data Retention Directive. It analyses its background and discusses its provisions. It addresses the general misconceptions between privacy and data protection that are voiced with regard to the Directive and attempts to clear out the confusion. For this purpose, it uses the theoretical framework set out in Chapter 1 and discusses its practical implications. It engages into a substantive assessment of the Directive on the basis of fundamental rights, and examines the relevant pronouncements on the issue of the European and national constitutional courts.

Chapter 5 considers the use of the information stored in the systems of SIS II, VIS and EURODAC for law enforcement purposes. It discusses the relevant legal framework of each database, by focusing in particular on SIS II that pursues law enforcement purposes. It analyses critically the new functionalities introduced to the second generation system and examines the fundamental rights question raised thereof. It takes a look at the Decision on the access to VIS for law enforcement purposes and the relevant proposal concerning EURODAC. It reflects on the problems posed in general by databases and explains how these are better dealt with the right to data protection.

Chapter 6 assesses the EU-US PNR case. It provides the chronology of the PNR saga and discusses the three relevant Agreements. It takes a look at the position of the European Parliament and of bodies such as the European Data Protection Supervisor and the Article 29 Working Party on the issue. It examines the relevant decision of the Court of Justice and by focusing on the Advocate General's Opinion it proves why the conceptual confusions of privacy and data protection are dangerous. It

assesses critically the EU's plans for the establishment of its own PNR system. It discusses the problems posed by datamining and profiling in the context of airline passenger surveillance. It concludes by assessing substantively the EU-US PNR Agreement on the basis of the right to data protection.

Chapter 7 deals with the TFTP case. It presents the timeline of events by focusing to the US secret operations on SWIFT data for almost six years. It discusses how the programme from operating secretly it became the subject of an international agreement between the EU and the US with the eulogies of the European Parliament. It analyses the problem posed by TFTP and explains why this is primarily a privacy issue. It discusses the problematic role of Europol in the context of the new TFTP Agreement and reflects on the establishment of an EU TFTS system.

The Conclusions wrap up the discussion and summarise the findings. It is argued that data protection has an added value in the context of law enforcement if this right is to be understood as it was reconstructed in the present thesis. The issue is not merely theoretical, but it has serious practical implications demonstrated by the different case-studies. Data protection has an important role to play in the context of law enforcement if it is understood correctly by courts and legislators.

PART I. THEORETICAL FOUNDATIONS

CHAPTER 1. 'Taking Data Protection Seriously': A New Theory For A (Not So) New Right.

1. Conceptualising Privacy

> *"Data protection laws have always been marked by the uneasiness in dealing with constantly advancing technology. Legislators deliberately chose a distinctly abstract language in order to improve the chances to address unknown aspects and new developments of technology."*[6]

1.1 Privacy and data protection: Two Nebulous Concepts?

Athena, the goddess of wisdom, and patron of Athens, sprang, according to ancient Greek mythology, fully armed and brandishing a sharp javelin out of her father's, Zeus, head, after he was tortured by a terrible headache. The life of privacy and data protection is reminiscent of this beautiful ancient Greek myth. The two rights seem to share a parent- child relationship. Data protection appeared as an offspring of privacy and the two rights still seem inextricably tied up together with a birth cord. However, -as any child-, data protection is trying to mark its own way in life.

At the outset, the two rights are mudded into a confusing cluster of differences and similarities. Books and articles on privacy normally begin with the assertion that this is the most difficult right to define.[7] On the other hand, legal scholars writing on data protection do not seem to find it hard to describe the main essence of data protection laws: they are rules that "specifically regulate all or more stages in the processing"[8] of *personal* information; which is normally defined as any information relating to an identified or identifiable person.[9]

---

[6] Spiros Simitis, *Privacy– An Endless Debate?*, 98 CALIFORNIA LAW REVIEW 1989, 1999 (2010).
[7] William Beaney comments that: "even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right." *See* William Beaney, *The Right to Privacy and American Law*, 31 L. & CONTEMP. PROBS. 253, 255 (1966).
[8] LEE BYGRAVE, DATA PROTECTION LAW : APPROACHING ITS RATIONALE, LOGIC, AND LIMITS 2 (2002).
[9] Article 2 (a) of Directive 95/46/EC.

Be that as it may, the conceptual difficulty to define privacy "does not undermine its importance".[10] Privacy has been described as 'the right most valued by civilized men'[11] and its value has been rarely questioned.[12] On the other hand, there is a general confusion among courts and legal scholars of the benefits of a right to data protection and doubts have been raised concerning its entrenchment.[13] In this context, the question normally goes: what is the added value of a right to personal data protection, or to put it more simply, does it add anything to the right to privacy, however the latter is being defined? Despite of these doubts, and characterised by what has been called by Stefano Rodotà as a "veritable social, political, and institutional schizophrenia",[14] data protection found its way in certain jurisdictions to the status of a fundamental right alongside with the right to privacy.[15]

It is, however, not questioned among commentators that privacy and data protection share a common characteristic: they are both confronted with serious interferences in the contemporary information society. Numerous authors have expressed concerns about the threats that privacy is facing in the 'surveillance' society.[16] Some go as far as to talk about its 'end', or its 'death'.[17] The diminution of the relevant principles and safeguards of data protection is equally lamented by scholars. [18]

---

[10] ADAM MOORE, PRIVACY RIGHTS : MORAL AND LEGAL FOUNDATIONS 11 (2010). Delany and Carolan note: "Most people would agree that privacy is important. Most people also, however, would disagree about what privacy precisely entails". HILARY DELANY & EOIN CAROLAN, THE RIGHT TO PRIVACY : A DOCTRINAL AND COMPARATIVE ANALYSIS 4 (2008).

[11] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis. J. , dissenting). *See* also Solove who notes that "…there appears to be worldwide consensus about the importance of privacy and the need for its protection". DANIEL SOLOVE, UNDERSTANDING PRIVACY 3 (2008).

[12] However, there are scholars that have questioned the inherent value of privacy. *See* for instance AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999); Richard A Posner, *Privacy and Related Interests*, THE ECONOMICS OF JUSTICE 229 (1983). For a more detailed analysis *see* DELANY & CAROLAN, *supra* note 10, at 5; GIOVANNI SARTOR, PRIVACY, REPUTATION, AND TRUST: SOME IMPLICATIONS FOR DATA PROTECTION 7 (European University Institute, EUI Working Papers, Law No. 2006/04).

[13] *See* for instance Lucas Bergkamp, *EU Data Protection Policy - The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER LAW & SECURITY REPORT 31, 31 (2002).

[14] Stefano Rodotà, *Data Protection as a Fundamental Right*, REINVENTING DATA PROTECTION?, 77 (Serge Gutwirth et al., 2009).

[15] Article 8 European Charter of Fundamental Rights.

[16] DAVID LYON, SURVEILLANCE AFTER SEPTEMBER 11 (2003); David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, CASE WESTERN RESERVE LAW REVIEW 831, 835–836 (1990).

[17] CHARLES SYKES, THE END OF PRIVACY (1st St. Martin's Griffin ed. ed. 2000); Michael Froomkin, *The Death of Privacy?*, 52 STANFORD LAW REVIEW 1461 (2000). *See* also the editorial of The *Economist* (The *Economist* 1999, 16): "Privacy is doomed…get used to it."
Solove, Understanding Privacy, 5.

[18] Rodotà, *supra* note 14, at 77.

The present study focuses on the infant of the two rights: the right to personal data protection. A large body of laws pertains already to data protection, however there are numerous uncertainties concerning the right's capabilities to resolve problems and provide for an effective protection. The right will be tested in the most difficult context: law enforcement and counter-terrorism. It is in this context that I endeavour to set forth a theory of data protection that will reshape in a clear and comprehensive manner the understanding of the right, and guide courts and legislators on data protection issues in the field of law enforcement.

This chapter aims to bring clarity on the concept of data protection, its underlying values and aims, and the approaches to this right. It discusses the current theories and the existing case-law on data protection by identifying their shortcomings. It elaborates a new theory on data protection and addresses its benefits and possible limitations in order to build a conceptual framework of the right that is to be tested in three specific cases of data processing in the field of law enforcement: 1) the information collection; 1) the information storage; and, 3) the information transfer case.

1.2 The Concept of Privacy

1.2.1 Conceptions of Privacy

Defining privacy has not proved an easy task. The question 'what is privacy' has bothered numerous legal scholars, philosophers, sociologists and psychologists. Many of them have expressed their despair to reach a satisfying definition of the concept of privacy.[19] Problems arise mainly because privacy is "exasperatingly vague and evanescent",[20] "notoriously elastic and equivocal",[21] "engorged with various and distinct meanings",[22] "highly subjective",[23] "culturally relative",[24] and operating "in a

[19] *See* C. D. Raab & C. J. Bennett, *Taking the Measure of Privacy: Can Data Protection Be Evaluated?*, 62 INTERNATIONAL REVIEW OF ADMINISTRATIVE SCIENCES 535, 537 (1996).
[20] ARTHUR MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1972).
[21] DELANY & CAROLAN, *supra* note 10, at 4.
[22] Robert C. Post, *Three Concepts of Privacy*, 89 GEORGETOWN LAW JOURNAL 2087, 2087 (2000).
[23] COLIN BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY : POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 8 (2006).

plethora of unrelated contexts".[25] Lillian BeVier notes eloquently: "Privacy is a chameleon-like word, used denotatively to designate a wide range of wildly disparate interests – from confidentiality of personal information to reproductive autonomy."[26]

A number of different methodologies have been suggested over time in order to approach the concept of privacy. It has been argued that one can identify different levels[27] or different contexts[28] of privacy: 'the descriptive level' which comprises the neutral definition of privacy that can be found in dictionaries;[29] the 'value level' that entails value considerations;[30] the 'legal level' which refers to the particular area of privacy that is protected by law;[31] and, the 'interest' level that expresses the reasons ('interests') justifying the protection granted to the right.[32] Another author points out that definitions of privacy can be couched in descriptive or normative terms, depending on whether privacy is seen as a "mere condition" or a "moral claim" on others to refrain from certain activities.[33] Furthermore, some commentators argue that privacy should be conceived as instrumental to other rights or values,[34] or as a "derivative notion" that rests upon more basic rights such as liberty or property.[35] Daniel Solove proposes that "[i]nstead of attempting to locate the common denominator of these activities", the disruptions of which are considered as interferences with privacy; "we should conceptualize privacy by focusing on the specific types of disruption".[36] He, thus, develops a "taxonomy" of privacy, a "framework for understanding privacy in a pluralistic and contextual manner", grounded "in the different kinds of activities which impinge upon privacy". [37]

---

[24] MOORE, *supra* note 10, at 11.
[25] J MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY ¶ 5.59 (1987).
[26] Lillian BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WILLIAM AND MARY BILL OF RIGHTS JOURNAL 455, 458 (1995).
[27] Blanca Rodriguez- Ruiz, *Protecting the Secrecy of Telecommunications : a Comparative Study of the European Convention on Human Rights, Germany and United States*, 30 (1995).
[28] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1979). Gavison distinguishes three different contexts of privacy: privacy as a neutral concept, privacy as a value and privacy as a concept useful in legal concepts.
[29] Rodriguez- Ruiz, *supra* note 27, at 37.
[30] *Id.* at 40.
[31] *Id.* at 42.
[32] *Id.* at 44.
[33] MOORE, *supra* note 10, at 11.
[34] Antoinette Rouvroy & Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, REINVENTING DATA PROTECTION?, 45 (Serge Gutwirth et al., 2009).
[35] SOLOVE, *supra* note 11, at 38.
[36] *Id.* at 9.
[37] *Id.* at 10.

Numerous definitions of the notion of privacy have been suggested. Among the most influential, is the conception of privacy as "the right to be let alone", based on the famous article "The Right to Privacy"[38] of Samuel Warren and Louis Brandeis. In their path-breaking work, Warren and Brandeis contended that "the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[39] Privacy has also been defined as the "right to decide how much knowledge of [a person's] personal thought and feeling… private doings and affairs…the public at large shall have."[40] Variations of this definition, which has been called the "limited access to the self"[41] conception of privacy have been developed by a number of scholars.[42] Privacy has also been seen as "concealment of information"[43] from others. Another theory views privacy as a form of protecting "the individual's interest in becoming, being, and remaining a person".[44] Furthermore, privacy has been conceived as a form of intimacy. In this sense, privacy is "the state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring, or liking."[45] Solove criticizes all the above concepts of privacy as being either too broad or too narrow, but instead of attempting to provide a definition of privacy himself, he proposes a so-called 'pragmatic' theory that "understands privacy as a set of protections against a related cluster of problems."[46] His theory focuses on four

---

[38] Samuel D. Warren & Louis D. Brandeis, *Right to Privacy*, 1890 HARV. L. REV. 193. The article has been characterized by Kalven as the "most influential law review article of all". *See* Harry Kalven, *Privacy in Tort Law- Were Warren and Brandeis Wrong?*, 31 L. & CONTEMP. PROBS. 326, 327 (1966).

[39] Warren & Brandeis, *supra* note 38, at 205. This definition of privacy has been criticized as unduly broad, because "it does not inform us about the matters in which we should be let alone." *See* SOLOVE, *supra* note 11, at 17; DELANY & CAROLAN, *supra* note 10, at 8.Solove, *Understanding Privacy*, 17; Delany and Carolan, *The right to privacy,* 8.

[40] El Godkin, *The Rights of the Citizen-IV-To His Own Reputation*, 8 SCRIBNER'S MAGAZINE 58, 65 (1890).

[41] SOLOVE, *supra* note 11, at 18.

[42] Sissela Bok considers privacy as the "condition of being protected from unwanted access by others". SISSELA BOK, SECRETS : ON THE ETHICS OF CONCEALMENT AND REVELATION 10 (1989). Ruth Gavison argues that limited access consists of "three independent and irreducible elements: secrecy (the extent to which we are known to others), anonymity (the extent to which we are the subjects of others' attention), and solitude (the extent to which others have physical access to us." *See* Gavison, *supra* note 28, at 423.The limited-access theory is criticized for being too broad and vague. SOLOVE, *supra* note 11, at 20.

[43] RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 46 (5th ed. ed. 1998).

[44] Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHILOSOPHY & PUBLIC AFFAIRS 26, 314 (1976).

[45] JULIE INNESS, PRIVACY, INTIMACY AND ISOLATION 56 (1996). For Charles Fried, "[i]ntimacy is the sharing of information about one's actions, beliefs or emotions which one does not share with all, and which one has the right not to share with anyone." CHARLES FRIED, AN ANATOMY OF VALUES PROBLEMS OF PERSONAL AND SOCIAL CHOICE. 142 (1970).

[46] SOLOVE, *supra* note 11, at 40.

principal privacy problems: 1) information collection, 2) information processing, 3) information dissemination, and 4) invasion.[47] Finally, privacy has been conceived as control over personal information. The following section will focus on this definition, not because the present author considers it as the most adequate to capture the notion of privacy, but because it uncannily reminds, more than any other conception of privacy described above, the object of the present thesis, ie, the right to data protection.

A further important point arises from the privacy debate that should not be missed here. This concerns the normative distinction that is made frequently between "private" and "public",[48] "privacy" and "publicity",[49] the "private" and the "public sphere".[50] Following this distinction, privacy is seen as "suspicious"[51] and "socially detrimental",[52] because it advocates a form of "retreat from society".[53] The origins of this approach to privacy are being traced by philosophers and legal scholars[54] to ancient Greece and Rome, where privacy had a negative connotation, since a citizen's life meant active participation in the *polis*.[55] This theory was further taken up by

---

[47] *Id.* at 10. Solove's theory has been criticised as "logically circular" because the identification of instances of privacy infringements necessarily pre-suppose some pre-existing idea of what privacy entails. *See* DELANY & CAROLAN, *supra* note 10, at 10.

[48] Paul De Hert, *The Case of Anonymity in Western Political Philosophy- Benjamin Constant's Refutation of Republican and Utilitarian Arguments Against Anonymity*, DIGITAL ANONYMITY AND THE LAW: TENSIONS AND DIMENSIONS 47, 52 (C Nicoll et al., 2003).

[49] Rodriguez- Ruiz, *supra* note 27, at 29.

[50] De Hert, *supra* note 48, at 52.

[51] *Id.*

[52] SOLOVE, *supra* note 11, at 80.

[53] *Id.*

[54] For an analysis of the historical development of the public- private debate *see* Joe Bailey, *From Public to Private: The Development of the Concept of the "Private,"* 69 SOCIAL RESEARCH: AN INTERNATIONAL QUARTERLY 15 (2002).

[55] Here Thoukidides, Pericle's Epitaph speech is normally cited, (para 40), where Perikles says to the Athenians:
"μόνοι γὰρ τόν τε μηδὲν τῶν δε μετέχοντα οὐκ ἀπράγμονα, ἀλλ' ἀχρεῖον νομίζομεν, καὶ οἱ αὐτοὶ ἤτοι κρίνομέν γε ἢ ἐνθυμούμεθα ὀρθῶς τὰ πράγματα, οὐ τοὺς λόγους τοῖς ἔργοις βλάβην ἡγούμενοι, ἀλλὰ μὴ προδιδαχθῆναι μᾶλλον λόγῳ πρότερον ἢ ἐπὶ ἃ δεῖ ἔργῳ ἐλθεῖν." ("We differ from the other states in regarding man who holds aloof from public life not as quiet, but as useless; we decide or debate, carefully and in person, all matters of policy, holding not that words and deeds go ill together but that acts are foredoomed to failure when undertaken undiscussed."). However, *see* also Pericles, para 37: "ἐλευθέρως δὲ τά τε πρὸς τὸ κοινὸν πολιτεύομεν καὶ ἐς τὴν πρὸς ἀλλήλους τῶν καθ' ἡμέραν ἐπιτηδευμάτων ὑποψίαν, οὐ δι' ὀργῆς τὸν πέλας, εἰ καθ'ήδονήν τι δρᾷ, ἔχοντες, οὐδὲ ἀζημίους μέν, λυπηρὰς δὲ τῇ ὄψει ἀχθηδόνας προστιθέμενοι. ἀνεπαχθῶς δὲ τὰ ἴδια προσομιλοῦντες τὰ δημόσια διὰ δέος μάλιστα οὐ παρανομοῦμεν, τῶν τε αἰεὶ ἐνἀρχῇ ὄντων ἀκροάσει καὶ τῶν νόμων, καὶ μάλιστα αὐτῶν ὅσοι τε ἐπ' ὠφελίᾳ τῶνἀδικουμένων κεῖνται καὶ ὅσοι ἄγραφοι ὄντες αἰσχύνην ὁμολογουμένην φέρουσιν." ("The freedom which we enjoy in our government extends also to our ordinary life. There, far from exercising a jealous surveillance over each other, we do not feel called upon to be angry with our neighbor for doing what he likes, or even to indulge in those injurious looks which cannot fail to be offensive, although they inflict no positive penalty. But all this

republican philosophers as Rousseau, who saw private concerns as a threat to the functioning of good government and the end of the state.[56] More recently, Hannah Arendt relying on the idea that privacy in ancient Greece meant "literally a state of being deprived of something",[57] heavily criticised private life.[58]

This distinction between private and public life, between the "self" and the "society",[59] sees privacy as an individual right in juxtaposition with the larger community.[60] This perception that fails to recognize the "broader social importance of privacy",[61] and views it as a right that serves solely the individual, is very problematic, because, as Priscilla Regan explains, "when privacy is defined as an individual right, policy formulation entails a balancing of the individual right to privacy against a competing interest or right. In general, the competing interest is recognized as a social interest. For example, the police interest in law enforcement,… it is also assumed that the individual has a stake in these societal interests. As a result, privacy has been on the defensive, with those alleging a privacy invasion bearing the burden of providing that a certain activity does indeed invade privacy and that the 'social' benefit to be gained from the privacy invasion is less important than the individual harm incurred…"[62] It should be accepted that "privacy has value beyond its usefulness in helping the individual to maintain his or her dignity or develop personal

---

ease in our private relations does not make us lawless as citizens. Against this fear is our chief safeguard, teaching us to obey the magistrates and the laws, particularly such as regard the protection of the injured, whether they are actually on the statute book, or belong to that code which, although unwritten, yet cannot be broken without acknowledged disgrace"); and, para 40:
"ἔνι τε τοῖς αὐτοῖς οἰκείων ἅμα καὶ πολιτικῶν ἐπιμέλεια, καὶ ἑτέροις πρὸς ἔργα τετραμμένοις τὰ πολιτικὰ μὴ ἐνδεῶς γνῶναι" ("Our public men have, besides politics, their private affairs to attend to, and our ordinary citizens, though occupied with the pursuits of industry, are still fair judges of public matters.")

[56] J.J. Rousseau, Du contrat social (1762), in *Oeuvres completes de Jean-Jaqcues Rousseau,* edited by B. Gagnebin and M. Raymond, Paris, Gallimard (Pleiade), 1964, Book 1, Chapter VIII, 365. Rousseau argued that: "As soon as public service ceases to be the chief business of the citizens and they would rather serve with their money than with their persons, the State is not far from its fall... The better the constitution of a State is, the more do public affairs encroach on private in the minds of the citizens. Private affairs are even of much less importance, because the aggregate of the common happiness furnishes a greater proportion of that of each individual, so that there is less for him to seek in particular cares. In a well-ordered city every man flies to the assemblies; under a bad government no one cares to stir a step to get to them, because no one is interested in what happens there, because it is foreseen that the "general will" will not prevail, and lastly because domestic cares are all-absorbing." *See* also De Hert, *supra* note 48, at 51.

[57] HANNAH ARENDT, THE HUMAN CONDITION 38 (2nd ed. ed. 1998).

[58] "To live an entirely private life means above all to be deprived of things essential to a truly human right." *Id.* at 50.

[59] RICHARD HIXSON, PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT 212 (1987).

[60] SOLOVE, *supra* note 11, at 89.

[61] PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 213 (1995).

[62] *Id.*

relationships. Most privacy scholars emphasize the individual is better of if privacy exists. I maintain that the society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public and collective purposes."[63] Privacy, thus, has a public value,[64] because it protects the individual "for the good of society".[65] In this sense, when the balancing of privacy with competing interests or rights is at stake, it would be a fallacy to base its outcome on the false premise of a balancing between an individual right on the one hand, and a social interest on the other, because, as seen above, privacy equally serves the social purpose.

1.2.2 Privacy as control over personal information

Alan Westin defined privacy as "the claim of individuals, groups, or institutions to determine for when, how, and to what extent information about them is communicated to others."[66] A number of other authors also conceive privacy as the individual's entitlement to control over personal information.[67] According to Charles Fried "privacy is not simply an absence of information about what is in the minds of others; rather it is the *control* we have over information about ourselves. To refer for instance to the privacy of a lonely man on a desert island would be to engage in irony. The person who enjoys privacy is able to grant or deny access to others.... Privacy,

---

[63] *Id.* at 321.

[64] Spiros Simitis points out that "privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone." *See* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 707, 709 (1987).

[65] Daniel Solove notes: "Privacy is valuable not only for our personal lives, but for our lives as citizens – our participation in public and community life. It is hard to imagine how people could freely participate in public life without some degree of control over… their private life. Thus privacy is more than a psychological need or desire; it is a profound dimension of social structure. In addition to protecting individuals, privacy safeguards relationships between individuals, which are essential for family life, social engagement, and political activities." SOLOVE, *supra* note 11, at 92–93.

[66] Alan Westin identifies four basic states of individual privacy: 1) solitude- "the individual is separated from the group and freed from the observation of other persons" 2) intimacy- "the individual is acting as a part of a small unit that claims and is allowed to exercise corporate seclusion so that it may achieve a close, relaxed and frank relationship between two or more individuals" 3) anonymity- "the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance 4) reserve- "the creation of a psychological barrier against unwanted intrusion; this occurs when the individual's need to limit communication about himself is protected by the willing discretion of those surrounding him." ALAN WESTIN, PRIVACY AND FREEDOM 31–32 (1970).

[67] *See* ADAM CARLYLE BRECKENRIDGE, THE RIGHT TO PRIVACY 1 (1970); Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990*, 80 CALIFORNIA LAW REVIEW 1133 (1992); DELANY & CAROLAN, *supra* note 10, at 22.

thus, is control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of the knowledge as well. We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details."[68]

The control-over-personal information conception has been criticised as a theory of privacy for being both too narrow and too vague.[69] On the one hand, it is too narrow because it excludes the non- informational aspects of privacy, also known as "decisional privacy", which in the USA constitutional protection of privacy, refers to the individual's entitlement to make his own decisions.[70] The distinction between "informational" and "decisional" privacy in US Constitutional law has been recognised by Justice Stevens, who, in his Opinion in *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[71] noted that privacy cases before the Supreme Court "in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[72] In this respect, the control-over personal information conception of privacy is narrow because it fails to take the second interest into account. On the other hand, it is too vague because it does not provide a clear definition of the notion of personal information, over which the individual is entitled to control.[73] For instance, while one definition of personal information as "control over who can see us, hear us, touch us, smell us, and taste us, in sum, control over who can sense us…",[74] is considered unduly broad; another, that sees personal information as "any data about an individual that is identifiable to that individual"[75] does not fit in well a privacy theory, because

[68] Charles Fried, *Privacy*, 77 YALE L.J. 475, 482–483 (1968).
[69] SOLOVE, *supra* note 11, at 24.
[70] DELANY & CAROLAN, *supra* note 10, at 21. As Solove and Schwartz explain, "decisional privacy involves matters such as contraception, procreation, abortion, and child rearing, and is at the center of a series of Supreme Court cases often referred to as "substantive due process" or "the constitutional right to privacy." Non-informational aspects of privacy are inherent also in the right to private and family life as protected in Article 8 ECHR. *See* DANIEL SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 1 (3rd ed. ed. 2009).
[71] *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989).
[72] *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 762. *See* also *Whalen v. Roe*, 429 U.S. 589 (1977), 598- 600.
[73] SOLOVE, *supra* note 11, at 24.
[74] Richard B. Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 280 (1974).
[75] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383 (1996).

"there is a significant amount of information identifiable to us that we do not deem as private."[76]

2. Conceptualising Data Protection

2.1 A first look at the Concept of Data Protection

Writing on the concept of data protection, Paul de Hert and Serge Gutwirth, comment that "it is impossible to summarise data protection in two or three lines. Data protection is a catch-all term for a series of ideas with regard to the processing of personal data."[77] If we attempt to take a look at data protection instruments, for instance, Directive 95/46/EC (the "European Data Protection Directive") regards data protection as the protection of "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".[78] The notions of "processing" and of "personal data", thus, appear central for the understanding of the concept of data protection. In general terms, "processing" can be seen as any operation performed upon the data, from their collection, recording, storage, use, to their disclosure, dissemination, erasure and destruction. The data are considered personal, when they can be linked to a certain individual.

Data protection can be conceived, thus, as referring to this set of legal rules that aim to protect the rights, freedoms and interests of individuals, whose personal data are collected, stored, processed, disseminated, destructed, etc.[79] The ultimate objective is to ensure "fairness in the processing of data and, to some extent, fairness in the outcomes of such processing".[80] The fairness of processing is safeguarded by a

[76] SOLOVE, *supra* note 11, at 25.
[77] Paul De Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, REINVENTING DATA PROTECTION? 3, 3 (2009).
[78] Article 1 (1) of the Data Protection Directive.
[79] FRITS HONDIUS, EMERGING DATA PROTECTION IN EUROPE 1 (1975).
[80] BYGRAVE, *supra* note 8, at 168.

number of principles (also known as "fair information principles" or "data protection principles), which, in general terms, can be couched as follows:[81]

1) personal information should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

2) it should be collected and processed fairly and lawfully;

3) it should be adequate, accurate, relevant and not excessive with regard to the purposes for which it is collected and processed;

4) it should not be kept for longer than is necessary for the purposes for which it was collected and processed;

5) the consent of the person to whom the information relates is necessary for some categories processing;

6) security measures should be taken in order to protect the data from accidental loss or unauthorized disclosure and use;

7) the individual should be informed that his/her data are held by others; should be given access to them and the possibility to correct them if they are inaccurate or misleading;

8) the processors of personal information should be accountable for complying with the fair information principles.[82]

While defining data protection does not seem to pose the philosophical controversies and difficulties that the concept of privacy faces; nevertheless, it is not a notion without problems itself. Its meaning is not very clear from the outset,[83] all the more because its definition appears to be quite technical and confusing, as it is based to further notions, such as 'personal data' and 'processing' that seek definition themselves.[84] The term 'data protection', which derived from the German '*Datenschutz*', is most commonly used in (continental) European jurisdictions; in the USA, Canada and Australia other terms such as 'informational privacy', 'data privacy' or simply 'privacy protection' are used.[85] Despite its problems, the term 'data

[81] The list presents indicatively only a core of fair information principles. The exact formulation of the principles differs in the various texts, for instance, the EU Data Protection Directive, the CoE Convention No 108, the OECD and the APEC privacy guidelines. For a presentation of the OECD data protection principles *see* below. For the Data Protection Directive principles *see* Chapter 2.

[82] Arguably, further principles could be included in the list. *See* BYGRAVE, *supra* note 8, at 2.

[83] *Contra* Hondius who argues that "Etymologically, … the term [data protection] is not quite correct, but its meaning is clear." HONDIUS, *supra* note 79, at 1.

[84] The term data protection has also been criticized for concentrating disproportionately on the data rather than the person as the object of protection. *See* BENNETT & RAAB, *supra* note 23, at 11.

[85] BYGRAVE, *supra* note 8, at 1.

protection' will be preferred in the present thesis, for reasons that will be explained below.

2.2 Data Protection as 'Informational Self-Determination'

Understanding data protection, however, as management of personal information is not enough. Data protection is not simply about informational privacy; it is about informational *autonomy.*[86] This concept of data protection cannot find a more accurate description in legal terms, than in the right to 'informational self-determination' ('informationelle Selbstbestimmung'), as pronounced by the German Constitutional Court (*Bundesverfassungsgericht*) in its landmark Census decision ('Volkszählungsurteil').[87] According to the Court, the right to 'informational self-determination' guarantees, in principle, the power of the individual to determine for himself the disclosure and use of his data. The right is based on Articles 1 (1) (human dignity)[88] and 2 (1) (personality right)[89] of the German Constitution. These require "clearly defined conditions of processing", which ensure "that under the conditions of automatic collection and processing of personal data the individual is not reduced to a mere object of information."[90]

The decision of the Constitutional Court is grounded on the idea of autonomy and the free development of the personality. As Julie Cohen astutely notes: "informational autonomy comports with important values concerning the fair and just treatment of individuals within society. From Kant to Rawls, a central strand of Western philosophical tradition emphasises respect for the fundamental dignity of persons, and a concomitant commitment to egalitarianism in both principle and practice… these principles have clear and very specific implications for the treatment of personally-identified data: They require that we forbid data-processing practices

[86] Emphasis added.
[87] Volkszählungsurteil, 65 BVerfGE 1, 68-69 (1983).
[88] Article 1 (1) of the German Constitution proclaims: "Human dignity is inviolable. To respect and protect it is the duty of all State authority."
[89] Article 2 (1) provides: "Everyone has the right to the free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or against morality."
[90] Volkszählungsurteil, *supra* note 80.

that treat individuals as mere conglomerations of transactional data, or that rank people… based on their financial or genetic desirability."[91]

The German Constitutional Court couched its concerns regarding modern methods of data processing that can result in treating the individuals as objects in similar terms. It noted that in order to reach a decision one can rely today on the technical means of storing information about personal or factual situations of an individual with the aid of automatic data processing. Furthermore, these data can be pieced together with other data collections –particularly when integrated information systems are built up - to add up to a partial or virtually complete personality profile ("Persönlichkeitsbild"), which normally the person concerned has no sufficient means of controlling its truth and application. According to the Court, these possibilities of inspection may influence the individual's behaviour by the psychological pressure exerted by public interest. Under conditions of modern information processing technology, individual self-determination presupposes that the person is left with the freedom of decision about actions that she should take or omit, including the possibility to follow that decision in practice. The Court opines that if someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu, and cannot estimate sufficiently the knowledge of parties to whom communication may possibly be made, he is crucially inhibited in his freedom to plan and decide freely, without being subject to any pressure or influence. The exercise of individual freedoms, such as freedom of speech or freedom of association and assembly is rendered excessively difficult when it is uncertain whether, under what circumstances, and for what purposes, personal information is collected and processed.[92] The right to informational self-determination, therefore, precludes a social order, in which the citizens no longer can know who knows what, when and on what occasion about them, as such would not only impair their chances of development, "but it would also impair the common good, because self-determination is an elementary functional condition of a free democratic community based on its citizens' capacity to act and to cooperate".[93]

The German Constitutional Court's reasoning on 'informational self-determination' is crucial for the definition and the understanding of the concept of

[91] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424 (2000).
[92] *See* Simitis, *Reviewing Privacy in an Information Society*, *supra* note 64, at 734.
[93] Volkszählungsurteil, *supra* note 80.

data protection. Following this path, the debate about data protection cannot be framed satisfactorily by referring merely to privacy, because the damage is not found, at the end of the day, in what we perceive as our private life or our private matters. Personal information is not necessarily private. Most importantly, the debate is not even about personal information. It is about the processing of this information.[94] Data protection, thus, is about power over the control over information,[95] which, in our age, is translated as "power over knowledge".[96] It has been pointed out that "the rush to capture ever-greater amounts of personally-identified information is premised on the assumption that this information will yield the ability to understand, and ultimately predict, individual behaviour... The view of human nature reinforced by data processing algorithms is both unforgiving and ungenerous."[97] The 'digital persona'[98] that emerges out of data processing presents such a powerful image of the individual, that it can be used as a "proxy for the real person".[99] In this sense, data processing may hold individuals accountable for whatever the combination of their information with powerful algorithms will reveal. In terms of commercial processing of data (e.g. consumer profiling, behavioural advertising, etc.), it has been argued that the evaluation of knowledge raises concerns about "behaviour modification and free will".[100] In terms of processing for law enforcement and counter-terrorism purposes, it could be about much more: discrimination, presumption of innocence, ultimately

---

[94] As Spiros Simitis notes "The processing is … seen as a challenge to human rights and the very structure of a democratic society." Spiros Simitis, *New Developments in National and International Data Protection Law*, RECENT DEVELOPMENTS IN DATA PRIVACY LAW : BELGIUM'S DATA PROTECTION BILL & THE EUROPEAN DRAFT DIRECTIVE 1, 17 (J Dumortier, 1992). *See* also Solove who explains "Information is not the key to power in the Information Age - knowledge is. Information consists of raw facts. Knowledge is information that has been sifted, sorted, and analyzed. The mere possession of information does not give one power; it is the ability to process that information and the capabilities to use the data that matters." Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1456 (2001).

[95] Bygrave argues that "information is increasingly being regarded as a valuable resource in itself. There exists a rapidly growing market in information services, a market in which information as such, and particularly personal data, can be bought and sold for significant financial sums." BYGRAVE, *supra* note 8, at 99.

[96] Jeffrey Rosen notes "Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge. True knowledge of another person is the culmination of a slow process of mutual revelation." JEFFREY ROSEN, THE UNWANTED GAZE : THE DESTRUCTION OF PRIVACY IN AMERICA 8 (1st Vintage Books ed. ed. 2001).

[97] Cohen, *supra* note 91, at 1408.

[98] The "digital persona" is a term used by Roger Clarke to describe "a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual." *See* Roger Clarke, *The Digital Persona and Its Application to Surveillance*, 10 THE INFORMATION SOCIETY 77 (1994).

[99] *Id.*

[100] Cohen, *supra* note 91, at 1408.

individual liberty. The concept of personal data protection is better understood as it was perceived by the German Constitutional Court: the right to 'informational self-determination' grounded on autonomy. This is the understanding of data protection that will be adopted here.

2.3 Dancing together apart: Privacy and data protection

Much ink has been spilt recently, after the constitutional entrenchment at the EU level of a right to data protection, on the exact nature of the relationship between privacy and data protection. The debate, which is live among European scholars, is concerned with the question whether data protection can be conceived as a "separate",[101] or an "autonomous"[102] fundamental right, "distinct"[103] from the right to privacy, or whether it should be regarded as a mere aspect of privacy. I do not wish to enter this discussion by focusing on terms such as the 'separateness' or the 'distinction' between the two rights, the more neutral assertion that privacy and data protection "interact in a variety of ways"[104] is more preferable here. That being said, a number of clarifications should be added on the issue.

First, we cannot lose sight of the EU constitutional reality: data protection has been enshrined as a fundamental right, alongside with privacy in the EU Charter of Fundamental Rights, which constitutes primary EU law. This means that, in the European constitutional context at least, data protection is considered (or expected) to add something to privacy. Whether this is the case, in the law enforcement context, is the question that the present research attempts to explore.

Second, we cannot lose sight of the historical reality: data protection legislation is a relative newcomer; it only appeared on the scene in the seventies as a response to the concerns raised about the increasingly centralized processing of

[101] NICOLAS SCANDAMIS ET AL., RIVAL FREEDOMS IN TERMS OF SECURITY: THE CASE OF DATA PROTECTION AND THE CRITERION OF CONNEXITY 15 (CEPS, CHALLENGE, Research Paper No. 7, December 2007).
[102] Rodotà, *supra* note 14, at 79.Rodota notes: "In 2000, the Charter of Fundamental Rights of the EU recognised data protection as an autonomous right. This can be considered the final point of a long evolution, separating privacy and data protection."
[103] Gloria González Fuster, Paul de Hert and Serge Gutwirth comment: "The right to privacy has been flanked in Europe with another, distinct right: the right to the protection of personal data." GLORIA GONZÁLEZ FUSTER ET AL., THE LAW-SECURITY NEXUS IN EUROPE: STATE-OF THE-ART REPORT 10 (INEX WP2 D2.1).
[104] Rouvroy & Poullet, *supra* note 34, at 69.

personal data and the establishment of huge data banks.[105] The first piece of data protection legislation was enacted in 1970 by the German state of Hesse.[106] It was followed by Sweden in 1973[107] and, subsequently, by other European countries.[108] In most of the cases, legislators opted out to legitimize the data protection regulation by simply referring to traditional privacy concepts.[109] As it has been pointed out, "provisions proclaiming the right to privacy or private life constitute the most direct inspiration for the principles of data protection laws."[110] On the other hand, to rephrase Spiros Simitis, privacy is "an old and venerable" [111] right, entrenched for many years as a fundamental right in national constitutions and international texts.

Nevertheless, privacy and data protection are not identical rights. On the one hand, data protection seems to fall in this aspect of privacy that is known, as seen above, as control over personal information. However, "what privacy protects is irreducible to personal information."[112] Privacy is a much broader concept that embodies a range of rights and values, such as non interference or the right to be let alone, limited access to oneself, intimacy, seclusion, personhood, and so on according to the various definitions.[113]

On the other hand, as the Court of First Instance (CFI) (now: General Court) rightly observed in *Bavarian Lager*[114] not all personal data are necessarily 'private':

> "It should be emphasised that the fact that the concept of 'private life' is a broad one, in accordance with the case-law of the European Court of Human Rights, and that the right to the protection of personal data may

[105] Bygrave aptly notes: "The emergence of data protection laws, along with their continued existence, cannot properly be explained without taking account of developments in information technology … particularly from the onset of the computer age in the 1950s. BYGRAVE, *supra* note 8, at 93. *See* also Simitis, *New Developments in National and International Data Protection Law*, *supra* note 94, at 22.
[106] Datenschutzgesetz, Oct. 7, 1970, § 6, 1 Gesetz- und Verordnungsblatt für das Land Hessen 625 (1970). For the history and development of the law, *see* Spiros Simitis, *Datenschutzrecht*, HESSISCHES STAATS- UND VERWALTUNGSRECHT: (HESSSTVWR) 111, 114 (Hans Meyer & Michael Stolleis, 2. Aufl. ed. 1986). *See* also HONDIUS, *supra* note 79, at 35.
[107] Datalagen (Swedish Data Act) of May 11, 1973, entered into force July 1, 1973.
[108] Austria (Federal Act of October 18, 1978 on the protection of personal data, Bundesgesetzblatt No. 565/1968); Denmark (Public Authorities Registers Act, No. 294 (1978), and Private Registers Act No. 293 (1978); France (Act 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties, [1978] J.O. 227); West Germany (Federal Data Protection Act, [1977] BGB1 I 201); Norway (Act of June 9, 1978 relating to Personal Data Registers).
[109] Simitis, *Reviewing Privacy in an Information Society*, *supra* note 64, at 730.
[110] BYGRAVE, *supra* note 8, at 116.
[111] Simitis comments: "Privacy is an old and venerable subject." Simitis, *Reviewing Privacy in an Information Society*, *supra* note 64, at 707.
[112] Rouvroy & Poullet, *supra* note 34, at 70.
[113] Christopher Kuner, *An International Legal Framework for Data Protection: Issues and Prospects*, 25 COMPUTER LAW & SECURITY REVIEW 307, 309 (2009).
[114] Case T-194/04 *Bavarian Lager*, judgment of the Court of First Instance of 8 November 2007.

> constitute one of the aspects of the right to respect for private life , *does not mean that all personal data necessarily fall within the concept of 'private life.'* A fortiori, *not all personal data are by their nature capable of undermining the private life of the person concerned.*"[115]

A different approach is very problematic as the UK case *Durant v. Financial Services Authority*[116] demonstrates. This case concerned an individual's request to access certain files containing information about a litigation he had with his bank. The Court of Appeals rejected his request on the basis that such information did not constitute personal data, because personal data personal data is only information which is

> "biographical in a significant sense; has to have the individual as its focus; and has to affect an individual's privacy whether in his personal family life, business or professional activity."[117]

Such a restrictive view of personal data cannot be accepted here. Personal data is information relating to an identified or identifiable individual and not information that might affect an individual's private life. This means that data protection and privacy are not exactly the same thing.

Furthermore, data protection is more than informational privacy itself because, as it will be demonstrated below, it serves other, further fundamental rights and values besides privacy.[118] At the same time, data protection applies to the processing of personal data, which often are hardly considered as private, a problem that was identified above, when the control over personal information theory of privacy was discussed. Furthermore, as Polcak points out:

> "Although the protection of personal data derives its basic legitimacy from the privacy protection and it is declared as protective of rights of individual persons, it does not use any *subjective* elements in constructing the limits and/or the grounds for remedies. The purely *objective* nature arises out of the fact that the protection of personal data is positioned by the European lawmakers into the

---

[115] *Id.* paras 118-119. Emphasis added.
[116] *Durant v. FSA* [2003] EWCA Civ 1746, Court of Appeal (Civil Division). For a comment *see* among others Lilian Edwards, *Taking the "Personal" Out of Personal Data: Durant v FSA and Its Impact on the Legal Regulation of CCTV*, 1 SCRIPT-ED 341 (2004).
[117] *Id. See* also Mario Viola de Azevedo Cunha et al., *Peer-to-Peer Privacy Violations and ISP Liability: Privacy Violations in the User-Generated Web*, INTERNATIONAL DATA PRIVACY LAW (2011).
[118] Serge Gutwirth & Mireille Hilderbrandt, *Some Caveats on Profiling*, DATA PROTECTION IN A PROFILED WORLD 31, 36 (Serge Gutwirth et al., 2010); UK INFORMATION COMMISSIONER, THE LEGAL FRAMEWORK: AN ANALYSIS OF THE "CONSTITUTIONAL" EUROPEAN APPROACH TO ISSUES OF DATA PROTECTION LAW 6 (Study Project).

area of public administrative law and that the standard of protection should not substantially differ across the Europe."[119]

This distinction between the subjective nature of privacy and the more objective nature of data protection can be generalised beyond the borders of the EU for a further reason: Unlike privacy's elusive and subjective nature that makes the right different in different contexts and jurisdictions, data protection has an essential *procedural* nature that it makes it more objective as a right in different contexts.[120]

2.4 Underlying values behind data protection

2.4.1 The case for privacy

It is not questioned that privacy is "one –if not *the*- major" [121] value that data protection laws aim to safeguard. A look in the first Article of both the Convention No. 108 of the Council of Europe[122] and the Data Protection Directive[123] confirms this. Other international data protection instruments, such as the UN and the OECD Guidelines, also stress the link between data protection and privacy, but remain, however "rather *unclear* about the precise nature of this link."[124] Moreover, national data protection texts or their *travaux préparatoires* refer to the right to privacy as one of the main aims[125] of their data protection legislation.[126] Paradoxically enough, though, as it has been pointed out, privacy is "never directly defined in those data

[119] Radim Polcak, *Aims, Methods and Achievements in European Data Protection*, 23 INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 179, 181 (2009). Emphasis added.
[120] *See* BENNETT & RAAB, *supra* note 23, at 8.
[121] BYGRAVE, *supra* note 8, at 125.
[122] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), adopted at 28.1.1981, entered into force 1.10.1985. Article 1 provides: "The purpose of this Convention is to secure in the territory of each Party for every individual,… respect for his rights and fundamental freedoms, and in particular his right to *privacy*, with regard to automatic processing of personal data relating to him ("data protection")."
[123] Article 1 (1) of Directive 95/46/ EC reads as follows: "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their *right to privacy* with respect to the processing of personal data."
[124] UK Information Commissioner, *supra* note 118, at 4.
[125] Writing on national data protection rules in Europe, Hondius contends that "Privacy plays a certain role in all the laws, but never a dominating one." *See* Frits W. Hondius, *Data Law in Europe*, 16 STAN. J. INT'L L. 87, 94–95 (1980).
[126] BYGRAVE, *supra* note 8, at 116; Simitis, *Reviewing Privacy in an Information Society*, *supra* note 64, at 730; Hondius, *Data Law in Europe*, *supra* note 125, at 92–93.

protection laws that employ the term", and therefore its "meaning for the purposes of data protection law must be sought partly in the substance of the principles laid down in the laws themselves, partly in the way those principles have been applied, and partly in general, societal notions of what privacy is."[127] The fact that the concept of privacy is somewhat elusive is not regarded as necessarily negative; on the contrary, it has been argued that this elusiveness enables data protection rules "to assimilate and express in a relatively comprehensive, economic manner the congeries of fears attached to increasingly intrusive data-processing practices."[128]

Be that as it may, it is not quite clear which of the various conceptions of privacy data protection laws aim to advance. Informational control is the concept of privacy regarded as the closest to data protection. However, as mentioned above, the control-over- personal information theory is not without problems. What is 'control', what is 'personal information' and where does control derive from? Is control to be understood as "ownership of information"?[129] Does control- over- information mean that privacy is only a "subjective matter of individual prerogative"[130] that can be disposed freely? Or is there, in certain cases, also a societal interest to protect privacy independent of the preferences of the individual? While it is outside the purposes of the thesis to enter this debate on privacy, some of the above questions are pertinent also in the data protection context, hence a number of clarifications are necessary.

First, it should be emphasised that what is protected by data protection rules is the informational self-determination, not some form of ownership over personal data.[131] Justifying data protection on property theories is as problematic as explaining the control-over- information privacy conceptions with reference to property rights.[132] First, the utility and the added value of an ownership approach is dubious, because property rights do not enjoy any kind of elevated protection and are not considered absolute in any case.[133] More importantly, property approaches to data protection

---

[127] Lee Bygrave, *The Place of Privacy in Data Protection Law*, 24 UNIVERSITY OF NEW SOUTH WALES LAW JOURNAL 277, 278 (2001).
[128] BYGRAVE, DATA PROTECTION LAW, *supra* note 8, at 127.
[129] Westin argues that "personal information, thought of as the right of decision over one's private personality, should be defined as a property right." WESTIN, *supra* note 66, at 324. For a more recent analysis on why privacy is better protected by property rights *see* Lawrence Lessig, *Privacy As Property*, 69 SOCIAL RESEARCH: AN INTERNATIONAL QUARTERLY 247 (2002).
[130] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 11, at 25.
[131] Theories of ownership have been also proposed in the context of personal data too. *See* BYGRAVE, DATA PROTECTION LAW, *supra* note 8.
[132] For the problems, *see* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 11, at 25.
[133] BYGRAVE, DATA PROTECTION LAW, *supra* note 8, at 120.

could be perilous. This is because property theories argue in favour of a commodification of personal data. Granting property rights on personal data means that they can be viewed as a commodity and become tradable. The argument goes, therefore, that from the moment the data are placed on the market, it is the market that is supposed to achieve the ideal amount of privacy protection by balancing the value of personal information to the potential buyers against the value of the information to the individual.[134] The market solution has serious deficiencies, however, because, on the one hand, it is difficult to ascribe a value to personal data; [135] and, on the other, a market approach can lead to inequalities. As Cohen notes correctly: "Personally-identified data is the wedge that enables "scientific," market -driven, and increasingly precise separation of "haves" from "have-nots"."[136] On the other hand, it is not accepted either that data controllers[137] enjoy property rights on information systems or the data contained therein, because they have invested in compiling the databases and developing algorithms to process the information.[138] The issue of whether data protection can be regarded as a subjective matter of individual preference that can be freely disposed by the individual, brings into question the notion of 'consent', and will be discussed later in the thesis. Suffice it to note in the context of the present debate, that rights are not "mere individual possessions",[139] that can be freely disposed, but they hold an importance for the society as a whole.

Although control-over- personal information is viewed as the conception of privacy predominantly advanced by data protection rules,[140] it would be mistaken to consider that it is the sole privacy concept behind data protection laws. Such an approach would narrow excessively the ambit of data protection, and in any case it is not followed by most data protection regulations. Data protection principles, thus, embody further privacy concerns –besides informational privacy- such as 'the right to be let alone' or privacy as non-interference, limited access to oneself, and even

---

[134] Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, *supra* note 94, at 1446–1447.
[135] For a detailed analysis on the deficiencies of the market solution *see Id.* at 1452–1453.
[136] Cohen, *supra* note 91, at 1378.
[137] Data controllers are in charge of the collection, storage, processing, use and dissemination of personal data.
[138] Cohen, *supra* note 91, at 1378.
[139] Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, *supra* note 94, at 1455.
[140] As Bygrave notes "In data protection discourse, … the most popular definitions of privacy are in terms of information control." BYGRAVE, DATA PROTECTION LAW, *supra* note 8, at 130.

conceptions of privacy such as intimacy (for instance in the processing of sensitive personal data).[141]

Privacy may well be the main value that data protection laws aim to safeguard, but there is a huge discussion on whether privacy itself has an 'intrinsic' or an 'instrumental' value, that is, whether it is valuable in itself,[142] or it aims to pursue other further interests and values. With most authors accepting that privacy does not have an intrinsic value in itself, but advances further values, the next question that arises is which are these.[143] Privacy has been viewed to promote a range of interests and values, from autonomy, integrity,[144] dignity,[145] individuality,[146] to self-realisation[147] and interpersonal relationships of love, friendship and trust. [148]

The debate is not without importance for data protection purposes as well. It has been argued above, that in terms of data protection it is more correct to speak about informational autonomy, as the capacity of the individual to decide for himself the disclosure and use of his personal data, than informational privacy. This approach that considers autonomy as an underlying value of data protection is based on a democratic claim – or what has been called as the "republican perspective on data protection rights."[149] According to this, informational self-determination promotes the value of democracy. The German Constitutional Court has followed this approach in its seminal Census decision. In the literature, Spiros Simitis couches aptly the democratic argument in the data protection discourse. Simitis argues:

> "If, as Jefferson suggests, democratic participation presupposes constant interaction between public and private life, the protection of privacy must be accompanied by an equally efficient, guaranteed access to the information necessary to follow and evaluate social processes… Social discourse depends on an information allocation policy that, through a mix of withholding and access,

---

[141] *Id.* at 132–133.
[142] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 11, at 84.
[143] There are further questions as well on what ways privacy safeguards those values, that is whether it is the "necessary prerequisite for realizing the value" or "simply a factor that enhances the likelihood of realization". *See* BYGRAVE, DATA PROTECTION LAW, *supra* note 8, at 133.
[144] Fried, *Privacy*, *supra* note 68, at 477–478.
[145] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1003 (1964).
[146] Reiman, *supra* note 44, at 26.
[147] WESTIN, *supra* note 66, at 39.
[148] INNESS, *supra* note 45, at 95.
[149] BYGRAVE, DATA PROTECTION LAW, *supra* note 8, at 136.

reflects a precise analysis and understanding of the consequences of automated processing for both the individual and society."[150]

In the context of the democratic argument, an ownership approach to personal data is rejected:

> "The contrary result is achieved, … when privacy protection is more or less equated with an individual's right to decide when and which data are to be accessible. The regulation thus reverts to well-known property schemes and leads to the division and monopolization of personal information. Public and private life are irrevocably disconnected. Open or hidden "sanctifications" of property sacrifice the *citoyen* and reduce the *constitutio libertatis* to a mere guarantee of the *bourgeois'* refuge."[151]

2.4.2 The case for data security and data quality

Privacy may well be the main value behind data protection rules, but data protection legislation advances further interests. As Raab and Bennett note "to protect privacy and to protect data protection are not identical aims; the second may lead to the former, but it also achieves other purposes that may or may not be compatible with the protection of privacy."[152] A set of interests that data protection laws aim to safeguard, further to privacy, concerns the security of the information systems ('data security') and the quality of data contained therein ('data quality').

'Data security' is the interest of keeping the data secure against certain risks, such as the risks of data being lost or accessed by unauthorized persons. In this regard, the Data Protection Directive requires data controllers to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network. The measures should ensure a level of security appropriate to the risks represented by the processing and the nature of the data.[153] Furthermore, the Directive obliges the controllers to

---

[150] Simitis, *Reviewing Privacy in an Information Society*, *supra* note 64, at 735.
[151] *Id.* at 736.
[152] Raab & Bennett, *supra* note 19, at 537.
[153] Article 17 (1) of the Data Protection Directive. A relevant provision is found in Article 7 of the Council of Europe Convention No. 108.

choose a processor that provides sufficient guarantees of technical and organizational security with respect to the processing.[154] Clarke points out that 'data security' is not rarely confounded with 'data privacy', as security specialists and computer scientists, especially in the United States tend to understand data protection as referring solely to the security of personal data against unauthorised disclosure and accidental losses.[155] The general public often follows the same misconception, and increased concerns on data protection issues are normally raised when a case of unwarranted access or loss of personal data is brought into light by the media.[156] 'Data security', however, is only an interest safeguarded by data protection laws, and should not be confused with data protection itself. As some commentators correctly note, "data security is a necessary but not a sufficient condition for information privacy".[157] Personal data may well be kept secure, but if they should not have been collected in the first place, or they are unlawfully processed, data protection principles are nevertheless violated.

'Data quality' is the interest that refers to the accuracy, adequacy, relevance and up-to-dateness of the personal information.[158] Personal information that is accurate, adequate and up to date does not safeguard solely the interests of data controllers that would be in principle able to make more accurate decisions based on valid, adequate and relevant data. It equally promotes the interests of the data subjects as inaccurate information held on them, means concomitantly inaccurateness in the sketching of the 'digital persona' of the individuals. For this reason, the Data Protection Directive stipulates that every reasonable step should be taken to ensure that data which are inaccurate or incomplete are erased or rectified.[159]

The Data Protection Directive couches both the data security and the data quality principles as obligations imposed on the data controllers, i.e. on the persons, public authorities, enterprises, agencies or other bodies that are responsible for data processing.[160] However, as already mentioned, data security and even more data quality serve the interests of data controllers as well.

---

[154] Article 17 (2) of the Data Protection Directive.
[155] Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*.
[156] *Id.*
[157] BENNETT & RAAB, *supra* note 23, at 11.
[158] Article 6 (1) (c) and (d) of the Data Protection Directive.
[159] Article 6 (1) (d) of the Data Protection Directive.
[160] Recital 25 of the Data Protection Directive.

2.4.3 The case for transparency and due process

Writing on computer databases, Daniel Solove argued that the Big Brother metaphor, that is often used by journalists, politicians, jurists, and legal academics to describe the privacy problem created by the collection and use of personal information through information systems is the wrong paradigm, and the metaphor of Franz Kafka's The Trial should be used instead because it depicts in the correct terms the problems posed by databases to data privacy.[161] According to Solove, the problems caused by the collection and storage of information in databases should not be couched on terms of surveillance, because databases do not "uncover one's hidden world", nor they "disclose concealed information".[162] On the contrary, the problem posed by databases is the powerlessness, vulnerability, and dehumanization created by the assembly of dossiers of personal information where individuals lack any meaningful form of participation in the collection and use of their information.[163] Whether Orwell's Big Brother or Kafka's Trial depicts better the problem posed by information systems will be discussed later in the thesis, in the chapter that deals with the exchange of information through EU's centralized databases. Solove's paradigm, however, is useful here, to the extent that it aptly describes one of the major concerns that data protection laws attempt to address: the relative inability of individuals to control what information is being collected on them and how this will be further used. Reading Solove's argument in this context, the Big Brother metaphor would more closely express the privacy concerns behind data protection regulation, while The Trial would explain the needs for transparency, accountability and foreseeability in the processing of personal data. In this sense, the two paradigms are not mutually exclusive; rather, they complement each other by accounting for the different values and purposes of data protection laws.

The processing of personal data bears inherent imbalances. These are manifest in the asymmetries between the two main actors of information processing: the data subject, on the one hand, and data controllers on the other hand. In terms of the Big Brother metaphor, and expressed more forcefully by Jeremy Bentham's

[161] Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, *supra* note 94, at 1426.
[162] *Id.* at 1437.
[163] *Id.* at 1423.

'panopticon'[164] as expounded by Michel Foucault,[165] the informational imbalance results in a form of social control: the observed are rendered virtually transparent to the observers, without the same applying *vice- versa.*[166] Drawing from Kafka's Trial as read by Solove, the imbalance between data subjects and data controllers is found somewhere else: data subjects lack means of meaningful control and participation over the processing of their personal data. Combining the two metaphors together in the light of the use of new information technologies, it has been argued that we are facing a situation where "a) there is virtually no limit to the amount of Information that can be recorded, b) there is virtually no limit to the scope of analysis that can be done- bounded only by human ingenuity and c) the information may be stored virtually forever."[167]

Data protection rules attempt to address this problem[168] by embodying the values of transparency, foreseeability in data processing, accountability of data controllers, and –to the extent that it is possible- participation of the data subject in the processing of his/ her information. These values are voiced in a number of fair information principles; above all, in the principle of fair and lawful processing, in the purpose specification principle, and in the individual participation principle.

The principle of 'fair and lawful' processing[169] expresses a number of the above mentioned data protection values. It strives, above all, for transparency in data processing and, thus, establishes (indirectly) a level of accountability of data controllers. That the processing should be lawful, is quasi self-explanatory, it should

---

[164] The 'Panopticon' was a prison building developed by philosopher and social theorist Jeremy Bentham. The design of the prison aims to allow the observers to observe all the prisoners without the latter being able to tell whether and by whom they are being watched.

[165] Foucault invoked Bentham's 'Panopticon' as a metaphor of modern disciplinary societies. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH : THE BIRTH OF THE PRISON 195 (2. Vintage Books ed. ed. 1995).

[166] *See* BYGRAVE, DATA PROTECTION LAW, *supra* note 8, at 109.

[167] Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW AND PHILOSOPHY 559, 576 (1998).

[168] In a very interesting analysis, Herbert Burkert argues: "Data protection (privacy protection) may not only be about protecting a perhaps old fashioned and perhaps too rigid and too inflexible socio-psychological concept of the "self". Data protection legislation may even not only be about the right to informational self-determination (or at least co-determination) in an age of local, regional, national and international social and economic dependencies but data protection (privacy protection) may also - and perhaps essentially so - be about the distribution of power within and between societies, addressing conflicts of power in such constellations by reframing them as informational and communicative power conflicts. Data protection (privacy) legislation - in this understanding would then seek to de-legitimize asymmetries of information distribution and aim at more equitable distribution patterns in the interest of individual freedoms and democratic participative structures." *See* Herbert Burkert, *Towards a New Generation of Data Protection Legislation*, REINVENTING DATA PROTECTION? 335, 339 (2009).

[169] *See* Article 6 (1) (a) Data Protection Directive; and, Article 5 (a) Convention No. 108.

be carried out in accordance with the law. Fairness is a more difficult notion to understand. In general, fairness in processing denotes that data controllers must make sure that the collection and processing of personal data is undertaken in accordance with the reasonable expectations of the data subjects; this seen from the point of view of the data subject, it means that the processing should be made transparent for the individuals whose personal data are being processed, in that they should be able to know the purposes of the collection and processing of their personal data. [170]

The interests of foreseeability and predictability of processing are echoed in the 'purpose specification principle'. 'Purpose specification' requires that personal data must be collected for specified, explicit and legitimate purposes and should not be further processed in a way incompatible with the initial purposes.[171]

Fair information principles, such as 'fair and lawful processing' and 'purpose specification' aspire to provide the data subject with meaningful control over the processing of his personal information, by taking account of the interests of transparency, foreseeability and accountability of data processing. To address further the asymmetries and power imbalances between data subjects and data controllers, data protection regulations attempt to grant the former some form of participation in the processing of their personal data. The 'due process' concerns in the processing of personal data normally find their expression in the so-called 'individual participation' principle.[172] The principle is manifested in a variety of data protection rules: certain processing operations cannot be undertaken without the consent of the data subject;[173] data subjects are given the right to know that information is held on them by others;[174] they have the right to access it;[175] and correct it if it is inaccurate or misleading.[176]

2.4.4 The case for non-discrimination

There is a further value safeguarded by data protection rules that goes well beyond the above categories of interests and should, thus, be mentioned separately:

---

[170] BYGRAVE, DATA PROTECTION LAW, *supra* note 8, at 58–59.
[171] *See* Article 6 (1) (b) Data Protection Directive; and, Article 5 (b) Convention No. 108.
[172] *See* for instance OECD Guidelines, para 13.
[173] *See* for instance Articles 7 (a) and 8 (2) (a).
[174] *See* Article 10 Data Protection Directive; and, Article 8 (a) Convention No. 108.
[175] *See* Article 12 (a) Data Protection Directive; and, Article 8 (b) Convention No. 108.
[176] *See* Article 12 (b) Data Protection Directive; and, Article 8 (c) Convention No. 108.

the principle of non-discrimination. The principle, which prohibits the different or unequal treatment of individuals based on their personal characteristics, is particularly pertinent for data protection regulations that aim to grapple with certain processes, such as profiling,[177] which can be discriminatory. The concern of data protection legislation for the principle of non-discrimination is, above all, manifest in the rules that require the additional protection of the processing of special categories of data that are normally described as 'sensitive'. Personal data that reveal racial or ethnic origin, political opinions, religious beliefs, sexual orientation and health, are made subject to enhanced protection, and their processing is in principle prohibited as a default rule in the European Data Protection context.[178] This is because the processing of such data can lead to illegal discrimination.[179] Concerns about discriminatory processes are also manifest in provisions, such as Article 15 of the European Data Protection Directive aimed at protecting individuals against fully automated decision making.[180]

2.4.5 The case for proportionality?

While it might be wrong to regard the proportionality principle as an autonomous value pursued by data protection laws, proportionality concerns run through data protection legislation, as they are manifest in several fair information principles, and they "underpin" the operation of most of these principles.[181] Direct references to the principle of proportionality can be found in the rules that require that

---

[177] *See* below.

[178] Article 8 (1) Data Protection Directive stipulates "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life." The processing of these special categories of data is allowed when the conditions of Article 8 (2) are met. Similarly, Article 6 of Convention No. 108 provides "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."

[179] *See* Rouvroy & Poullet, *supra* note 34, at 70.

[180] Article 15 (1) of the Data Protection Directive provides "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."

[181] Lee Bygrave & Dag Wiese Schartum, *Consent, Proportionality and Collective Power*, REINVENTING DATA PROTECTION? 157, 162 (2009).

personal data should be "relevant" and "not excessive" in relation to the purposes for which they are collected and further processed;[182] that they are "necessary";[183] and, that they are kept for no longer than is necessary for the purposes for which the data were collected or further processed.[184] But, as it has been correctly pointed out, the proportionality principle, albeit not directly mentioned, it is "manifest in the criterion of "fairness" inherent in the bulk [of the fair information] principles."[185] In essence, 'fairness' in processing of personal data "undoubtedly connotes proportionality in the balancing of the respective interests of data subjects and controllers."[186]

3. A Fundamental Right to Data Protection?

3.1 Approaches to Data Protection

It was mentioned above that data protection suffers from a kind of schizophrenia; this is all the more evident in the debate about its exact nature. While understanding the concept of data protection might have seemed relatively easy, there is confusion on how data protection should be perceived. Is data protection a human right? Is it a factor of economic growth? Is it a consumer concern?[187] Or it can be simply seen as a "problem of trust" over the security of personal information?[188] There

[182] *See* Article 6 (1) (c) Data Protection Directive.
[183] *See* Article 6 (1) (d) Data Protection Directive.
[184] *See* Article 6 (1) (e) Data Protection Directive.
[185] Bygrave & Schartum, *supra* note 181, at 162.
[186] *Id.* at 163.
[187] This approach is followed in the APEC Privacy Framework (available at < http://www.dpmc.gov.au/privacy/apec/apec_privacy_framework.cfm>, [accessed 30.04.2011]). The Framework contains nine Privacy Principles: 1) Preventing Harm; 2) Notice; 3) Collection Limitations; 4) Uses of Personal Information; 5) Choice; 6) Integrity of Personal Information; 7) Security Safeguards; 8) Access and Correction; and, 9) Accountability. The Framework also contains guidance on international implementation between member economies. Three key issues are identified for international implementation: information sharing between economies on privacy issues; developing arrangements for cross-border cooperation in investigation and enforcement; and the cooperative development of a system for the use by business of Cross-Border Privacy Rules (CBPRs). In general, the APEC Framework avoids to use the word 'right' for data privacy. *See* also, Cécile de Terwangne, *Is a Global Data Protection Regulatory Model Possible?*, REINVENTING DATA PROTECTION? 175, 181, 183–185.
[188] This was the approach adopted by the World Summit on the Information Society in its Declaration of Principles (Declaration of Principles - Building the Information Society: a global challenge in the new Millennium, Document WSIS-03/GENEVA/DOC/4-E, Geneva, 12 December 2003). According to

are different ways of approaching data protection[189] and the debate is not without practical consequences on the content of the notion. Below, the two main approaches to data protection, the economic approach and the human rights' approach will be discussed. The OECD privacy regulatory framework will be used as an example of the former, the EU of the latter. However, it should be wrong to assume that the two approaches are mutually exclusive, or that there is a clear delineation between them in the two regulatory regimes that will be investigated.

3.2 The economic approach to Data Protection

A good example of the economic approach to data protection are the OECD Privacy Guidelines. The aim of the Organisation for Economic Co-operation and Development (OECD) is to promote policies that will improve the economic and social well-being. It is an economic organisation that measures productivity and global flows of trade and investment, carries out analysis mainly in economic matters, and is not involved in human rights activities. It attempts to promote rules and set international standards in many areas, such as, for instance, development, education, employment, energy, environment, finance, investments, science and technology, taxation and trade.

In a symposium organized by the OECD in 1977 on "Transborder Data Flows and the Protection of Privacy", the economic value and national interest of transborder data flows was discussed by the participants. In a comment made by Louis Joinet, who participated later in the drafting of the OECD Guidelines, it was noted:

> "Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows."[190]

---

this approach, data protection coincides with data security, and security breaches are the problems to be dealt with.

[189] For an analysis of the different regulatory regimes worldwide *see* ABRAHAM NEWMAN, PROTECTORS OF PRIVACY : REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY (2008).

[190] Louis Joinet as quoted in John Eger, *Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non- Tariff Barriers?*, 10 LAW AND POLICY IN INTERNATIONAL BUSINESS 1065, 1066 (1978).

Following the symposium, an Expert Group was created to begin work on the privacy guidelines. The main aim was to tackle the concerns about the growing use of personal data and the computerised processing. But, given OECD's mandate to foster economic growth and contribute to the expansion of world trade, a further aim was to prevent national laws from creating barriers to the free flow of information that would impede growth.[191] Thus, the emphasis on ensuring that the measures being introduced to protect personal data would not result in restrictions on transborder data flows runs through the Guidelines, which were adopted on 23 September 1980.[192]

The Guidelines contain eight fair information principles:

1) Collection Limitation Principle;
2) Data Quality Principle;
3) Purpose Specification Principle;
4) Use Limitation Principle;
5) Security Safeguards Principle;
6) Openness Principle;
7) Individual Participation Principle; and,
8) Accountability Principle.

The purpose of the OECD information principles is twofold: advance the free flow of information and avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries.[193] For this reason, data protection is considered as a factor fostering international economic aims, by facilitating the free and unimpeded transfers of personal information.[194]

---

[191] *See* WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, THE EVOLVING PRIVACY LANDSCAPE: 30 YEARS AFTER THE OECD PRIVACY GUIDELINES 10 (OECD Digital Economy Paper 176, April 30, 2011), *available at* http://www.oecd.org/officialdocuments/displaydocumentpdf/?cote=dsti/iccp/reg(2010)6/final&doclanguage=en.

[192] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at < http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html> [accessed 30.04.2011]). The OECD Privacy Guidelines are not legally binding.

[193] *See* OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), available at < http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html> [accessed 30.04.2011]).

[194] *See* Sjaak Nouwt, *Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union*, REINVENTING DATA PROTECTION? 275, 278.

3.3 The EU Approach: Data Protection as a Fundamental Right

Conceiving data protection as a human right is not unique only in the European Union legal context. A series of other international instruments, such as the UN Guidelines on Computerised Data Files[195] and the Council of Europe Convention No. 108 for the protection of individuals with regard to automatic processing of personal data, adopt the same 'human rights' approach to personal data protection. What's more, the EU is not a human rights organisation itself, as the Council of Europe. It was born as an economic union, and while it has gone a long way from that, still, its more important competences are of economic nature. In this respect, it reminds the OECD that pursues economic purposes. So, against this background, why does the EU constitute the most comprehensive (at least at the international level) 'human rights' approach to data protection? For two reasons: First, because data protection is recognized as a fundamental right in primary EU constitutional law, and, second, because, for the first time at the international level, data protection is 'disassociated' from the right to privacy, in that it is not any longer regarded as a human right, insofar as it can be seen as an aspect of privacy. This approach is followed, for instance, by the Council of Europe Convention No. 108, which in Article 1 describes its object as securing for every individual "respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."[196]

The evolution of data protection to a fundamental right within the EU legal order has its own history. Let us unravel the thread from the triumphant end:[197] Data protection is enshrined as a fundamental right in Article 8 of the EU Charter of Fundamental Rights (EUCFR).[198] The EUCFR enjoys the status of EU primary law

---

[195] Guidelines for the Regulation of Computerized Personal Data Files (DocE/CN.4/1990/72, 20 February 1990) adopted by General Assembly resolution 45/95 of 14 December 1990, available at < http://www.unhcr.org/refworld/docid/3ddcafaac.html> [accessed 1 May 2011]

[196] A similar approach is followed by the UN Privacy Guidelines.

[197] De Hert and Gutwirth note: "Very recently, the proper role of data protection has received constitutional recognition…" Paul De Hert & Serge Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, PRIVACY AND THE CRIMINAL LAW 61, 81 (Erik Claes et al., 2006).

[198] Charter of Fundamental Rights of the European Union proclaimed on 7 December 2000 in Nice (OJ C 364/1). The right to privacy is found in Article 7 EUCFR. For a commentary on the Articles of the Charter *see* EU NETWORK OF INDEPENDENT EXPERTS ON FUNDAMENTAL RIGHTS, COMMENTARY OF THE EU CHARTER OF FUNDAMENTAL RIGHTS (2006).

pursuant to Article 6 (1) TEU, [199] since the Lisbon Treaty entered into force as from December 1, 2009. Article 8 of the Charter provides as follows:

> "1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority."[200]

This might be the happy end, but the Cinderella story of data protection within the EU is not that romantic.[201] Let us now go to the beginning. Directive 95/46/EC, also known as the 'Data Protection Directive' was the first piece of legislation adopted in the EU on the protection of personal data.[202] The Directive had two objectives: harmonise the different national rules on data protection, and ensure simultaneously the free movement of such data.[203] Data protection, hence, at its birth in the EU, was no more than an internal market concern, not bearing many differences from the economic approach of the OECD Guidelines analysed above. Fundamentals

---

[199] Article 6 (1) TEU provides: "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties."

[200] For a detailed analysis of Article 8 EUCFR *see* BIRTE SIEMEN, DATENSCHUTZ ALS EUROPÄISCHES GRUNDRECHT (2006).

[201] Writing on the UK Data Protection Act, Diane Rowland comments that "although frequently now discussed in terms of the rhetoric of rights, the original objectives of data protection rules were arguably much less aspirational. The Data Protection Act 1984 was enacted not so much as to provide fundamental rights for data subjects, as to protect Britain's international trade which was feared to be under threat if the Council of Europe Convention on the protection of personal data could not be ratified." Diane Rowland, *Data Retention and the War Against Terrorism – A Considered and Proportionate Response?*, 3 THE JOURNAL OF INFORMATION, LAW AND TECHNOLOGY (JILT), 3 (2004).

[202] For an analysis of the EU legal framework *see* Maria Tzanou, *Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence*, PERSONAL DATA PRIVACY AND PROTECTION IN A SURVEILLANCE ERA: TECHNOLOGIES AND PRACTICES 273, 273 (Christina Akrivopoulou & Athanasios Psygkas, 2011).

[203] Article 1 of the Data Protection Directive.

rights and market freedoms were placed at the same footing under the Directive.[204] In this respect, Recital 3 of the Directive states that:

> "… the establishment and functioning of an internal market in which … the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded."

On the one hand, insofar fundamental rights are concerned, the Directive explains:

> "… the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; … this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law… in order to remove the obstacles to flows of personal data the level of protection of the rights and freedoms of individuals… must be equivalent in all Member States… "[205]

On the other hand, if equivalent protection of fundamental rights is achieved, it is expected that the free movement of data will be rendered possible:

> "… given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to the protection of the rights and freedoms of individuals, and in particular the right to privacy…"[206]

But, it is not only that data protection was born out of internal market, economic concerns; its concept was uncertain as it was recognised as a dimension of privacy and its protection was dependent on it. According to the Data Protection Directive:

[204] This can be seen also at the title of the Directive: "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data."
[205] Recitals 7 and 8 of the Data Protection Directive.
[206] Recital 9 of the Data Protection Directive.

"…the object of the … laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the ECHR and the general principles of Community law…"[207]

Now that the story is told, we are faced with the paradox of data protection. Why a fundamental right's approach to data protection? How is the 'happy ending' to be explained after the conditions of the genesis?

The Explanations to the Charter do not help much.[208] They only mention the legislative inspirations of the right: Article 286 of the EC Treaty, Directive 95/46/EC, Article 8 of the ECHR, and Council of Europe Convention No. 108. The shift of data protection within the EU, from the original economic approach to a fundamental rights approach is, most commonly, attributed to two reasons.[209] First, the European Union, fifteen years after the Data Protection Directive is more than an economic union as its own name illustrates. Its competences extend to Common Foreign and Security Policy (CFSP)- former Second Pillar, and Police and Judicial Cooperation in Criminal Matters (PJC)- former Third Pillar. Data protection had, therefore, to be distanced somehow from internal market freedoms in order to cover those areas. As the Commission noted in its First Report on the Implementation of the Data Protection Directive, "Article 8, which incorporates the right to data protection, has given added emphasis to the fundamental rights dimension of the Directive."[210] This fundamental rights dimension means that data protection applies to further areas of processing, besides the common market, and the commercial flows of personal data. Data protection is made, thus, "a legal requirement throughout the Union",[211] and

[207] Recital 10 of the Data Protection Directive. Article 1 of the Directive stipulates: "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

[208] Updated Explanations relating to the text of the Charter of Fundamental Rights, CONV 823/03 (Brussels, 9 June 2003).

[209] In UK Information Commissioner Study Project, The Legal Framework: An analysis of the "constitutional" European approach to issues of data protection law, it is argued that "…data protection directives and several national laws also expressly extend some data protection guarantees to legal persons. This again emphasizes the special, *sui generis* nature of the concept." *See* UK Information Commissioner, *supra* note 118, at 7.

[210] Commission of the European Communities, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, Brussels, 15.5.2003 COM(2003) 265 final.

[211] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp26en.pdf> [accessed 2.5.2011].

covers processing for law enforcement purposes.[212] Second, the time seemed mature for the 'independence' of data protection from privacy, so that the former can be protected in its aspects that do not form part of the right to privacy.[213] In the words of the Article 29 Data Protection Working Party, "the rules on protection of personal data go beyond the protection of the broad concept of the right to respect for private and family life."[214] As it has been pointed out, "data protection and privacy are not interchangeable",[215] a fundamental right to data protection is, thus, necessary in order to cover values that are not related to privacy.[216] Closely connected to this, it has been argued by some authors that the recognition of a separate right to data protection, next to privacy, is "more respectful of the different European constitutional traditions",[217] because it takes into account that certain EU Member States, for instance, Germany and France, do not link data protection to privacy, but base it on different constitutional values, such as liberty (France) or dignity (Germany).

[212] Nouwt notes: "there seems to be a swift for data protection within the EU from the original economic approach, to a human rights approach, influenced by new EU activities with regard to law enforcement issues." Nouwt, *supra* note 194, at 286.
[213] De Hert and Gutwirth eloquently note that the recognition of a constitutional right to data protection in the EU Charter "allows for a sensible constitutional division of labour." De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197, at 81.
[214] ARTICLE 29 WORKING PARTY, OPINION 4/2007 ON THE CONCEPT OF PERSONAL DATA.
[215] De Hert & Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, *supra* note 77, at 9.
[216] In UK Information Commissioner Study Project, The Legal Framework: An analysis of the "constitutional" European approach to issues of data protection law, it is noted that "the fact that data protection was increasingly seen as a *sui generis* right, related to but distinct from Articles 8 and 10 ECHR, was one of the main reasons for giving it protection separate from those articles." UK Information Commissioner, *supra* note 118, at 7.
[217] De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197, at 82.

4. Theories of Data Protection and their Shortcomings

> *"We consider the right to privacy, as formulated in Article 8 of [the European Convention on Human Rights] hardly fit for such new case-law even with Westin's added dimension of 'information privacy'. It simply does not correspond to the reality of data processing. Article 10, freedom of information is not very suited either because data protection deals both with access to and limitations on access to information. Article 8 and 10 are each other's reflection in the mirror, each having a second paragraph enabling them to undo undesirable effects of the application of the main rule. For the citizens and the data users it seems unsatisfactory to construct data protection by a complicated juggling act between two counterbalancing articles and their restrictions."*[218]

4.1 Theories of Data Protection

It was mentioned above that there is an extensive literature attempting to develop a theory of privacy by a vast number of scholars coming from different disciplines: jurists, sociologists, philosophers, psychologists.[219] The same cannot be said, unfortunately, for data protection. The right is certainly not so young anymore, celebrating more than 15 years of life in the EU, and the evolution in legal discipline of an autonomous branch of law, known as 'data protection law'. Besides the abundant legal scholarship, data protection is also studied by researchers in the fields of political science, public administration and public policy,[220] and informational scientists. The debate is joined by data protection authorities and information commissioners, civil society associations, companies and individuals that assume the role of data controllers, and finally by (national or supranational) administrations and law enforcement authorities. However, despite the extensive writing from scholars and practitioners on various data protection issues, the research could pinpoint two theories on data protection, which will be approached critically below, before I turn,

---

[218] Frits Hondius, *A Decade of International Data Protection*, NETHERLANDS INTERNATIONAL LAW REVIEW 103, 127 (1983).
[219] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 11, at 12.
[220] Wim van de Donke et al., *The Politics and Policy of Data Protection: Experiences, Lessons, Reflections and Perspectives*, 62 INTERNATIONAL REVIEW OF ADMINISTRATIVE SCIENCES 459, 460 (1996).

at the second part of this Chapter, to the presentation of a new theory on data protection, which aims to deal with the particular problems posed by law enforcement and counter-terrorism.

4.2 The 'separatist' approach

The most comprehensive, until now, theory on data protection has been developed by Paul de Hert and Serge Gutwirth.[221] The theory discusses the respective roles that privacy and data protection can play in a democratic constitutional State. It is based on the premise that privacy and data protection can be seen as two distinct legal tools of power control, that perform different, but complementary functions (an approach I call the 'separatist model'). According to the two authors, "much can ... be learned from making and ascertaining the *difference* in scope, rationale and logic between privacy on the one hand, and data protection on the other."[222] In this respect, privacy is conceived as a tool of *opacity*, while data protection as a tool of *transparency*. Their function is different: opacity tools "embody normative choices about the limits of power";[223] transparency tools "come into play after these normative choices have been made in order still to channel the normatively accepted exercise of power."[224] Privacy, hence, on the one hand, as a tool of opacity, aims to protect individuals against illegitimate and excessive use of power (non-interference); data protection, on the other hand, as a tool of transparency, is directed towards the control and channeling of legitimate use of power. Pursuant to this approach, while data protection can be seen as offering a regulated acceptance,[225] privacy is presenting a

[221] De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197.
[222] *Id.* at 62. *See* also 94, "On the level of the legislator more attention should be paid to the distinct nature of the two sorts of legal tools that were invented to cope with power in a democratic constitutional state…"
[223] *Id.* at 70.
[224] *Id.* "Data protection regulations mainly belong to the tools of transparency, as opposed to the protection of privacy that pertains to the tools of opacity. The sheer wording of data protection principles (the fairness principle, the openness principle and the accountability principle, the individual participation principle,…) already suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice. The data protection regulations create a legal framework based upon the assumption that the processing of personal data is in principle allowed and legal. As such, these regulations implicitly accept that a processing of personal data is closely linked to the exercise of power and that it facilitates its establishment."
[225] De Hert and Gutwirth note "Data protection is not prohibitive. On the contrary, in the public sphere, it is almost a natural presumption that public authorities can process personal data as this is necessary

prohibition rule,[226] which is, however, in general subject to exceptions, since privacy is not an absolute right itself.[227] In the question of "how much of which tool is necessary when?", de Hert and Gutwirth explain that data protection -transparency tools, should be considered as the default rules;[228] "only in rare cases or after due consideration of actual risks will prohibitive opacity measures be taken to protect rights and freedoms and to promote trust in the Information Society."[229]

It cannot be denied that the 'separatist model' has many obvious merits. For the first time, it presents a comprehensive approach, long missed in the data protection literature, on the value of a right to data protection in the contemporary democratic constitutional States. It attempts to understand and ascertain the role of data protection in a legal system through the very content of its principles: they are designed to promote procedural justice, rather than normative (or substantive) justice.[230] Therefore, according to de Hert and Gutwirth, data protection does not operate in a prohibitive manner, but it "ruptures" the common legal logic: it replaces the traditional prohibitionary rule 'thou shall not kill' with 'thou can process personal data under certain circumstances'.[231] The prohibitive role is found by these authors in the function of privacy. Due to these different functions, de Hert and Gutwirth explain, for the first time, why data protection is needed alongside with privacy in a democratic constitutional state. Its added value in a democratic constitutional framework can be seen, according to these authors, in the clear separation of the two rights,[232] which implies a distinction between the legal tools of opacity, on the one hand, and transparency, on the other.

---

for the tasks they have to perform under statute… The main aims of data protection consist in providing various specific procedural safeguards to protect individuals' privacy and in promoting accountability by government and private record-holders. Data protection laws were precisely enacted not to prohibit, but to channel power, viz. to promote meaningful public accountability, and provide data subjects with an opportunity to contest inaccurate or abusive record holding practices. The rationale behind data protection in the public sector is the knowledge that authorities can easily infringe privacy and that in all administrative systems there is an urge to collect, store and use data, an urge which must be curtailed by legal regulation... A similar rationale explains the European option to regulate processing done in the private sector." *Id.* at 77.

[226] De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197.

[227] *Id.*

[228] *Id.*

[229] *Id.* at 96.

[230] *Id.* at 78.

[231] *Id.* at 77.

[232] De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197.

It is this insistence, however, on the necessity of the separation between privacy and data protection that makes de Hert's and Gutwirth's theory weak and subject to criticism. As it has been rightly pointed out, "it is not… that the 'classical' privacy regime is there to protect the facets of human life that need 'opacity' to best develop and that data protection regimes are there to organize the partial disclosures that social life interactions require. Rather, both facets- 'seclusion and 'inclusion and participation', are best preserved… by a combination of legal tools…"[233] Privacy and better protection should be regarded as pursuing one unique, rather than two separate, goal, and be, thus, conceived "together as forming the evolving bundle of legal protections of the fundamental… value of the autonomic capabilities of individuals in a free and democratic society."[234]

There is, however, a more fundamental problem with de Hert's and Gutwirth's approach that undermines the basic core of their argument altogether. The theory of these two authors seeks to establish, above all, the added value of the constitutional entrenchment of a separate right to data protection, next to the right to privacy. The enthusiasm of the two scholars could not be more evident: "Apparently, something new is happening at constitutional level";[235] "very recently, the proper role of data protection has received constitutional recognition in Article 8 of the 2000 Charter of Fundamental Rights of the EU";[236] "this recognition of a constitutional right should be welcomed",[237] and so on. There is, however, a paradox in their line of thinking: their theory, while it aims to be a theory on data protection, it does not focus on data protection itself. Rather, the added value of data protection is demonstrated through its distinction from privacy. By preaching separation, they strive to show the indispensability of data protection. But, their very argument proves them wrong. In the end, according to de Hert and Gutwirth, everything will be judged on the basis of privacy, as the tool of opacity,[238] will be the benchmark for establishing prohibited interferences. Data protection, as a transparency tool, merely describes the permitted processing; the limits will then be set on the basis of privacy. This, however, means

[233] Rouvroy & Poullet, *supra* note 34, at 76.
[234] *Id.*
[235] De Hert & Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, *supra* note 77, at 7.
[236] De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197, at 81.
[237] *Id.*
[238] Opacity as a notion for describing privacy is also problematic because it appears to conceive privacy as secrecy.

that data protection is not indispensable: we could live well without it. Of course we are better off with it, as it has some utility as a useful transparency tool, but still we could live without it, since every possible interference will be judged against privacy. De Hert and Gutwirth, fail to prove, therefore, why data protection is so fundamental, that it explains its constitutional entrenchment.

4.3 The 'instrumentalist' approach

Despite its problems, the 'separatist' approach is the most comprehensive theory of data protection elaborated so far. The research could identify in the literature a further approach to data protection, with the essential caveat, however, that this has been developed mainly as a response-criticism to the 'separatist' model analysed above, and thus, cannot be viewed as a stand-alone, comprehensive theory on data protection.

Replying essentially to de Hert and Gutwirth, Antoinette Rouvroy and Yves Poullet argue that privacy and data protection have "an 'intermediate' rather than a 'final' value, because they are 'tools' through which more fundamental values, or more 'basic' rights –namely human dignity and individual personality right- are pursued."[239] For this reason, they should be conceived as *instruments* for fostering the autonomic capabilities of individuals that are necessary for sustaining a vivid democracy[240] (an approach I call the 'instrumentalist' model). The two authors explain that the emergence of a right to data protection is due to the technological evolutions that "may require legal protections of privacy to evolve, simply because those technological evolutions threaten, in new ways, the fundamental value of personal autonomy."[241] They support this argument by invoking the German Constitutional Court's Census decision,[242] according to which, "the development of the data processing technologies obliged the State to revise and adapt the guarantees it provides to individuals in order to protect and foster the capabilities needed to implement their right to freely self-determine their personality."[243]

[239] Rouvroy & Poullet, *supra* note 34, at 53.
[240] *Id.* at 46.
[241] *Id.* at 54.
[242] *See* above.
[243] Rouvroy & Poullet, *supra* note 34, at 55.

Rouvroy and Poullet contend, however, that privacy and data protection "are not to be put on the same footing",[244] because they are different tools for enabling individual reflexive autonomy. They criticise, therefore, the acknowledgement of the right to data protection as a fundamental right, distinct to the traditional fundamental right to privacy, in the EUCFR, because "by placing the right to data protection on the same level as privacy, the European text carries the risk that the fundamental anchoring of data protection regimes in the fundamental values of dignity and autonomy will soon be forgotten by lawyers and that legislators will soon forget to refer to these fundamental values in order to continuously assess data protection legislation taking into account the evolution of the Information Society."[245] In this regard, they explain, in a rather confusing way, that making the right to data protection a distinct fundamental right "risks obscuring the essential relation existing between privacy and data protection and further estrange data protection from the fundamental values of human dignity and individual autonomy, foundational to the concept of privacy in which data protection regimes have their roots."[246]

Besides the fact that the 'instrumentalist' approach fails to provide a robust analysis of the right to data protection, it is fraught with fears that remain unsubstantiated. It is not clear why data protection cannot have an instrumental value, while at the same time being at an equal footing with privacy. The two authors seem to negate any value of data protection, because this might allegedly end up in trumping the instrumental value of privacy, and thus undermine privacy as a fundamental right. Rouvroy and Poullet make a valid point about the uniqueness of the final goals of the two rights (be that autonomy or dignity or the right to individual personality), but, they do not convince why the constitutional entrenchment of data protection is so harmful.

[244] *Id.* at 70.
[245] *Id.* at 71.
[246] *Id.* at 74.

5. Reconstructing Data Protection

5.1 Method: how should we approach data protection?

Despite the differences in the conclusions of the two approaches analysed above -the 'separatist' model is recognising an added value to data protection, while the 'instrumentalist' is negating it- , the two theories share a common insightful point: they both view data protection through privacy. They attempt, therefore, to formulate a data protection theory by looking into its relationship with privacy.

Starting from the premise that data protection is a fundamental right, at least within the EU legal framework,[247] I argue that an approach to understanding the added value –if any- of this right must have a focus. Its focus should be data protection, not its possible interactions with privacy. This does not mean, however, that I deny that the two rights are closely related. Privacy is an umbrella notion for a plurality of things[248] that covers aspects of data protection in any case. This does not imply, necessarily, that data protection has no added value. My argument, therefore is, that if we want to approach this value, we should try to see data protection at isolation for a moment.

5.2 Is data protection 'mature' to stand alone? Problems and limitations

That being said, why, is it that the two theoretical attempts to approach data protection, that exist so far, find it necessary to view it next to the right to privacy? Certainly, it has been noted various times in the present thesis that data protection pursues, above all, privacy objectives, but is this the real reason? Or is there something missing from data protection rules that makes the right unable to stand alone? De Hert and Gutwirth view data protection as a tool of transparency, aimed to channel or regulate, but not prohibit power. This is because, according to these two

[247] The UK Information Commissioner Study Project, The Legal Framework: An analysis of the "constitutional" European approach to issues of data protection law notes astutely: "Irrespective of whether one sees data protection as a right flowing (in particular) from the right to "private life" in Art. 8 ECHR or as a new *sui generis* right, one matter is clear: from the European- legal perspective at least, it is to be regarded as a fundamental right." UK Information Commissioner, *supra* note 118, at 8.
[248] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 11, at 45.

authors, it is "almost a natural presumption" that public authorities and private individuals or entities "can process personal data as this is necessary for the tasks they have to perform".[249] Data protection operates, thus, only as an affirmative liberty. It is a necessary, therefore, to fall back to privacy, to determine if certain processing is illegitimate, as this presents the 'hard core' negative rule of non-interference.

Indeed, a closer look at Article 8 of the EUCFR, confirms de Hert's and Gutwirth's conclusion: data protection is depicted in affirmative terms, as a transparency tool. The first paragraph of Article 8 introduces the general right - everyone has the right to the protection of personal data concerning him or her-, while the second paragraph goes on to set the rules of the permissible processing –fair processing, for specified purposes, on the basis of the consent of the person concerned or some other legitimate basis, granting the data subject the right of access and rectification. The right to privacy in Article 7 is also formulated in an affirmative way.[250] One should not be confused though. Pursuant to Article 52 (3) EUCFR, in so far as the Charter contains rights which correspond to rights guaranteed by the ECHR, the meaning and scope of those rights shall be the same as those laid down by the Convention. The right to privacy is found in Article 8 of the ECHR. The second paragraph stipulates that:

> "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."

This means that, as de Hert and Gutwirth contend, the right to privacy in the EUCFR has the function of the opacity, non-interference tool.

Viewing data protection merely in affirmative terms is, however, problematic. The problem is not only theoretical. As Cohen astutely points out, "the conventional wisdom is that... affirmative liberty claims are weaker and less principled than negative liberty claims."[251] This is why data protection cannot stand alone as a

---

[249] De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197, at 77.
[250] "Everyone has the right to respect for his or her private and family life, home and communications."
[251] Cohen, *supra* note 91, at 1400. *See* also David Currie who notes that "one should not quibble over the question whether the rights acknowledged… are in some linguistic or logical sense "really"

fundamental right. This is why the right to privacy is needed in the end to determine the prohibitive instances of non-interference.

I argue that the way in which data protection has been drafted obstructs the right itself to operate independently from privacy.[252] Contrary to what de Hert and Gutwirth contend, the value, of a fundamental right to data protection, as it stands now, is limited: it can operate only as a transparency tool, but illegitimate interferences will be determined on the basis of privacy.[253] These limitations, whether they are attributed to the drafters of the right, or the particularities of its genesis and its initial drafting to take into account economic concerns, demonstrate that data protection is not 'mature' to operate alone, as it currently stands.[254]

5.3 'Reconstructing' data protection: 'hard core' data protection principles

If the right to data protection is to be a *bona fide* fundamental right with a value of its own, it needs to be reconstructed, in order to satisfy certain conditions. The first is that data protection as a fundamental right should be able to function both positively and negatively. It should be able, on the one hand, to regulate, channel and control power, and on the other hand, to prohibit power.

I argue that this can be done, by recognising a 'core' or 'essence' of the right to data protection that cannot be subjected to restrictions. Determining which elements of the fair information principles represent the 'essential core' of the right to

---

positive." David Currie, *Positive and Negative Constitutional Rights*, 53 U. CHICAGO. L. REV. 864, 887 (1986).

[252] Compare Bygrave who notes that the drafting and enactment of data protection laws has frequently involved "lengthy processes fraught with controversy." BYGRAVE, DATA PROTECTION LAW, *supra* note 8, at 4.

[253] Martin Scheinin and Mathias Vermeulen contend that "Addressing issues related to the protection of personal data will not suffice to determine the limits of the use of detection technologies. Data protection rules formulate the conditions under which the processing of data is legitimate. The right to data protection will therefore come into play only secondarily, in order to minimize the negative impact of the use of technology on the right to privacy. The right to protect personal data is a procedural right in this context: it informs the right to privacy and provides important parameters of *control* over some aspects of the private life of a person." MARTIN SCHEININ & MATHIAS VERMEULEN, DETECTER, DETECTION TECHNOLOGIES, TERRORISM, ETHICS AND HUMAN RIGHTS 7 (European Commission, Seventh Framework Programme).

[254] Rowland aptly argues that "The interaction of the social and political requirements which led to data protection regulation, the resulting legal framework for the protection of informational privacy, together with the political, social and legal constraints on the exemptions to the regulation, create an intrinsically complex system with correspondingly complex modes of failure." Rowland, *supra* note 201, at 10.

data protection is not an easy task. However, it is not impossible. As the Article 29 Working Party has noted under a different context

> "Using Directive 95/46/EC as a starting point, and bearing in mind the provisions of other international data protection texts, it should be possible to arrive at a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection... Such a minimum list should not be set in stone. In some instances there will be a need to add to the list..."[255]

Following this pronouncement of the Working Party, it can be argued that sensitive data, such as data revealing racial or ethnic origin, political and religious beliefs, health and sexual life, should be shielded from certain categories of processing, especially if this is undertaken for the use of the data for different purposes from the ones initially collected. The purpose specification principle should also have a 'hard core' which will prohibit the secondary use of personal data, even if those are not necessarily sensitive. This 'essence' of the purpose specification principle should apply when the further processing of personal data threatens the principle of non-discrimination or the core of the right to 'informational self-determination' of the individual.

In essence, the 'hard core' of data protection would be what needs to be protected, so that the final values that data protection pursues -in the words of Rouvroy and Poullet- such as individual autonomy, dignity and personal identity are safeguarded. Thus reconstructed, data protection can be seen also as having a negative function: ensure the liberty "to preclude certain types of probabilistic judgements about one's inclinations, abilities, or short-comings."[256] Thus reframed, it is difficult to see why the right to data protection cannot stand independently on the side of the right to privacy.

---

[255] WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, WORKING DOCUMENT, TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES: APPLYING ARTICLES 25 AND 26 OF THE EU DATA PROTECTION DIRECTIVE 5 (July 24, 1998).

[256] Cohen, "Examined Lives: Informational Privacy and the Subject as Object", 1400.

5.4 A balancing mechanism for data protection

Data protection -as privacy- is not an absolute right.[257] On the contrary, it should be weighed against contrasting values and rights in a democratic society.[258] This means, furthermore, that data protection can be legitimately subjected to restrictions. These restrictions, however, will be permissible, insofar as they meet the following conditions: 1) they are provided by law 2) they pursue a legitimate aim 3) they are necessary in a democratic society 4) they conform with the principle of proportionality and 5) they respect the 'essence' of the right to data protection.

This is the second condition that data protection needs to satisfy in order to be a fully-functional fundamental right. It should be balanced against opposing interests as such, not through the proxy of privacy. This means that infringements of the right to data protection should be determined on the basis of the data protection principles themselves, with the application of the principle of proportionality,[259] without the need to recourse to the right to privacy. The processing, thus, of personal data should be deemed proportionate or disproportionate, on the basis of the specific fair information principle, with which it interferes. Determining disproportionate processing on the basis of the right to privacy and not of the specific data protection principle that this goes against, is not only an unnecessary circumvention of the existing law that renders data protection virtually useless. It is also dangerous, because there could be instances of disproportionate processing of personal data that hardly, however, constitute disproportionate interferences with the right to privacy. The problem posed in the case *United States v. Miller*[260] of the US Supreme Court could be a useful example here.[261] In this case, federal law enforcement officials issued subpoenas to two banks to produce a customer's financial records. The banks complied with the subpoenas, but the customer was not notified of the disclosure of the records until later in the course of prosecution. He contended that the subpoenas violated his Fourth Amendment

[257] De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197, at 74.
[258] As the Court of Justice has held human rights are "far from constituting unfettered prerogatives" and they are subject "to limitations laid down in accordance with the public interest." *See Case 4/73 Nold v Commission* [1974] ECR 491, para 14.
[259] On the relationship between the 'principle of proportionality' and the 'essential core' doctrine *see* the very interesting analysis of Robert Schutze, *Three "Bills of Rights" for the European Union*, 30 YEARBOOK OF EUROPEAN LAW 131, 140 (2011).
[260] 425 U.S. 435, 437 (1976).
[261] For an analysis of the case, *see* Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528–529 (2006).

rights,[262] but the Court concluded that he lacked a reasonable expectation of privacy in the financial records maintained by his bank,[263] because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[264] According to the Court, "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[265] Leaving aside, the problems of the US constitutional protection of privacy through the 'legitimate expectations' doctrine, this example is illuminating also in the EU fundamental rights context.[266] The further use by the government of personal financial data is specifically addressed by the purpose/ use limitation principle, a keystone principle of data protection laws. It is not so evident, however, whether an interference with the right to privacy can be established here, without recourse to other fundamental rights and principles, such as, for instance, procedural rights of the individual to know if his personal information is further disseminated, or in certain cases, the principle of non-discrimination. Moreover, any potential claim of the customer against his bank would have to be established not on the basis of his right to privacy, but on breach of contractual obligations.

Taking data protection principles seriously is, therefore, a necessity. Data protection principles should not be seen as mere proclamations, void of any coercive meaning. Viewing fair information principles as coercive principles is not merely a theoretical issue emanating of the debate on the added value of data protection. It can have serious practical consequences in the drafting of legislation. This is because data protection principles are more specific and they can provide for prescriptive guidance better than the general privacy concept. They can be, thus, very informative for legislators, when they seek to adopt measures that clearly go against specific fair information principles. In these cases, stricter scrutiny against the test of proportionality should be applied, not only on the basis of privacy, but also of the specific data protection principle at stake. The problem remains the same, when the measure should be judged *ex post*, by Courts: if a certain data protection principle is at

[262] *Id.* at 438.
[263] *Id.* at 442.
[264] *Id.* at 443.
[265] *Id.* at 442.
[266] For a discussion on how the ECtHR has applied a "reasonable expectations" test *see* the very interesting analysis of Tomás Gómez-Arostegui, *Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations*, 35 CAL. W. INT'L L. J. 153 (2005).

issue, then it would be clearer if the Court focused on that in order to perform the proportionality analysis, instead of seeking recourse to a general notion of privacy. Whether this is actually the case, it will be examined below.

6. Judicial assessment of data protection: Is it all about privacy?

> *"I firmly believe that we should care where the judges are. I believe equally firmly that if the judges are not around in the field of data protection law, or not around often enough, then this absence is problematic. It is problematic because it increases the risk of compromising basic rule of-law ideals. And it is problematic because an absence or scarcity of judicial opinion inevitably impoverishes law and policy on data protection."*[267]

6.1 The approach of the European Court of Human Rights

Attempting to find data protection as a fundamental right in the jurisprudence of the Strasbourg court is a somewhat quaint exercise. This is because a right to personal data is not mentioned, as such, in the European Convention of Human Rights. Data protection, which is recognised as a right by the Council of Europe Convention No. 108 is not, however, unknown to the Strasbourg court. The European Court of Human Rights finds it encompassed in Article 8 ECHR, which recognises the right to respect for private and family life. For instance, in *M.S. v. Sweden*, the Court held that 'the protection of personal data ... is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention'.[268] The Court does not endorse a specific, clear-cut definition of privacy,[269] it rather keeps the notion open on purpose: "private life should be considered as broad term which is not susceptible to an exhaustive definition."[270]

In a set of different judgments, the Court held that the storing of information relating to an individual's private life in a secret register and the release of such information amounted to an interference with his right to privacy as guaranteed by

---

[267] Lee Bygrave, *Where Have All the Judges Gone? Reflections on Judicial Involvement in Developing Data Protection Law*, 7 PRIVACY LAW & POLICY REPORTER 11, 35 (2000).
[268] *M.S. v Sweden* (Appl. No 20837/92), judgment of 27 August 1997. *See* also *Rotaru v Romania* (*Rotaru v Romania* (Appl. No. 28341/95), judgment of 4 May 2000, para 43) where the ECtHR recognised that Article 8 ECHR is interpreted in such way as to encompass the guarantees concerning data protection enshrined in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[269] EVELIEN BROUWER, DIGITAL BORDERS AND REAL RIGHTS: EFFECTIVE REMEDIES FOR THIRD-COUNTRY NATIONALS IN THE SCHENGEN INFORMATION SYSTEM 153 (2008).
[270] *P.G. and J.H. v. UK,* 25 September 2001, No 44787/98.

Article 8 (1); [271] that the protection of medical data is of fundamental importance to a person's enjoyment of his or her right to private life;[272] that the refusal to allow an opportunity for the personal data to be refuted constitutes an interference with the right to privacy;[273] that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences constituted a disproportionate interference with the right to privacy life and therefore a violation of Article 8 ECHR.[274]

Besides the fact that much of this case-law concerns, in most cases, data processing in rather special contexts, such as secret surveillance activities by the police or intelligence agencies,[275] the Court's approach to data protection is not surprising. It is viewed as an aspect of the very broad notion of private life, following the Court's interpretation of Article 8 ECHR.[276] This approach, while understandable, is not without shortcomings: not all personal data are deemed to form part of the right to private and family life, and the recognition of specific data protection principles, such as the right to access to personal data does not always derive automatically for the Court from Article 8.[277]

6.2 The approach of the Court of Justice of the European Union

Unlike the European Convention of Human Rights that enshrines the right to privacy, but makes no mention to a right to data protection, the EU recognises explicitly a fundamental right to personal data protection in Article 8 EUCFR. It can be legitimately assumed, therefore, that the European Court of Justice (ECJ) (now: the Court of Justice of the European Union) has adopted a more clear stance in its jurisprudence than the ECtHR regarding the nature of the right to data protection. A closer look to the ECJ's case-law, however, proves this perception rather misguided.

---

[271] *Leander v. Sweden* (Appl. No. 9248/81), para. 48. See also *Amann v Switzerland* (Appl. No. 27798/95), judgment of 16 February 2000, para 70.
[272] *Z. v. Finland* (Appl. No. 22009/93), judgment of 25 February 1997, *Rep*. 1997-I, para 95.
[273] *Rotaru v Romania,* para 45.
[274] *S and Marper v UK* (Appls. Nos 30562/04 and 30566/04), judgment of 4 December 2008.
[275] Bygrave, *Where Have All the Judges Gone? Reflections on Judicial Involvement in Developing Data Protection Law*, *supra* note 267, at 12.
[276] As the Court puts it: its case-law "emphasise[s] the correspondence of this broad interpretation [of Art. 8 of the Human Rights Convention] with that of the [Data Protection Convention]."
[277] De Hert & Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, *supra* note 77, at 27.

Several judgments have been pronounced by the Court of Justice of the EU concerning data protection issues.[278] Most often, they regard preliminary rulings on questions of interpretation of the Data Protection Directive. If we attempt a general comment on this case-law, this would be that "the Court, in essence, has interpreted an internal market harmonisation instrument (the Directive) in a manner that fosters the protection of a fundamental right".[279] This notwithstanding, the Court has been accused of viewing "data protection as privacy, no more no less."[280] According to this argument, the Court's approach is simple: "A breach of the right to privacy implies an unlawful processing in the sense of the Directive; no breach of privacy implies no breach of the Directive."[281] The analysis will discuss this argument by focusing on four cases where the Court of Justice dealt with the nature of data protection: *Österreichischer Rundfunk,*[282] *Lindqvist,*[283] *Promusicae,*[284] and *Schecke.*[285]

Österreichischer Rundfunk was a preliminary ruling case on the compatibility with Community law of an Austrian provision requiring entities which were subject to control by the Austrian Court of Audit, the Rechnungshof, to inform the latter about the salaries of their employees when they exceeded a certain level. This information was subsequently published by the Rechnungshof in a report which contained the names of the persons and the level of their respective salaries. In this respect, the Court was asked to rule whether the Data Protection Directive was applicable at all to this control activity exercised by the Rechnungshof. Unlike Advocate General Tizziano who pleaded against the applicability of the Directive, the ECJ found that it was applicable. According to the Court, "since any personal data can move between Member States, Directive 95/46 requires in principle compliance with the rules for protection of such data with respect to any processing of data as defined by Article

---

[278] For an analysis of the ECJ case-law on data protection *see* Tzanou, *supra* note 202, at 284.
[279] Maria Tzanou, *Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection*, 6 CROATIAN YEARBOOK OF EUROPEAN LAW & POLICY 53, 59 (2010).
[280] De Hert & Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, *supra* note 77, at 33.
[281] *Id.* at 32.
[282] Joined Cases C-465/00, C-138/01 & C-139/01, *Österreichischer Rundfunk*, Judgment of 20 May 2003, Full Court, [2003] ECR I-4989.
[283] Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.
[284] Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU*, judgment of 29 January 2008.
[285] Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR* (C-92/09), *Hartmut Eifert* (C-93/09) *v Land Hessen*, Judgment of the Court (Grand Chamber) of 9 November 2010.

3."[286] The ECJ rejected the argument that the Data Protection Directive applies only to activities which have a sufficient connection with the common market, by holding that recourse to Article 95 EC (now 114 TFEU) as a legal basis "does not presuppose the existence of an *actual link* with free movement between Member States *in every situation* referred to by the measure founded on that basis."[287] If a contrary interpretation were to be adopted, it would make the limits of the field of application of the Data Protection Directive particularly unsure and uncertain, which would be contrary to its essential objective that is the harmonisation of the data protection rules of the Member States, in order to eliminate obstacles and ensure the free movement of personal data within the internal market.[288]

The same wide interpretation of the scope of the Data Protection Directive was reiterated in *Lindqvist*. Before moving to the reasoning of the Court, it is worth taking a closer look at the Opinion of the Advocate General. In particular, Advocate General Tizzano reasoned against the applicability of the Data Protection Directive to the processing of personal data which consisted of setting up an Internet page as an ancillary activity to Mrs Lindqvist's voluntary work as a catechist in a parish of the Swedish Protestant Church. To refute the Commission's argument that Mrs Lindqvist's activity fell within the scope of the Directive because this is not confined to pursuing economic objectives but also has objectives connected with social imperatives and the protection of fundamental rights, the Advocate General observed that the need to safeguard the fundamental rights of individuals in order to ensure a high level of protection of those rights "was conceived in the course of and with a view to achieving the *main objective* of the Directive, namely the *free movement* of personal data inasmuch as it is held to be 'vital to the internal market'."[289] According to the Advocate General, contributing to economic and social progress and

[286] *Österreichischer Rundfunk*, *supra* note 265, para 40.
[287] *Österreichischer Rundfunk*, *supra* note 265, para 41 (emphasis added). Classen argues that: "But it is, above all, questionable … [that the Court] took no account of the limits of the legal basis in the Treaty when dealing with the question how to define the scope of a provision of secondary legislation. Article 95 EC is not a sufficient legal basis for a Directive applying within the whole scope of Community law. The Court of Justice did not even try to find any relation to the internal market beyond the realization of fundamental freedoms… the present decision is particularly disappointing. Certainly it proves the increasing interest of the ECJ in human rights questions, but this does not exonerate the Court from the obligation to examine the applicability of Community law – a criticism which can be addressed also towards some other recent judgments." Claus Dieter Classen, *Joined Cases C-465/00, C-138/01 & C-139/01, Österreichischer Rundfunk, Judgment of 20 May 2003, Full Court, [2003] ECR I-4989*, 41 COMMON MARKET LAW REVIEW 1377, 1382 (2004).
[288] *Österreichischer Rundfunk*, *supra* note 265, para 42.
[289] Opinion of Advocate General Tizzano *Lindqvist* Case C-101/01, para 40.

safeguarding fundamental rights represent important values and imperatives which the Community legislature took into account in framing the harmonised rules required for the establishment and functioning of the internal market but they are not *independent* objectives of the Directive.[290] In accordance with its legal basis, Directive 95/46 has, in the view of the Advocate General, as its *principal* objective the guaranteeing of the free movement of data within the internal market. Thus, the harmonization of national legislation on the protection of personal data is only a *means* of guaranteeing free movement of personal data. This means that, although it calls upon the Member States to adopt a harmonized system of protection of personal data, the Directive is not a norm for the protection of fundamental rights. To support this analysis, Advocate General Tizzano adopted a strict reading of the principle of 'attributed competences' and recalled that the European Community does not have any general competence to design provisions protecting fundamental rights. On the basis of Article 95 EC, the Community legislature did not have competence to design an act guaranteeing, in all cases, the protection of fundamental rights. Thus, far from offering general protection to individuals, the Directive, according to the Advocate General, applies only to the activities within the scope of Community law.

The ECJ did not agree with this approach. It stressed once more that a distinction should be made between the general objective of an act adopted on the basis of Article 95 EC and the specific situations where this act can be applied even if those are not directly linked to the internal market. It clarified that the exception of Article 3 (2)[291] applies only to the activities which are expressly listed there or which can be classified in the same category. As a result, the Directive applies to all the other activities regardless of their connection with the internal market. Thus, it applied to the charitable and religious activities carried out by Mrs Lindqvist.

Having established that the applicability of the Data Protection Directive is not based on the 'connection' of the processing activity with the internal market, on the substantive issue of the nature of data protection, the Court seems to think that this should be interpreted on the basis of the right to privacy:

> "It should also be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe *fundamental freedoms*, in

[290] *Id.*, para 41.
[291] Article 3 (2) lays down the cases that fall outside the scope of application of the Directive. *See* Chapter 4.

particular the right to *privacy*, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures."[292]

This pronouncement is rather puzzling, because it seems to suggest that the Court does not consider data protection as a fundamental right, but is only concerned over certain forms of processing that might infringe fundamental rights, and in particular the right to privacy; in this case, the protection afforded to fundamental rights as general principles of EU law will apply. Having stated this, the ECJ goes on to examine in *Österreichischer Rundfunk* whether the activities of the Rechnungshof constitute an interference with the right to privacy. It concludes that:

"while the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life, the communication of that data to third parties, in the present case a public authority, infringes the right of the persons concerned to respect for private life, whatever the subsequent use of the information thus communicated, and constitutes an interference within the meaning of Article 8 of the Convention."[293]

This approach of the Court is problematic, because by failing to recognise data protection as a fundamental right, all possible interferences have to be assessed on the basis of the right to privacy. Thus, activities that would constitute, without doubt, interferences with data protection, such as the recording of remuneration, are not deemed to interfere with the right to privacy, unless the recorded data are communicated to third parties. This lessens the scope of protection, especially since data protection was recognised as a fundamental right, next to privacy, in the EU legal order.

While the ECJ chose to look away from the provision of Article 8 of the EU Charter of Fundamental Rights in *Österreichischer Rundfunk* and *Lindqvist* and focus solely on the Data Protection Directive, in *Promusicae,* it did a remarkable turn and recognized data protection as a fundamental right enshrined in the Charter. *Promusicae* concerned the refusal of a commercial company, which provided internet access services, Telefónica, to disclose to Promusicae, a non-profit-making organisation of producers and publishers of musical and audiovisual recordings, acting on behalf of its members who were holders of intellectual property rights,

[292] *Österreichischer Rundfunk*, *supra* note 265, para 68.
[293] *Österreichischer Rundfunk*, *supra* note 265, para 74.

personal data of certain persons whom it provided with internet access services. Promusicae sought disclosure before the Commercial Court of Madrid, of the above information in order to be able to bring civil proceedings against those persons, who, according to it, used the KaZaA file exchange program (peer-to-peer) and provided access in shared files of personal computers to phonograms in which the members of Promusicae held the exploitation rights. The Spanish Court referred the issue to the ECJ by asking it essentially whether Community law, in particular Directives 2000/31,[294] 2001/29[295] and 2004/48,[296] read in the light of Articles 17 and 47 of the EUCFR, require Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.

Having established that the secondary Community legislation did not provide a clear answer on the issue at stake, the Court turned its attention to primary EC constitutional law, namely fundamental rights. In this part of its analysis, it noted from the outset that while the fundamental right to property, which includes intellectual property rights such as copyright, and the fundamental right to effective judicial protection constitute general principles of Community law,[297] the situation in respect of which the national court put the question at issue involves, in addition to those two rights, a *further fundamental* right, namely the right that "guarantees protection of personal data and *hence of private life*."[298] This is the first time that the Court expressly recognized that the right to data protection enjoys the status of a fundamental right within the EU. It did so by looking at Article 8 of the EUCFR, which expressly proclaims the right to data protection.[299] It seems, though that the ECJ in this case went one step forward from its existing case-law concerning the Charter: until *Promusicae*, if a right was contained in the Charter, this created a

[294] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178/1 of 17.7.2000.
[295] Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167/19 of 22.6.2001.
[296] Directive 2004/48 of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157/32 of 30.4.2004.
[297] *Promusicae*, *supra* note 267, para 62.
[298] *Promusicae*, *supra* note 267, para 63 (emphasis added).
[299] *Promusicae*, *supra* note 267, para 64.

presumption that it was protected under the general principles of Community law.[300] In *Promusicae* however, the fact that the protection of personal data was enshrined in the Charter was enough for the ECJ to identify it as an autonomous fundamental right.[301]

Promusicae is remarkable from this point of view, on the substance, however, it marked no real difference from the ECJ's understanding of data protection in *Österreichischer Rundfunk* and *Lindqvist*. The Court seems to think that data protection is a fundamental right that guarantees protection of personal data and *hence of private life*. The balancing of fundamental rights, therefore, in this case will take place between "the right to respect for *private life* on the one hand and the rights to protection of property and to an effective remedy on the other."[302] Data protection is not mentioned by the Court since apparently it is a part of privacy.

In *Schecke* the Court was presented with a unique opportunity to clarify its position regarding the nature of data protection as a fundamental right. The case concerned the questions raised in the course of proceedings between two German nationals, a natural and a legal person, and the Land Hessen concerning the publication on the Internet site of the Bundesanstalt für Landwirtschaft und Ernährung (Federal Office for Agriculture and Food) of personal data relating to them as recipients of funds from the EAGF or the EAFRD. The publication was mandatory pursuant to Article 44a of Regulation No 1290/2005,[303] which obliges Member States to ensure "annual *ex-post* publication of the beneficiaries of the EAGF and the EAFRD and the amounts received per beneficiary under each of these Funds."

Before turning to the reasoning of the Court of Justice, it is worth taking a look at the national court's position. This opined that the obligation to publish under Article 44a of Regulation No 1290/2005 constituted an unjustified interference with the fundamental right to the protection of personal data.[304] In particular, it considered that that provision, which pursues the aim of increasing the transparency of the use of European funds, does not improve the prevention of irregularities, since extensive

---

[300] *See* Michael Dougan, *The Treaty of Lisbon 2007: Winning Minds, Not Hearts*, 45 COMMON MARKET LAW REVIEW 617, 662 (2008).
[301] Tzanou, *Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence*, *supra* note 202, at 275.
[302] *Promusicae*, *supra* note 265, para 65 (emphasis added).
[303] Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, OJ L 209/ 1 of 11.8.2005.
[304] *Schecke*, *supra* note 268, para 30.

control mechanisms exist for that purpose. In any event, according to the German court, that obligation to publish was not proportionate to the aim pursued, because the Regulation did not limit access to the Internet site concerned to 'Internet Protocol' (IP) addresses situated in the European Union, and it was not possible to withdraw the data from the Internet after the expiry of the two-year period laid down in Article 3(3) of Regulation No 259/2008.[305] The German court's pronouncements on the case is very important, because it invited essentially the Court of Justice of the EU to recognise data protection as a self-standing fundamental right: the court suggested that any possible interference had to be determined on the basis of the fundamental right to data protection without any recourse to privacy.

The Court, however, did not follow that path. It started by pointing out that the relevant provision on publication of the Regulation should be assessed in the light of the EU Charter of Fundamental Rights, which constituted at the time of the delivery of the decision binding EU law. The Court mentioned that Article 8 EUCFR was the relevant Charter provision at this case, but with the necessary clarification that "that fundamental right is *closely connected* with the right to respect of private life expressed in Article 7 of the Charter."[306] Having said that, the Court proceeded its analysis on the permissible limitations that can be imposed to the right to data protection by confounding, however, data protection and privacy, in what it calls "the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter".[307]

The Court of Justice cannot be criticised for this approach. Certainly, taking into account the right to data protection as it currently stands in Article 8 of the EUCFR, it reaches the conclusion that the right cannot operate alone, without privacy.[308] The only solution, therefore, for the Court is to consider them together as 'the right to respect for private life with regard to the processing of personal data.' Privacy is needed in the equation, because on the basis of this, the possible interferences will be determined, according to Article 8 (2) ECHR. The Court could have, however, followed the way shown by the national court, and for the first time demonstrated that data protection can operate independently. This reading could have been possible since it could have applied directly to the right to data protection in

[305] *Schecke*, *supra* note 268, para 31.
[306] *Schecke*, *supra* note 268, para 47 (emphasis added).
[307] *Schecke*, *supra* note 268, para 52.
[308] Compare BOEHM, *supra* note 5, at 126.

Article 8 EUCFR the conditions of Article 52 (1) EUCFR,[309] without the need to go through Article 52 (3) to the relevant provision of Article 8 (2) ECHR on the permissible limitations to the right to privacy.

[309] Article 52 (1) EUCFR stipulates: "Any 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."

Chapter 2. The Data Protection Legal Framework

"The EU's special rules on policing and criminal law (the 'third pillar') may be as hard to kill as the legendary Rasputin."[310]

1. The EU data protection regime

1.1 The constitutional framework for the EU data protection regime[311]

Following the entry into force of the Treaty of Lisbon on 1 December 2009, the constitutional legal base for measures concerning data protection within the EU is Article 16 of the Treaty on the Functioning of the European Union (TFEU).[312] The Article, which replaces Article 286 EC, applies both to the former first and the former third pillar and provides for the use of the ordinary legislative procedure[313] when rules "relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law", or "rules relating to the free movement of data" are adopted.[314] Furthermore, Article 16 TFEU stipulates that compliance with data protection rules will be subject to the control of independent authorities.[315] The similar provision regarding Common Foreign and Security Policy (CFSP) is found in Article 39 of the Treaty on the European Union (TEU).[316]

---

[310] Steve Peers, *Finally "Fit for Purpose"? The Treaty of Lisbon and the End of the Third Pillar Legal Order*, 27 YEARBOOK OF EUROPEAN LAW 47, 47 (2008).

[311] The term 'constitutional' is used here to describe primary EU law, in the sense of the European Court's of Justice pronouncement in *Les Verts* that the EC Treaty has created a municipal legal order of transnational dimensions, of which it forms the 'basic constitutional charter'. Case 294/83 *Les Verts* [1986] ECR 1339, para 23.

[312] Article 16 (1) TFEU provides: "Everyone has the right to the protection of personal data concerning them."

[313] *See* STEVE PEERS, EU JUSTICE AND HOME AFFAIRS LAW 874 (3rd ed. ed. 2011).

[314] Article 16 (2) TFEU.

[315] Article 16 (3) TFEU.

[316] Article 39 TEU provides: "In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal

Data protection is also recognised as a fundamental right by the EU Charter of Fundamental Rights (EUCFR),[317] which enjoys the status of EU primary law after the entry into force of the Lisbon Treaty.[318] Furthermore, data protection rights are considered general principles of EU law either as a dimension of the right to respect for private life,[319] which is enshrined in Article 8 of the European Convention on Human Rights (ECHR), as reflected in Article 6 (3) TEU,[320] or independently.[321]

1.2 Legislative instruments

Besides the EU primary law, a rather extensive EU legislation on data protection also exists: On the one hand, within the scope of the former first pillar (Community), there is the Data Protection Directive; the ePrivacy Directive, the Data Protection Regulation; and the Data Retention Directive that was presented as a modification of EC data protection legislation. On the other hand, within the scope of the former third pillar, there is only one general instrument applying to the processing of data in the area of Police and Judicial Cooperation in Criminal matters (PJC), the relevant Framework Decision. This is supplemented by several data protection rules in further specific third pillar instruments, which concern the processing of personal data for different purposes. As the Article 29 Working Party has noted, the current situation in the former third pillar can be described "as a patchwork of data protection regimes, which are applicable in different situations."[322]

---

data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

[317] Article 8. For an analysis *see* below.

[318] Article 6 (1) TEU provides: "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties."

[319] Scandamis et al., *supra* note 101, at 6.

[320] Article 6 (3) TEU reads as follows: "Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law."

[321] *See* Case C-369/98 *Fisher* [2000] ECR I-6751. *See* also PEERS, EU JUSTICE AND HOME AFFAIRS LAW, *supra* note 313, at 882.

[322] ARTICLE 29 WORKING PARTY, WORKING PARTY ON POLICE AND JUSTICE, 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 7 (December 01, 2009).

Even though the Treaty of Lisbon has repealed the former Title VI of the TEU and abolished the distinction between the first and the third pillar,[323] "the data protection rules adopted within the framework of the former third pillar will remain valid until they are amended",[324] due to the Treaty's transitional provisions.

Since the Lisbon Treaty establishes a single legal base for data protection measures for the former first and third pillars, dichotomies between them and 'commercial' and 'law enforcement processing' should cease to exist.[325] In this respect, the Commission should propose legislation that will amend –and hopeful consolidate- the EU data protection rules.[326] On 25 January 2012, the Commission put forward a proposal for a new legal framework for data protection in the EU. Despite the expectations for a consolidated regime, the Commission's proposal package includes two separate instruments: A Regulation –aimed to replace the Data Retention Directive- setting out a general framework for data protection,[327] and a Directive – aimed to replace the Data Protection Framework Decision- laying down rules on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.[328]

For the time being, all the current general data protection instruments will be examined in the present Chapter, with the exception of the Data Retention Directive, which will be dealt with separately in Chapter 4. The specific data protection rules of the former third pillar will be addressed by this thesis, only to the extent that they pertain to legal instruments that are under examination.

---

[323] Elspeth Guild & Sergio Carrera, *The European Union's Area of Freedom, Security and Justice Ten Years On*, THE AREA OF FREEDOM, SECURITY AND JUSTICE TEN YEARS ON SUCCESSES AND FUTURE CHALLENGES UNDER THE STOCKHOLM PROGRAMME 1, 4 (Elspeth Guild et al., Centre for European Policy Studies ed. 2010). On the problems of the former third pillar *see* Sionaidh Douglas-Scott, *The Rule of Law in the European Union - Putting the Security into the Area of Freedom, Security and Justice*, 29 E.L. REV. 219, 221 (2004).

[324] PEERS, EU JUSTICE AND HOME AFFAIRS LAW, *supra* note 313, at 883–884.

[325] BOEHM, *supra* note 5, at 120.

[326] PEERS, EU JUSTICE AND HOME AFFAIRS LAW, *supra* note 313, at 883.

[327] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final, Brussels, 25.1.2012.

[328] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM(2012) 10 final, Brussels, 25.1.2012.

1.2.1 The Data Protection Directive

i. Introduction

Directive 95/46/EC[329] (hereinafter the 'Data Protection Directive') constitutes the central legislative measure of the EC data protection regime. It is the first piece of legislation adopted at the EU level concerning the protection of individuals with regard to the processing of personal data, and it is still considered as the most important data protection initiative within the EU[330]- and "the leading force of globalizing data protection"[331] in the rest of the world.

ii. Background to the adoption of the Data Protection Directive

The negotiations for the adoption of the Data Protection Directive,[332] which took almost five years to complete, provide a good example of the different interests and approaches of the three main actors involved in the Community's legislative process.[333] While the European Parliament had adopted as early as the 1970s a clear "fundamental human rights approach,"[334] the Council and the Commission seemed more concerned with "the promotion of a European data processing industry"[335] and the facilitation of transborder data flows.

The European Parliament had asked the Commission three times (in 1976, 1979, and 1982) to propose a directive in order to harmonise the data protection

---

[329] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281 of 23.11.1995, p. 31.

[330] Lee Bygrave, *International Agreements to Protect Personal Data*, GLOBAL PRIVACY PROTECTION THE FIRST GENERATION 15, 31 (James Rule & Graham Greenleaf, 2008).

[331] Michael Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUTER LAW & SECURITY REPORT 508, 512 (2008).

[332] *See* Andrew Charlesworth, *Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?*, 54 HASTINGS L.J. 931 (2003).

[333] On the role of the data privacy authorities for the adoption of the Directive *see* Abraham Newman, *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive*, 62 INTERNATIONAL ORGANIZATION 103, 119 (2008).

[334] DOROTHEE HEISENBERG, NEGOTIATING PRIVACY : THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION 53 (2005); CENTER FOR INTERNATIONAL LEGAL STUDIES, DATA TRANSMISSION AND PRIVACY 150 (Dennis Campbell, 1994).

[335] A NUGTER, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EC: A COMPARATIVE ANALYSIS OF THE PRIVACY STATUTES OF THE FEDERAL REPUBLIC OF GERMANY, FRANCE, THE UNITED KINGDOM, AND THE NETHERLANDS AND THEIR IMPACT ON THE PRIVATE SECTOR 32 (1990).

regulations across the EC. The Commission provided a first draft of a directive harmonizing data protection legislation only in 1990. This draft was largely inspired by the German and French data protection laws, and thus had fundamental rights as its central focus. What has been characterized by an author as "Germany's disproportionate influence"[336] to this first Commission draft was mainly a consequence of the significant contribution of Hesse's data protection commissioner, Spiros Simitis, who acted as the Chairman of the Commission's drafting group. Simitis, who held also the Chair of the Council of Europe's Data Protection Experts Committee, was keen to emphasise the fundamental human rights aspect of the Directive that could not be traded off against other interests.[337] It is hardly surprising that this position was not welcomed by certain Member States and in particular the UK, which did not see any need for harmonisation of data protection rules at the EC level. Furthermore, the Commission's proposal was severely criticised by trade and industry, on the ground that it was too bureaucratic and gave a clear priority to the protection of personal data at the expense of other public policy objectives such as the need of commercial exchange of data.[338]

In view of those criticisms, the Commission submitted in October 1992 a second amended draft. The tensions within the Council between the different Member States were obvious even after this second proposal. The UK continued to object to a directive that would harmonize data protection laws in Europe to a higher than the UK standard degree. However, in the end it chose to abstain from the Directive, rather than to vote against it. The Directive was finally signed by the presidents of the

---

[336] HEISENBERG, *supra* note 334, at 55.

[337] "While the traditional four freedoms may still play a crucial role, the Union's explicit commitment to the fundamentals of a democratic society entails the duty to respect the basic rights of its citizens. Indeed, the Member States, rather than simply relying on the decisions of the European Court, stressed the importance of these rights and the necessity of safeguarding them in the Maastricht Treaty.
Against this background, the Commission not only paved the way for a Directive, but also expressly declared its 1990 proposals to be an immediate consequence of the European Community's duty to guarantee the fundamental rights of its citizens.
The Commission's change of position has … far-reaching consequences… The Commission … must give a clear preference to a regulatory scheme that best secures the protection of the individuals concerned. In other words, the commitment to fundamental rights forces the Commission to achieve not merely some level of protection, but protection of "a high degree," which in the Union's language means the maximum possible." *See* Spiros Simitis, *SYMPOSIUM: DATA PROTECTION LAW AND THE EUROPEAN UNION'S DIRECTIVE: THE CHALLENGE FOR THE UNITED STATES: From the Market To the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 447–448 (1995).

[338] The Union of Industrial and Employers' Confederations in Europe (UNICE) stated in March 1991its objections against the Directive which would potentially lead to 'a fortress Europe' by cutting off data flow to countries that did not have as strict data protection laws. See *Tech Europe*, March 1, 1991.

Council and the European Parliament on 24th October 1995, giving Member States a period of three years for transposition into domestic law. All Member States have implemented Directive 95/46 in their national legislation.[339]

iii. Objectives and legal base

The Data Protection Directive aims to harmonise the different national rules on the protection of personal data, by ensuring at the same time the free movement of such data. In this respect, it can be seen, on the one hand, as a 'negative harmonisation' instrument to the extent that it intends to remove obstacles to the establishment of the internal market by ensuring and facilitating free trade of data between different Member States. However, on the other hand, it can be considered as a measure of 'positive harmonisation' in that it replaces the divergent data protection regimes across the Community with a harmonised EC regulatory framework which establishes a high level of protection of personal data. To this end, Recital 3 of the Directive states that

> "... the establishment and functioning of an internal market in which ... the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded."

This linking by the Directive of the two seemingly conflicting principles of free trade and data protection was not immune from criticism both from the point of view of fundamental rights protection, as well as from the standpoint of business interests. The major concern regarding fundamental rights was whether the protection of the right to data protection was in fact "totally subordinate" to internal market prerogatives.[340] One commentator did not hesitate to characterise the Commission as a "European Midas" in that everything it touches becomes a market."[341] On the other hand, concerns about the need to establish a fundamental right to data protection at the

---

[339] All Member States have implemented Directive 95/46 in their national legislation. *See* 'Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data', available at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm.
[340] SERGE GUTWIRTH, PRIVACY AND THE INFORMATION AGE 91–92 (2002).
[341] *Id.*

EU level were -and still are- also voiced.[342] According to one author, the EU data protection regime imposes an onerous set of requirements on all sectors of industry, from financial institutions to consumer goods companies, and from list brokers to employers.[343]

These criticisms, though, appear rather unsubstantiated, if one takes into account the more than fifteen years of life of the Directive, during which the right to data protection and the internal market freedoms seemed to have co-existed in harmony.[344]

The Directive was intended as a harmonisation instrument and was, therefore, adopted under the legal base of Article 95 of the EC Treaty (now Article 114 TFEU), which concerns the approximation of legislation relating to the internal market. According to Recital 7 of the Directive

> "... the differences in the levels of protection of the rights ...to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; … this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law."

iv. Scope and definitions

The scope of application of the Data Protection Directive is very broad. According to Article 3 (1) it applies "to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."

---

[342] For instance Bergkamp notes that "[d]ata protection as currently conceived by the EU is a fallacy. It is a shotgun remedy against an incompletely conceptualised problem. It is an emotional, rather than rational reaction to feelings of discomfort with expanding data flows. The EU regime is not supported by any empirical data on privacy risks and demand." Bergkamp, *supra* note 13, at 33.

[343] *Id.* at 37. Bergkamp also observes that the "EU policy … is driven by paternalistic motives; individuals need to be protected and be given inalienable but vague fundamental rights, the scope of which government officials define *ex post* in specific cases."

[344] Tzanou, *Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection*, *supra* note 279, at 58.

The Directive applies to the processing of data both in the private and in the public sector. Article 3 (2) lays down the two areas where the Directive does not apply. First, processing of personal data "in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI TEU and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law." Second, the processing of data "by a natural person in the course of a purely personal or household activity" falls outside the scope of application of this Directive.

At the heart of the Directive are the definitions of the notions of 'personal data' and 'processing.' 'Personal data' is defined as "any information relating to an identified or identifiable natural person ('data subject'); 'an identifiable person' is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[345]

'Processing' is understood as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[346]

The Directive grants a number of (primarily procedural) rights to the 'data subject' and imposes obligations on the so-called 'controller' of personal data. The notion of the 'controller' is also very important. 'Controller' is "the natural or legal person, public authority, agency or any other body which alone or jointly with other determines the purposes and means of the processing of personal data."[347] The 'controller' should be distinguished from the 'processor', who according to the Directive, "processes personal data on behalf of the controller."[348] 'Controller' and 'processor' might coincide on one person; if, however, they do not, it is very

[345] Article 2 (a). *See* also Article 29 Working Party, *supra* note 214; Boštjan Berčič & Carlisle George, *Investigating the Legal Protection of Data, Information and Knowledge Under the EU Data Protection Regime*, 23 INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 189 (2009).
[346] Article 2 (b).
[347] Article 2 (d).
[348] Article 2 (e).

important to identify who plays each role. In its Opinion of 16 February 2010 on the concepts of 'controller' and 'processor', the Article 29 Working Party clarified that:

> "The concept of controller is autonomous, in the sense that it should be interpreted mainly according to Community data protection law, and functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis." [349]

Nevertheless, the Working Party recognised that there are difficulties applying the definitions of the Directive "in a complex environment, where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility."[350]

v. Data protection safeguards

Directive 95/46/EC contains a number of principles concerning the legitimate processing of personal data, normally referred to as 'data protection' or 'fair information principles', with which the 'controller' has the obligation to comply[351] (Articles 6 and 7). The Directive is not addressed to 'controllers' directly, but it refers to the Member States that "shall provide" that data must be: processed fairly and lawfully;[352] collected for specified, explicit and legitimate purposes, and not further processed in a way incompatible to those purposes;[353] adequate, relevant, and not excessive in relation to the purposes for which they were collected and/or further processed;[354] accurate, up to date,[355] and kept for no longer than is necessary for the purposes for which they were collected or processed.[356] The notion of consent is also very important in the Directive, which makes processing conditional on the unambiguous consent of the data subject.[357]

---

[349] ARTICLE 29 WORKING PARTY, OPINION 1/2010 ON THE CONCEPTS OF "CONTROLLER" AND "PROCESSOR."
[350] *Id.*
[351] Article 6 (2).
[352] Article 6 (1) (a).
[353] Article 6 (1) (b).
[354] Article 6 (1) (c).
[355] Article 6 (1) (d).
[356] Article 6 (1) (e).
[357] Article 7 (a).

These principles are not, however, without exceptions. For instance, despite the relevant prohibition, data may be further processed for historical, statistical or scientific purposes, even if those are incompatible with the purposes of the initial collection.[358] Furthermore, the rule that processing may take place only where the data subject has given unambiguously his consent is also subject to several exceptions. According to the Directive, data may be processed where processing is necessary: for the performance of a contract to which the data subject is party;[359] for compliance with a legal obligation to which the controller is subject;[360] in order to protect the vital interest of the data subject;[361] for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;[362] and, for the purposes of the legitimate interests pursued by the controller.[363]

Article 8 (1) contains a prohibitory rule: the processing of sensitive data, namely data that reveal "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning sex or health life" is prohibited. Once again, this rule is not without exceptions.[364] Processing of sensitive data is permitted for several different reasons, and the consent of the data subject for the processing of his sensitive data can raise the prohibition.[365]

Article 9 attempts to provide a balance between the right to personal data and the freedom of expression, and it provides for exceptions from data protection principles for the processing of personal data carried out "solely for journalistic purposes or the purpose of artistic or literary expression."[366]

Furthermore, the Directive provides for the rights of the data subject, which, as noted above, are primarily procedural. The data subject has a right to information (Article 10), a right of access (Article 12) and a right to object (Article 14). The right to information obliges the controller to inform the data subject on his identity, the purposes of the processing, and any further issues as necessary. The right of access grants the data subject access to his data that are being processed, to the recipients to

[358] Article 6 (1) (b).
[359] Article 7 (1) (b).
[360] Article 7 (1) (c).
[361] Article 7 (1) (d).
[362] Article 7 (1) (e).
[363] Article 7 (1) (f).
[364] *See* Article 8 (2) and (3).
[365] Article 8 (2) (a).
[366] The interpretation of this Article was subject to a preliminary question in the Case C-73/07 *Satakunnan Markkinapörssi and Satamedia*, judgment of 16 December 2008.

whom the data are disclosed, and to the logic involved in an automating processing. The right to object means that the data subject may "object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him."[367]

An innovative provision is Article 15 which grants to every person the right "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."[368]

The Directive allows the Member States to adopt measures that restrict the rights of the data subjects for several reasons, from the safeguarding of national security and defence, to the ensuring of an important economic or financial interest of a Member State or of the EU.[369]

The Directive imposes a number of further obligations to controllers: confidentiality of processing (Article 16), security of processing (Article 17), and the obligation to notify the supervisory authority before carrying out any processing operation (Article 18).

Chapter III of the Data Protection Directive sets out the judicial remedies available to every person "for any breach of the rights guaranteed him by the national law applicable to the processing in question."[370] Article 23 envisages the possibility of compensation received by the controller for the damage suffered as a result of unlawful processing. Finally, the Directive provides for the adoption of sanctions in case of infringement of its provisions.[371]

[367] Article 14 (a).
[368] For a more detailed analysis of Article 15 of Directive 95/46/EC and for a discussion of the extent to which it applies to automated profiling practices *see* Lee Bygrave, *Automated Profiling. Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUTER LAW & SECURITY REPORT 17 (2001).
[369] Article 13.
[370] Article 22.
[371] Article 24.

vi. Transfer of personal data to third countries

Chapter IV of the Directive regulates the transfer of data to third countries. The regime is substantially different from the free movement of data, which is ensured in the EU due to the harmonised fundamental rights provisions. Personal data can cross the EU's external borders only if an 'adequate level of protection' is ensured in the country of destination. The regulation of transborder data flows is based on a centralised model. According to this, it is the EU institutions that have the final saying on whether a third country ensures adequate protection.

Let us take a closer look at the relevant provisions of the Data Protection Directive. Article 25 (1) sets the general rule, according to which, "the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if ... the third country in question ensures an adequate level of protection." The Member States and the Commission are obliged to inform each other of cases where they consider that a third country does not ensure an adequate level of protection.[372] However, it is the Commission that has the last word on the assessment of the adequacy of the protection provided by a third country, and if it finds that a third country does not ensure adequate protection, Member States must prevent any transfer of data to this country.[373]

The decision on adequacy is taken under a complex comitology procedure, which involves: a proposal from the Commission; an opinion of the Article 29 Working Party; an opinion of the Article 31 Management committee delivered by a qualified majority of Member States; and, a thirty-day right of scrutiny for the European Parliament, to check if the Commission has used its executing powers correctly. The decision is adopted finally by the College of Commissioners.

The central question raised here is what constitutes an 'adequate level of protection' and what criteria should be used to assess adequacy. In this respect, the Directive stipulates that "the adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer...; particular consideration shall be given to the nature of the data, the purpose and the duration of the proposed processing operation, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are

[372] Article 25 (3).
[373] Article 25 (4).

complied with in that country."[374] According to the Working Document adopted by the Article 29 Working Party, a "meaningful analysis of adequate protection must comprise two basic elements: the content of the rules applicable and the means for ensuring their effective application." [375] The Directive's approach to the standard of adequate protection is characterised by Poullet as "open", "functional" and "risk-oriented."[376] Poullet argues, in particular, that "this attitude is the contrary of any EU imperialism as regards the way by which the protection would have to be ensured."[377]

Until the time of the writing, the Commission has recognized Switzerland, Canada, Andorra, Argentina, Guernsey, Isle of Man, Faroe Islands, Israel and Jersey as providing adequate protection. Since the USA lacks comprehensive data protection legislation, an adequacy finding would be difficult in the case. However, in order not to impede international trade, the US-EU Safe Harbor programme was developed. Under Safe Harbor US-based companies can self-certify that they abide with certain data protection principles. In such a way, they are deemed by the Commission as providing for an adequate level of protection, and they can engage, thus, in trade with the EU, avoiding EU data protection restrictions.[378]

However, even when there is no adequate protection, transfers may still take place under the specific circumstances provided for in Article 26 of the Directive. This is the case if: a) the data subject has given his unambiguous consent to the transfer; b) the transfer is necessary for the performance of a contract or for the implementation of pre-contractual measures taken in response to the data subject's request; c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject; d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defence of legal claims; e) the transfer is necessary in order to protect the vital interests of the data subject; and, f) the transfer is made from a register which is

---

[374] Article 25 (2).
[375] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *supra* note 255, at 5.
[376] Yves Poullet, *Transborder Data Flows and Extraterritoriality: The European Position* (Public Seminar of the European Parliament: PNR/SWIFT/Safe Harbour: Are transatlantic data protected? (Transatlantic relations and data protection), March 26, 2007), *available at* http://www.europarl.europa.eu/hearings/20070326/libe/poullet_en.pdf.
[377] *Id.*
[378] Maria Tzanou, *The EU Data Protection Directive as a Model for Global Regimes*, GLOBAL ADMINISTRATIVE LAW: CASES, MATERIALS, ISSUES THIRD EDITION (Sabino Cassese et al.).

intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

The existence of these exceptions is not always enough. For this reason, the Data Protection Directive gives the possibility to Member States to authorise a transfer of personal data to a third country which does not ensure an adequate level of protection, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals; such safeguards may in particular result from appropriate contractual clauses.[379] In this case, the Commission and the other Member States should be informed.[380]

vii. Supervision

The supervision by independent authorities of the compliance of the controllers with the data protection principles is central in the EU data protection regime. In this respect, the Directive stipulates that each Member State must set up a supervisory authority responsible for monitoring the compliance within its territory with the provisions of the Directive.[381] The National Data Protection Authorities (DPAs) are endowed with investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of their supervision duties; powers of intervention, such as, for example, delivering opinions before processing operations are carried out; and, the power to engage in legal proceedings where the national data protection law implementing the Directive has been violated.[382] Furthermore, supervisory authorities can hear claims concerning data protection issues lodged by individuals or associations.[383] Finally, they should issue public reports on their activities at regular intervals.[384]

[379] Article 26 (2).
[380] Article 26 (3).
[381] Article 28.
[382] Article 28 (3).
[383] Article 28 (4).
[384] Article 28 (5).

viii. The Article 29 Data Protection Working Party

Alongside the NDPAs, the Directive establishes also an independent EU Advisory Body on the protection of individuals with regard to the processing of personal data, normally referred to as the 'Article 29 Working Party' or the 'Working Party'. The Working Party is composed of representatives of national data protection authorities, the European Data Protection Supervisor, and the Commission.[385]

Its main tasks, which are laid down in Article 30 of the Directive, consist in examining any question covering the application of the national measures adopted under the Directive in order to contribute to the uniform application of such measures; in providing expert opinions from member state level to the Commission on questions of data protection; in advising the Commission on any proposed measures affecting data protection rights; and in making recommendations on its own initiative on matters relating to the protection of persons with regard to the processing of personal data in the Community.[386]

Even though the Working Party has only advisory competences, it has played an important role in promoting data protection issues within the EU, and has produced a significant number of reports, recommendations and opinions on privacy matters. In addition to that, it must be pointed that the Working Party enhances the co-operation and the informal exchanges of 'best practices' concerning data protection between national Data Protection authorities. In this respect, this unique body of the EU's institutional system contributes to a harmonisation of the interpretation of the provisions of the Data Protection Directive.[387]

1.2.2 "The third generation of EU data protection legislation"[388]: The e-Privacy Directive

On 12 July 2002, the Community lawmaker adopted a data protection legislative instrument that deals with the challenges posed by the new advanced

[385] The Working Party meets in five plenary meetings every year. However, it also progresses on issues through work in subgroup meetings.
[386] Article 30.
[387] *See* Yves Poullet, *The Directive 95/46/EC: Ten Years After*, 22 COMPUTER LAW & SECURITY REPORT 206, 208 (2006).
[388] *Id.* at 216.

digital technologies. Directive 2002/58/EC[389] concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter the 'e-Privacy Directive'), replaces and modifies Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[390] in order to adapt the Community legislation to the developments of the Internet, and thus to "provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used."[391]

The e-Privacy Directive aims at harmonising the different national provisions on the protection of the right to privacy, with respect to the processing of personal data in the electronic communication sector while ensuring the free movement of such data and of electronic communication equipment and services in the Community (Article 1 (1)). In essence, it particularises and complements the provisions of the Data Protection Directive with respect to the processing of personal data of natural persons in the electronic communication sector. However, it goes beyond the Data Protection Directive in many respects, and offers a new approach to the protection of privacy in the information society.[392] For instance, unlike Directive 95/46/EC, which applies only to the processing of data of individuals, the e-Privacy Directive includes in its scope also the protection of legal persons (Article 1 (2)). Furthermore, it regulates unsolicited communications.[393] In particular, according to Article 13 of the ePrivacy Directive, the use of automatic calling machines, fax or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. In addition, the Directive takes into account a number of particularities of the Internet environment such as cookies, spyware, web bugs,

[389] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L201 of 31.07.2002, p.37.
[390] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L24, 30.1.1998, p.1. Directive 97/66/EC translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector.
[391] Recital 4 of Directive 2002/58/EC.
[392] Poullet, *The Directive 95/46/EC: Ten Years After*, *supra* note 387, at 216.
[393] According to Recital 40 of Directive 2002/58/EC, safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment.

hidden identifiers and other similar devices that may seriously intrude upon the privacy of users by entering their terminal without their knowledge in order to gain access to information, to store hidden information or to trace their activities.[394] It allows the use of such devises only for legitimate purposes, with the knowledge of the users concerned.

Naturally, as a former first pillar measure, the ePrivacy Directive, like the Data Protection Directive, does not apply to activities that fall outside the scope of the EC Treaty (Article 1 (3)). According to Article 5 (1) of the e- Privacy Directive Member States shall ensure the confidentiality of communications and the related traffic data[395] through national legislation. In particular, they must prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so. Furthermore, traffic data relating to subscribers and users processed and stored by the provider of a public communications network must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication (Article 6). However, Article 15 enables Member States to adopt legislative measures to restrict the scope of the rights provided for in the Directive "when such restriction 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."

The ePrivacy Directive was amended on 19 December 2009.[396] Under the new regime, communications service providers are required to notify national data protection authorities and consumers of security breaches (Article 4 (3)); legal remedies are provided to natural and legal persons adversely affected by infringements concerning unsolicited communications (Article 13 (6)); enhanced

[394] Recitals 6, 7, 8, 24 and 25.

[395] According to the definition provided in Article 2 (b) of Directive 2002/58/EC 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. *See* also below.

[396] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337/11 of 18.12.2009.

penalties (with the possibility of adoption of criminal sanctions) are laid down for infringements of the Directive (Article 15a (1)); and national data protection authorities receive new enforcement and investigative powers (Article 15a (2, 3, 4)).

1.2.3 Protection of personal data by the Community institutions: the Data Protection Regulation

i. The Regulation 45/2001/EC

Directive 95/46/EC and Directive 2002/58/EC are addressed to the Member States and, accordingly, they do not apply as such to the EU institutions and bodies. However, Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data[397] lays down the data protection rules for the EU institutions.

The Regulation which is based on Article 286 EC, aims at protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data (Article 2). It applies to the processing of such data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law (Article 3). Regulation 45/2001 specifies the data processing obligations of the controllers within the Community institutions and bodies (Articles 5-12), sets out the rights of the data subject (Articles 13-19), provides the individuals with judicial remedies (Article 32) and establishes an independent supervisory authority, the European Data Protection Supervisor (Articles 41-48).

[397] Regulation (EC) 45/2001/EC 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 L 8/1 of 12.1.2001.

ii. The European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) aims to promote a "data protection culture" in Community institutions and bodies. He is the independent authority that ensures at the EU level that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by the EU institutions and bodies. His tasks consist in supervising personal data processing by the institutions or bodies of the Community, in examining the data protection and privacy impact of proposed new legislation, and in cooperating with other data protection authorities, mainly within the platform of the Article 29 Working Party, in order to ensure consistency in the protection of personal data.

Insofar as his supervisory role is concerned, the EDPS undertakes prior checks on the processing of data by Community institutions and bodies and carries out inquiries on complaints received from EU staff members or from other people that allege that their data has been mishandled. Furthermore, the EDPS advises the EU institutions and bodies on data protection issues in a range of policy areas. His consultative role relates to proposals for new legislation as well as soft law instruments like communications that affect personal data protection in the EU. He also monitors new technologies that may have an impact on data protection. Overall, the European Data Protection Supervisor contributes significantly to the establishment of a high level of protection of personal data within the framework of the first pillar can be characterised as significant.[398]

1.2.4 The case-law of the Court of Justice on data protection

Since the adoption of the Data Protection Directive the Court of Justice of the EU has been called upon several times to rule on questions of interpretation and application of the Directive. If we attempt a comment of the Court's reading of the Data Protection Directive, this would be that the Court, in essence, has interpreted an

[398] *See* Hielke Hijmans, *The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority*, 43 COMMON MARKET LAW REVIEW 1313, 1341 (2006).

internal market harmonisation instrument (the Directive) in a manner that fosters the protection of a fundamental right within the Community.[399]

The Court has adopted an expansive reading of the protective scope of the Directive, which goes beyond the exercise of economic activities,[400] and a restrictive one concerning the exemptions not covered by it.[401] The ECJ clarified that the exception of Article 3 (2) applies only to the activities which are expressly listed there. As a result, the Data Protection Directive applies to all the other activities regardless of their connection with the internal market. Thus, it applied to the charitable and religious activities carried out by Mrs Lindqvist, who worked as a volunteer catechist in a parish of the Swedish Protestant Church. Mrs Lindqvist had published on her internet site personal data on a number of people working with her and the ECJ found this activity to fall within the scope of the Data Protection Directive.[402] Furthermore, the Court has held that the processing of personal data files which contain solely, and in unaltered form, material that has already been published in the media, falls within the scope of application of the Data Protection Directive.[403] In this regard, the ECJ stressed that a general derogation from the application of the directive in respect of published information would largely deprive it of its effect. It would be sufficient for the Member States to publish data in order for those data to cease to enjoy the protection afforded by the Directive.[404]

The flexible interpretation adopted by the Court has also opened the way to apply the guarantees offered by the Directive to new technological developments, and in particular the Internet.[405] In this respect, in the same case the Court ruled that information published on a website containing the name, telephone number and the working conditions or hobbies of specified people, was covered by the definition of 'personal data' of Article 2 (a) of the Directive. Furthermore, the placing of this

---

[399] Tzanou, *Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence*, *supra* note 202. As the Data Protection Supervisor P. Hustinx points out: "Data protection is more and more considered as a "horizontal" issue of a wider relevance than the well being of the internal market." *See* Peter Hustinx, *Data Protection in the EU*, P& I 62, 64 (2005).
[400] Joined Cases C-465/00, C-138/01 & C-139/01, *Österreichischer Rundfunk*, Judgment of 20 May 2003, Full Court, [2003] ECR I-4989.
[401] Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.
[402] *Id.*
[403] Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831.
[404] *Id.*
[405] *See Lindqvist*, *supra* note 83.

information in the Internet constituted 'processing of personal data wholly or partly by automatic means'.[406]

When the rights of the Union citizens have been at issue, the ECJ has proved to be even more cautious in its analysis based on the central for the EU legal system principle of non-discrimination on the ground of nationality, and has found suspicious every national measure discriminating against Union citizens from other Member States.[407] In this case, its scrutiny of the national legislation has been stricter, and it has not hesitated to strike down such legislation as incompatible with primary Community law, even though the Member State at issue invoked the argument of the fight against crime which falls outside the scope of the Data Protection Directive.[408]

Moreover, the Court has stressed the need for independence of the national data protection supervisory authorities. The Court has interpreted the notion of "independence" broadly. In this context, it has emphasized that independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance of their tasks.[409]

Concerning the interpretation of the right of access to personal data found in Article 12 of the Data Protection Directive, the Court stated that this right is necessary, on the one hand, to enable the data subject to exercise a number of other rights, such as the rights of rectification, erasure or blockage of data; and on the other hand, to enable the data subject to exercise his right to object to his personal data being processed or his right of action where he suffers damage. Thus, Article 12 (a) requires Member States to ensure a right of access to information not only in respect of the present but also in respect of the past.[410]

The Court has been asked several times to balance the right to data protection with other fundamental rights and freedoms protected within the EC legal order.[411] While it has normally noted the importance of all the fundamental rights at issue, it has avoided pronouncing on the final outcome of this reconciliation. Instead, it has

[406] *Id.*
[407] Case C-524/06 *Huber v Bundesrepublic Deutschland* [2008] ECR I-9705.
[408] *Id.*
[409] Case C-518/07 *Commission v. Germany*, judgment of 9 March 2010.
[410] Case C-553/07 *Rijkeboer* ECR I-3889.
[411] Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-271; C-557/07 *LSG* [2009] ECR I-1227.

left the final decision on the matter to the (referring) national court.[412] This is because, according to the Court, a balance must be found between the rights and interests involved at the stage of the application at national level of the legislation implementing the Data Protection Directive in individual cases. However, it has sought to provide guidance to the national court by stressing the importance of the principle of proportionality. In this regard, certain measures have been found inacceptable by the Court. For instance, it has held that the adoption of a court injunction requiring an Internet Service Provider (ISP) to install a filtering system that monitors, without any limitation in time, all the electronic communications made through the network of the ISP in the interests of copyright rightholders, would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other, and therefore is precluded from the relevant EU legislation.[413]

The Court has also noted that "not all personal data are capable by their nature of undermining the private life of the person concerned,"[414] and has ruled in favour of the disclosure of the names of the representatives in the Commission meeting according to the fundamental right to access to the EU documents. The Court has stressed, however, that no automatic priority can be conferred on the objective of transparency over the right to protection of personal data, even if important economic interests are at stake.[415]

The ECJ has shown itself to be very sensitive in cases that concern the balancing between the freedom of expression, and more particularly, journalism, on the one hand, and data protection on the other.[416] In these cases, it seemed ready to accept an exception from data protection rules.[417]

Finally, the Court has ruled on which pillar different types of processing fall. While it has held that the transfer of airline passenger data to the US law enforcement

---

[412] Bignami notes that in cases that present ""tough constitutional questions" like the balance between privacy and freedom of expression, the ECJ, by sending the questions back to the national Court, gives precedence to national constitutionalism. In this way, it affirms a set of principles common to the entire EU, yet it also defers to national constitutional values. This shows that the Court tolerates constitutional diversity." *See* Francesca Bignami, *The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts*, 41 CORNELL INTERNATIONAL LAW JOURNAL 211, 237 (2008).
[413] Case C-70/10 *Scarlet Extended*, judgment of 24 November 2011.
[414] Case C- 28/08P *Bavarian Lager II,* judgment of 29 June 2010.
[415] Joined Cases C-92/09 and C-93/09 *Schecke*, judgment of 9 November 2010.
[416] *See Satakunnan Markkinapörssi and Satamedia*, *supra* note 85.
[417] *Id.*

authorities falls outside the scope of the Data Protection Directive;[418] it has found that the retention of traffic and location data by the telecommunications service providers for law enforcement purposes falls within the Community powers.[419]

1.2.5 The Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation

i. Background

The adoption of the framework decision took three years of vigorous discussions. The Commission submitted its proposal in October 2005 and the Council adopted finally the framework decision in its meeting on 27-29 November 2008. The European Parliament was consulted twice on the data protection framework decision: once in September 2006 and a second time in June 2007. The European Data Protection Supervisor issued three Opinions[420] in which while he welcomed the importance of the proposal as a considerable step forwards for the protection of personal data in an important area, he expressed his concerns that developments in the negotiations in the Council were leading towards a level of protection of personal data not only below the standards laid down in the Data Protection Directive, but also incompatible with the more generally formulated Council of Europe Convention No 108.[421]

---

[418] Joined Cases C-317/04 and C-318/04, *European Parliament* v. *Council and Commission (PNR)*, Judgment of the Grand Chamber of 30 May 2006, [2006] ECR I-4721. *See* below.

[419] Case C-301/06 *Ireland v. European Parliament and Council*, Judgment of the Grand Chamber of 10 February 2009. *See* below.

[420] *See* Opinion on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005) 475 final) (2006/C 47/12), OJ C 47/27 of 25.2.2006; Second opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (2007/C 91/02), OJ C 91/9 of 26.4.2007; Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (2007/C 139/01), OJ C 139/1 of 23.6.2007.

[421] *See* Joaquín Bayo Delgado, *The Area of Freedom, Security and Justice and the Role of National Courts in the EU Data Protection System*, THE AREA OF FREEDOM, SECURITY AND JUSTICE TEN YEARS ON SUCCESSES AND FUTURE CHALLENGES UNDER THE STOCKHOLM PROGRAMME 31, 35 (Elspeth Guild et al., Centre for European Policy Studies ed. 2010); PEERS, EU JUSTICE AND HOME AFFAIRS LAW, *supra* note 313, at 921.

ii. Aim and scope

The purpose of the Framework Decision is to "ensure a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters..., while guaranteeing a high level of public safety."[422] It applies to personal data that are exchanged within the framework of police and judicial cooperation[423] for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Framework Decision allows the Member States to provide for higher-level safeguards for protecting personal data than those established in this instrument.

The scope of application of the Framework Decision is limited. First, it applies only to transborder flows of data between the law enforcement authorities of the Member States, and does not cover the collection and processing of personal data at national level. Second, it does not affect the relevant set of sector-specific data protection regimes found in the acts governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS).[424] Third, the Framework Decision applies "without prejudice to essential national security interests and specific intelligence activities in the field of national security."[425] Forth, it is also "without prejudice to any obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements with third States" existing at the time of its adoption.[426]

iii. Content

Most of the substantive provisions of the Framework Decision seek to mirror the data protection safeguards stipulated in the Data Protection Directive. The

[422] Article 1 (1).
[423] According to Article 1 (2) the framework decision applies a) to the personal data transmitted or made available between Member States; b) to personal data transmitted or made available by Member States to authorities or to information systems established on the basis of Title VI TEU; and c) to personal transmitted or made available to the competent authorities of the Member States by authorities or information systems established on the basis of the TEU or the EC Treaty.
[424] Recital 39.
[425] Article 1 (4).
[426] Article 26.

Decision provides for the principles of lawfulness, proportionality and purpose limitation (Article 3); the rectification, erasure and blocking of data (Article 4); the right of information (Article 16), the right of access (Article 17), the right to rectification, erasure or blocking (Article 18), the right to compensation (Article 19); judicial remedies (Article 20); and, the establishment of national supervisory authorities, responsible for advising and monitoring the application of the Framework Decision within the territory of each Member State (Article 25).

The safeguards may be there, but they are fraught with exceptions or their content is significantly different from that found in the provisions of the Data Protection Directive.[427] For instance, while the Framework Decision establishes that "personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected";[428] the second paragraph of the same Article comes to introduce several exceptions, where further processing for another purpose shall be permitted. The same applies to the rights of the data subjects. In this respect, the right of access can be restricted for reasons such as obstruction of official or legal inquiries, investigations or procedures, public security, national security, and the protection of the data subject or the rights and freedoms of others.[429] Numerous other provisions of the Framework Decision suffer from the same problem.[430] Exceptions to data principles are too many and too often.

Concerning sensitive data, the Framework Decision stipulates that their processing "shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards." This, of course, contradicts the in-principle prohibition rule laid down both by Article 8 of the Data Protection Directive and by Article 6 of Convention 108, pursuant to which sensitive data may not be processed unless in certain cases provided specifically by the law and respecting a number of safeguards. The same applies to the rule of prohibition of the automated

---

[427] De Hert and Papakonstantinou comment: "data protection principles were compromised in the final text of the DPFD. Almost each and every one of them comes with an exemption that opens the door to the police to do otherwise than the principle prescribes, if they see fit." *See* Paul De Hert & Vagelis Papakonstantinou, *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*, 25 COMPUTER LAW & SECURITY REPORT 403, 411 (2009).

[428] Article 3 (1).

[429] Article 17 (2). *See* also Conny Rijken, *Re-Balancing Security and Justice: Protection of Fundamental Rights in Police and Judicial Cooperation in Criminal Matters*, 47 COMMON MARKET LAW REVIEW 1455, 1469 (2010).

[430] *See* Articles 4 (2), 8, 11, and 16 (2).

processing of data found in Article 15 of the Data Protection Directive. In this respect, the Framework Decision provides that automated processing "shall be permitted if authorised by a law."[431]

While on the one hand, data protection principles are "emptied"[432] of their essential core through a number of exceptions, on the other hand, the Framework Decision includes an innovative provision on the sharing of information with the private sector, creating, thus, public-private partnerships to fight crime.[433]

iv. Transborder data flows

The regulation of the transfer of data to third states or international bodies is found in Article 13 of the Framework Decision. According to this, personal data transmitted or made available by the competent authority of another Member State may be transferred to third States or international bodies, only if a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; b) the receiving authority in the third State or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; c) the Member State from which the data were obtained has given its consent to transfer in compliance with its national law; and d) the third State or international body concerned ensures an adequate level of protection for the intended data processing. However, prior consent is not needed when the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and it cannot be obtained in good time. In this case, the authority responsible for giving consent should be informed without delay.[434]

---

[431] Article 7.
[432] De Hert & Papakonstantinou, *supra* note 427, at 411.
[433] Article 14. As Recital 17 to the Framework Decision explains: "in many cases the transmission of personal data by the judiciary, police or customs to private parties is necessary to prosecute crime or to prevent an immediate and serious threat to public security or to prevent serious harm to the rights of individuals, for example, by issuing alerts concerning forgeries of securities to banks and credit institutions, or, in the area of vehicle crime, by communicating personal data to insurance companies in order to prevent illicit trafficking in stolen motor vehicles or to improve the conditions for the recovery of stolen motor vehicles from abroad."
[434] Article 13 (2).

The Framework Decision provides for a number of derogations, whereby personal data can be transferred to third countries even if these do not ensure an adequate level of protection. This may happen if: a) the national law of the Member State transferring the data so provides because of: i) legitimate specific interests of the data subject; or ii) legitimate prevailing interests, especially important public interests; or b) the third State or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law.[435]

Once again the provisions of the Framework Decision seem to fall short the relevant stipulations of the Data Protection Directive under the former first pillar. Although the Decision provides that transborder data flows should take place when the third State or the international body concerned ensures an adequate level of protection, the adequacy decision is not taken in this case under the centralised model of the Data Protection Directive. Instead, the absence of a harmonised system means that each Member State will assess at its own discretion the level of adequacy provided for by the third country or international organisation.[436] As a consequence, the list of adequate countries and international organisations to which a transfer is allowed will considerably vary from Member State to Member State.[437]

[435] Article 13 (3).

[436] As Rijken notes, this might lead to a "jumble of bilateral relations with third countries." Rijken, *supra* note 429, at 1470. *See* also Els de Busser & Gert Vermeulen, *Towards a Coherent EU Policy on Outgoing Data Transfers for Use in Criminal Matters? The Adequacy Requirement and the Framework Decision on Data Protection in Criminal Matters*, EU AND INTERNATIONAL CRIME CONTROL: TOPICAL ISSUES 95, 110 (Governance of Security (Gofs) Research Paper Series, Vol. 4 ed. 2010).

[437] *See* Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matter, *supra* note 102, para 27.

Chapter 3. EU Counter-terrorism and its particularities

> *"The EU counter-terrorism and police co-operation measures are based largely on the gathering and exchange of personal data. This may lead to maximisation of surveillance via the collection of a wide range of personal data and thus pose significant challenges to privacy and data protection. This is true in particular in the light of the fragmentation of the EU data protection framework applying to the various databases and forms of information exchange."*[438]

1. The European Union's Counter-Terrorism Policy

It has been repeatedly argued by the mass media that "9/11 was the day that changed the world..." Ironically enough, for the EU's counter-terrorist policies this statement seems to be true. Although a form of counter-terrorism cooperation[439] existed in the EU since 1975 with the establishment of the Terrorism, Radicalism, Extremism, and International Violence group, the TREVI group;[440] this was rather loose since it "did not involve EC competences and institutions and had no legal base."[441] The TREVI group and other forms of EU counter-terrorism co-operation[442] may have gone a long way since 1975, but September 11, 2001 brought up a new phase in the EU's fight against terrorism,[443] characterised by "an unprecedented

---

[438] VALSAMIS MITSILEGAS & ANNELIESE BALDACCINI, INTERDEPENDENCE OF THE VARIOUS INITIATIVES AND LEGISLATIVE PROPOSALS IN THE FIELDS OF COUNTER-TERRORISM AND POLICE CO-OPERATION AT THE EUROPEAN LEVEL 11 (Briefing Note requested by the European Parliament's LIBE Committee, October 2007).

[439] On the EU and its Internal Security Srategy in general *see* VALSAMIS MITSILEGAS ET AL., THE EUROPEAN UNION AND INTERNAL SECURITY : GUARDIAN OF THE PEOPLE? (2003).

[440] The TREVI group consisted of European police officers that exchanged information on terrorism and international crimes. *See* Davide Casale, *EU Institutional and Legal Counter-terrorism Framework*, 1 DEFENCE AGAINST TERRORISM REVIEW 49, 50 (2008).

[441] Jörg Monar, *Common Threat and Common Response? The European Union's Counter-Terrorism Strategy and Its Problems*, 42 GOVERNMENT AND OPPOSITION 292, 293 (2007); Jörg Monar, *The Dynamics of Justice and Home Affairs: Laboratories, Driving Factors and Costs*, 39 JOURNAL OF COMMON MARKET STUDIES 747, 750 (2001).

[442] For instance the Police Working Group on Terrorism and the Counter Terrorist Group.

[443] CHRISTINA ECKES, EU COUNTER-TERRORIST POLICIES AND FUNDAMENTAL RIGHTS: THE CASE OF INDIVIDUAL SANCTIONS (2009); Monica den Boer et al., *Legitimacy Under Pressure: The European*

acceleration of political decision making... of counterterrorism measures and instruments in Europe."[444]

In its extraordinary meeting of 21st September 2001, the European Council having described the 9/11 attacks as "an assault on our open, democratic, tolerant and multicultural societies", and "a challenge to the conscience of each human being",[445] held that

> "[t]errorism is a real challenge to the world and to Europe... the fight against terrorism will, more than ever, be a priority objective of the European Union."[446]

The EU agreed on its own common definition of terrorism[447] on 13 June 2002 with the adoption of the Framework Decision on combating terrorism.[448] The Framework Decision described terrorism as "one of the most serious violations" of the principles of democracy and the rule of law,[449] and called upon the Member States to impose penalties and sanctions against terrorist offences.[450]

Web of Counter-Terrorism Networks, 46 JOURNAL OF COMMON MARKET STUDIES 101 (2007); Evelien Brouwer, *Immigration, Asylum and Terrorism: A Changing Dynamic Legal and Practical Developments in the EU in Response to the Terrorist Attacks of 11.09*, 4 EUROPEAN JOURNAL OF MIGRATION AND LAW 399 (2003).

[444] Doron Zimmermann, *The European Union and Post-9/11 Counterterrorism: A Reappraisal*, 29 STUDIES IN CONFLICT & TERRORISM 123, 126 (2006).

[445] Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001 (EU Council document SN 140/01), at 1.

[446] *Id.*

[447] The EU defines terrorist offenses as "offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of: seriously intimidating a population, or unduly compelling a Government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation, shall be deemed to be terrorist offences: (a) attacks upon a person's life which may cause death; (b) attacks upon the physical integrity of a person; (c) kidnapping or hostage taking; (d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss; (e) seizure of aircraft, ships or other means of public or goods transport; (f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons; (g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life; (h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life; (i) threatening to commit any of the acts listed in (a) to (h)."

[448] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism OJ L 164/3 of 22.6.2002.

[449] *See* Recitals 1 and 2 of the Framework Decision on combating terrorism.

[450] Article 5 of the Framework Decision on combating terrorism.

The European Security Strategy adopted on 12 December 2003,[451] identified terrorism as "a growing strategic threat to the whole of Europe"[452] that constitutes both "a target and a base" for terrorism.[453] The Strategy did not approach terrorism as an individualised threat, but it linked it with other events that take place internationally, such as the proliferation of weapons of mass destruction, regional conflicts, state failure and organised crime.[454] In this respect, the Strategy found that the Union was "particularly well equipped to respond to such multi-faceted situations", and held that "dealing with terrorism may require a mixture of intelligence, police, judicial, military and other means."[455]

The Madrid attacks of March 2004 and the London attacks of July 2005 provided new impetus to the EU's counter-terrorism policies.[456] The position of the EU Counter-terrorism coordinator was created,[457] and on 15 December 2005, the European Council adopted the EU's response to terrorism, the EU Counter-Terrorism Strategy.[458] The Strategy recognises that terrorism constitutes a particular threat for Europe internally and externally.[459]

> "The European Union is an area of increasing openness, in which the internal and external aspects of security are intimately linked. It is an area of increasing interdependence, allowing for free movement of people, ideas, technology and resources. This is an environment which terrorists abuse to pursue their

[451] A Secure Europe in a Better World. European Security Strategy, Brussels, Council of the European Union, 12 December 2003.
[452] *Id.* at 3. "Increasingly, terrorist movements are well-resourced, connected by electronic networks, and are willing to use unlimited violence to cause massive casualties."
[453] *Id.*
[454] *Id.* at 5.
[455] *Id.* at 7.
[456] *See* DIDIER BIGO & SERGIO CARRERA, FROM NEW YORK TO MADRID: TECHNOLOGY AS THE ULTRA-SOLUTION TO THE PERMANENT STATE OF FEAR AND EMERGENCY IN THE EU (CEPS Commentary, 2004); Monica den Boer, *Fusing the Fragments. Challenges for EU Internal Security Governance on Terrorism*, INTERNATIONAL TERRORISM : A EUROPEAN RESPONSE TO A GLOBAL THREAT? 83 (Dieter Mahncke & Jörg Monar, 2006).
[457] Gilles de Kerchove & Serge de Biolley, *The EU Counter-Terrorism Coordinator*, THE INSTITUTIONAL DIMENSION OF THE EUROPEAN UNION'S AREA OF FREEDOM, SECURITY AND JUSTICE 233 (Jörg Monar, 2010); Lauri Lugna, *Institutional Framework of the European Union Counter-Terrorism Policy Setting*, 8 BALTIC SECURITY & DEFENCE REVIEW 101, 111–112 (2006).
[458] The European Union Counter-terrorism Strategy, Council document 14781/1/05, 24 November 2005.
[459] *See* Daniel Keohane, *Implementing the EU's Counter-Terrorism Strategy. Intelligence, Emergencies, and Foreign Policy*, INTERNATIONAL TERRORISM : A EUROPEAN RESPONSE TO A GLOBAL THREAT? 63 (Dieter Mahncke & Jörg Monar, 2006).

objectives. In this context concerted and collective European action, in the spirit of solidarity, is indispensable to combat terrorism."[460]

The purpose of EU's Counter-Terrorism Strategy is, therefore to

"combat terrorism globally while respecting human rights, and make Europe safer, allowing its citizens to live in an area of freedom, security and justice."[461]

The EU counter-terrorism strategy is built around four strands: Prevent (radicalisation and recruitment); Protect (citizens and critical infrastructure from terrorist attacks); Pursue (terrorists across borders and globally); and Respond (to the consequences of terrorist attacks by improving the capabilities to deal with the aftermath).[462] The EU has also in place an Action Plan against terrorism,[463] which comprises over 100 measures on fighting terrorism internally and externally.[464] The Action contains besides legislative also operational measures against terrorism.[465]

2. The Particularities of the EU's Counter-Terrorism Regime

Counter-terrorism may well be high on the EU's political agenda, but the EU's ability to turn political goals into actual legislative measures is limited in this field for two major reasons. First and most important, the EU is not a State[466] and therefore it cannot ensure directly security by itself.[467] The EU "cannot arrest or prosecute terrorists, nor can it use spies or satellites to track them",[468] since there are no

[460] EU Counter-terrorism Sreategy, para 2.
[461] *Id.* at 1.
[462] *Id.*
[463] Commission document SEC(2006) 686, EU Council document 10043/06, 31 May 2006. For a commentary *see* Hans G. Nilsson, *The EU Action Plan on Combating Terrorism. Assessment and Perspectives*, INTERNATIONAL TERRORISM : A EUROPEAN RESPONSE TO A GLOBAL THREAT? 73 (Dieter Mahncke & Jörg Monar, 2006).
[464] *See* Monar, *Common Threat and Common Response?*, *supra* note 441, at 303; Raphael Bossong, *The Action Plan on Combating Terrorism: A Flawed Instrument of EU Security Governance*, 46 JOURNAL OF COMMON MARKET STUDIES 27 (2007).
[465] Monar, *Common Threat and Common Response?*, *supra* note 441, at 306.
[466] As Gijs de Vries, former Counter-Terrorism Coordinator of the EU explained to an American audience, "we are not the United States of Europe . . . we do not have an EU police force, or an EU army." *See* Gijs de Vries, *European Strategy in the Fight Against Terrorism and the Co-operation with the United States* (Center for Strategic and International Studies (CSIS) European Dialogue Lunch, May 13, 2004).
[467] Maria Tzanou, *The EU as an Emerging "Surveillance Society": The Function Creep Case Study and Challenges to Privacy and Data Protection*, 4 VIENNA ONLINE JOURNAL OF INTERNATIONAL CONSTITUTIONAL LAW 407, 413 (2010).
[468] DANIEL KEOHANE, THE EU AND COUNTER-TERRORISM 2 (Centre for European Reform- Working Paper, May 2005).

European police or law enforcement authorities with executive powers to do so.[469] The EU's contribution to counter-terrorism is limited, therefore, to the adoption of measures that are intended to enable the authorities of the Member States to fight terrorism themselves.[470] In this respect, the EU has laid down several legislative instruments aimed to harmonise, coordinate and facilitate the Member States' action against terrorism.[471] The main focus of such instruments will be explained in the following section; also, the present thesis utilises some examples of these measures as case-studies affecting the rights to privacy and data protection.

A second limitation is that counter-terrorism is not a defined EU competence or policy area.[472] This is due to a number of reasons. As criminal law, counter-terrorism is a contested field of EU action because it goes to the core of national sovereignty.[473] It is not easy, therefore, for Member States to grant powers to the EU that might interfere with their existing laws and national security practices.[474] As Valsamis Mitsilegas astutely explains with regard to criminal law, the reason for this is *legitimacy* of power.

> "The acceptance by citizens of the democratically negotiated powers of the State in criminal matters grants *legitimacy* to State power, which in turn reinforces sovereignty translated into the capacity of the State to impose power. It comes thus as no surprise that the prospect of the transfer of power in the criminal law field from the State to the Union level has been met with consistent and considerable resistance by Member States, with sovereignty concerns being

---

[469] Hielke Hijmans & Alfonso Scirocco, *Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?*, 46 COMMON MARKET LAW REVIEW 1485, 1490 (2009).

[470] Giovanni Buttarelli, *Legal Restrictions – Surveillance and Fundamental Rights* (New Technical Means of Surveillance and the Protection of Fundamental Rights - Challenges for the European Judiciaries, June 19, 2009), *available at* http://www.richtervereinigung.at/images/Texte/NTMoS/fg%20grundrechte_tagung%2019%2006%202009_buttarelli_speech.pdf; Hijmans & Scirocco, *supra* note 469, at 1490; Tzanou, *The EU as an Emerging "Surveillance Society": The Function Creep Case Study and Challenges to Privacy and Data Protection*, *supra* note 467, at 414.

[471] Tzanou, *The EU as an Emerging "Surveillance Society": The Function Creep Case Study and Challenges to Privacy and Data Protection*, *supra* note 467, at 414.

[472] Keohane, *The EU and Counter-terrorism*, *supra* note 468, at 2–3.

[473] Monar notes: "While agreeing on certain common principles, objectives, mechanisms and even institutional structures, the EU Member States have certainly so far resisted the creation of any 'integrated'- in the supranational sense – system of anti-terrorism capabilities." Jörg Monar, *International Terrorism- A "European Response" to a Global Threat?*, INTERNATIONAL TERRORISM : A EUROPEAN RESPONSE TO A GLOBAL THREAT? 151, 153 (Dieter Mahncke & Jörg Monar, 2006).

[474] Keohane, *The EU and Counter-terrorism*, *supra* note 468, at 3.

at the heart of every single attempted step to bring criminal law within the realm of the European Union."[475]

The same reasoning applies to counter-terrorism, irrespective of whether this is to be considered as an aspect of criminal law or a different policy area. The resistance of the Member States to transfer the relevant powers to the EU is demonstrated in various ways. First, counter-terrorism measures fell normally in the framework of the intergovernmental pillars: they were adopted primarily within the Area of Freedom, Security and Justice, (and secondary the Common Foreign and Security Policy), i.e. (the former) third and (second) pillars, which required unanimity and lacked democratic scrutiny and judicial control. It is not excluded that counter-terrorism measures could be adopted under the (former) first Community pillar or under a bridge of different pillars, but the diverse pillar structure demonstrated at least in the pre-Lisbon era that counter-terrorism spanned in a number of policy areas of the EU and could be adopted under different levels of cooperation: from harmonisation when the regulation of economic activities is at stake –for example, in the case of the Data Retention Directive- to mere cooperation and coordination when the Member States felt that their sovereignty could be impinged upon.[476] Second, despite the EU's increasing enthusiasm to adopt counter-terrorism measures, commentators observe that, paradoxically enough, the implementation of these is often poor.[477]

Despite these limitations, the EU can play a crucial role in combating terrorism through the creation of a common area of information exchange. Why this constitutes the major contribution of the EU to counter-terrorism will be discussed in the following section.

---

[475] VALSAMIS MITSILEGAS, EU CRIMINAL LAW 321 (2009).

[476] Monar notes that "the EU's response is based on cooperation and coordination rather than on any form of integration." *See* Monar, *Common Threat and Common Response?*, *supra* note 441, at 309.

[477] This might also be due to the differences in the threat perceptions of terrorism among the EU Member States. For an interesting analysis on the issue *see* Edwin Bakker, *Differences in Terrorist Threat Perceptions in Europe*, INTERNATIONAL TERRORISM : A EUROPEAN RESPONSE TO A GLOBAL THREAT? 47 (Dieter Mahncke & Jörg Monar, 2006). On the issue also Monar, *Common Threat and Common Response?*, *supra* note 441, at 310.

3. The importance of information exchange in countering terrorism

One of the primary aims of the EU's counter-terrorism policies –but also of counter-terrorism measures in general- is to prevent future attacks, rather than to solve crimes after they occur.[478] It is self-evident why information is crucial for this purpose.[479] The nexus between counter-terrorism and information sharing was stressed by the Commission in its Communication of 10 June 2009 on an area of freedom, security and justice serving the citizen:

> "security in the EU depends on effective mechanisms for *exchanging information* between national authorities and other European players. To achieve this, the EU must develop a European information model based on a more powerful strategic analysis capacity and better gathering and processing of operational information."[480]

Along the same lines, the Stockholm Programme,[481] the EU's five-year plan (2010-2015) in the Area of Freedom, Security and Justice states that

> "[s]ecurity in the Union requires an integrated approach where security professionals share a common culture, pool information as effectively as possible and have the right technological infrastructure to support them."

Furthermore, preventing terrorist attacks means that information should be collected and analysed proactively. [482] For this reason, the main focus of EU counter-terrorism measures[483] has been the facilitation of the 'free movement of information' by enabling the Member States to collect, analyse and exchange information -in many cases- on the basis of a *proactive* and *intelligence-led* approach.[484] As a commentator

---

[478] Helen Fenwick, *Proactive Counter-terrorist Strategies in Conflict with Human Rights*, 22 INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 259, 259 (2008).

[479] The former EU Counter-Terrorism Coordinator Gijs de Vries could not have put it more accurately: "[t]imely and accurate information-its collection, analysis and dissemination-is essential to prevent acts of terrorism and to bring terrorist suspects to justice." Gijs de Vries, *The European Union's Role in the Fight Against Terrorism: [Opening Address - The Role of the EU in the Fight Against Terrorism]*, 16 IRISH STUDIES IN INTERNATIONAL AFFAIRS 3, 3 (2005).

[480] COM 2009 (262) final, p. 16. Emphasis added.

[481] European Council, The Stockholm Programme- An Open and Secure Europe Serving and Protecting Citizens (2010/C 115/01) OJ C 115/1 of 4.5.2010.

[482] COUNTER-TERRORISM COORDINATOR, IMPLEMENTATION OF THE EU COUNTER-TERRORISM STRATEGY - DISCUSSION PAPER 3 (Council doc. 15448/07, November 23, 2007).

[483] This does not mean that the EU does not have other counter-terrorism measures, such as for instance the highly controversial terrorist sanctions.

[484] *See* Stockholm Programme, *supra* note 164, para 4.1 (emphasis added). As the Counter-Terrorism Coordinator explains "[o]ne of the major specific features of investigations into terrorism cases, particularly with a proactive approach, is the need for frequent recourse to special investigation methods such as the interception of telecommunications..." Counter-terrorism Coordinator, *supra* note 482, at 3.

has correctly noted, of the four strands of the EU's counter-terrorism strategy (Prevent, Protect, Pursue and Respond),

> "information exchange *subsumes* the others. Indeed, the prevention of radicalisation, border management and the protection of critical infrastructures depend, to a large extent, on the exchange of information under different schemes established by the EU."[485]

In particular, the EU has "created an extensive toolbox for collecting, processing and sharing information between national authorities and other European players in the area of freedom, security and justice."[486] The legal base for the exchange of information for police cooperation purposes is currently found in Article 87 (2) (a) TFEU.[487] Article 87 provides:

> "1. The Union shall establish police cooperation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences.
>
> 2. For the purposes of paragraph 1, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures concerning:
>
> (a) the collection, storage, processing, analysis and exchange of relevant information."

The other measures that can be adopted in the context of police cooperation under Article 87 (2) are more operational and entail, for instance, support for the training of staff, cooperation on the exchange of staff, and common investigative techniques in relation to the detection of serious forms of organised crime.

4. Channels of information exchange

In July 2010, the Commission issued a Communication to the Parliament and the Council, providing "a full overview of the EU-level measures in place, under

---

[485] Thierry Balzacq, *The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies*, 46 JOURNAL OF COMMON MARKET STUDIES 75, 77 (2007). Emphasis added.
[486] Stockholm Programme, *supra* note 164.
[487] The relevant legal base for judicial cooperation is Article 82 (1) (d).

implementation or consideration that regulate the collection, storage or cross-border exchange of personal information for the purpose of law enforcement or migration management."[488] In this Communication, having noted the importance of information exchange for the internal market,[489] the Commission went on to state that

> "[t]he terrorist attacks in the United States in 2001, as well as the bombings in Madrid and London in 2004 and 2005, triggered *another dynamic* in the development of Europe's information management policies."[490]

There are multiple channels of information exchange in the EU. The 'Hague Programme', the EU's five year (2005-2010) Action Plan for Freedom, Justice and Security that was adopted on 5 November 2004 by the European Council in response to the 'war on terrorism',[491] introduced the so-called 'principle of availability', which purported to be the governing standard for information flows throughout the Union. According to this principle, "a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State."[492]

The 'Stockholm Programme', which is the EU's five year plan for Justice and Home Affairs for 2010-2014, endorsed an even more powerful vision of information sharing possibilities. In the Programme, the European Council called for a definition of a comprehensive EU internal security strategy based, *inter alia*, on a proactive and intelligence-led approach, that requires stringent cooperation between EU agencies, including a further improving of their information exchange.[493] In this respect, the European Council invited the Council and the Commission to adopt and implement an EU Information Management Strategy that should be based among others on business-driven development (a development of information exchange and its tools that is driven by law enforcement needs), guiding principles for a policy on the exchange of information with third States for law enforcement purposes,

---

[488] Communication from the Commission to the European Parliament and the Council, Overview of information management in the area of freedom, security and justice COM(2010)385 final.
[489] *Id.* "Neither the Schengen area nor the EU internal market could function today without cross-border data exchange."
[490] *Id.* Emphasis added.
[491] The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53/1 of 3.3.2005.
[492] *Id.*
[493] Stockholm Programme, p. 36.

interoperability of IT systems, a rationalisation of the different tools, including the adoption of a business plan for large IT systems, and overall coordination, convergence and coherence. The European Council also called for the establishment of an administration, having the competence and capacity to develop technically and manage large-scale IT-systems in the area of freedom, security and justice.

The exchange of information for security purposes in the Area of Freedom, Security and Justice,[494] involves various different actors. The actors that take part in the EU's information exchange architecture are four: the EU, its Member States, private parties, and third countries (or international organisations). This leads to different exchange possibilities: reciprocal data transfers between Member States and EU institutions in the framework of EU-centralised databases; exchanges of information between Member States and private actors (public/private partnership in combating terrorism and crime); data transfers between private actors and third countries; and, the exchanges of data between Member States themselves.

The relevant measures for the exchange of information are numerous. In 2006, the Data Retention Directive was adopted in order to facilitate the Member States' fight against terrorism and serious crime through the retention of telecommunications' data.[495] The principle of availability stipulated in the Hague Programme was mainly implemented in the so-called 'Swedish framework decision', which simplifies the exchange of information and intelligence between the law enforcement authorities of the Member States.[496] In 2008, the EU endorsed the Prüm Decision[497] for the speeding up of the exchange of DNA profiles, fingerprints and vehicle registration data in order to fight terrorism and other forms of crime. The EU has also established several databases to support the implementation of its policies in the field of immigration, visa, asylum, and law enforcement. Currently, a number of EU databases and systems of cross-border information exchange are already in place, while others are envisaged to become operational soon. Those include the Schengen Information System (SIS),

[494] On the Area of Freedom, Security and Justice *see* Jörg Monar, *The Institutional Framework of the AFSJ Specific Challenges and Dynamics of Change*, THE INSTITUTIONAL DIMENSION OF THE EUROPEAN UNION'S AREA OF FREEDOM, SECURITY AND JUSTICE 21 (Jörg Monar, 2010).
[495] For an analysis *see* below.
[496] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union OJ L386/89 of 29.12.2006.
[497] 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 L 210/1 of 6.8.2008. The Decision implemented the Prüm Treaty that was signed in 2005 by Germany, Spain, France, Luxembourg, the Netherlands, Austria and Belgium.

the Visa Information System (VIS), EURODAC, the Customs Information System (CIS), the Europol Computer System, and the Eurojust files. These store data, inputted by the Member States, and provide access to them for a number of purposes, among which also law enforcement.[498] Furthermore, the EU has put in place Financial Intelligence Units (FIUs) for the purpose of combating money laundering and terrorist financing.[499] Finally, the EU has concluded international agreements for the exchange of personal data with third countries. In particular, the EU has agreed on the transfer of Passenger Name Record (PNR) data to the US, Canada and Australia, and the transfer of financial transactions data to the US under the Terrorist Finance Tracking Programme (TFTP).[500]

This Chapter sought to demonstrate that information exchange can be considered as a part of the EU's counter-terrorism measures. In fact, even more than that: information exchange can be regarded as a cornerstone of the EU's counter-terrorism strategy, taking into account the limitations that the EU faces in adopting and implementing operational measures, and the added value of information in the pro-active approach to terrorism. But, this does not constitute the main focus of the present analysis. As already mentioned, the present thesis will discuss in Part II the added value of the fundamental right to data protection in the context of four specific case-studies of information exchange: the Data Retention Directive, the exchange of information through the databases of SIS II, VIS and EURODAC, the EU-US PNR Agreements, and the EU-US TFTP Agreements.

---

[498] FLORIAN GEYER, TAKING STOCK: DATABASES AND SYSTEMS OF INFORMATION EXCHANGE IN THE AREA OF FREEDOM, SECURITY AND JUSTICE 4 (CHALLENGE Research Paper No. 9, May 2008), *available at* http://www.ceps.eu/book/taking-stock-databases-and-systems-information-exchange-area-freedom-security-and-justice.

[499] Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information OJ L 271/4 of 24.10.2000.

[500] For a detailed analysis *see* below.

PART II. CASE STUDIES

CHAPTER 4. The Information Collection Case.

1. The EU Data Retention Directive

> *"A key element in the fight against terrorism involves ensuring that we preserve the fundamental values which are the basis of our democratic societies and the very values that those advocating the use of violence seek to destroy."*[501]

1.1 Background

In the aftermath of the Madrid train bombings, the European Council adopted on 25 March 2004 a Declaration on Combating Terrorism,[502] in which it instructed the Council, among others, to examine measures for establishing rules on the retention of communications traffic data by service providers.[503] One month later, on 28 April 2004, France, Ireland, Sweden and the UK presented a proposal for a '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'[504] to be adopted by the Council under the framework of police and judicial cooperation in criminal matters (the former third pillar).[505] The Draft Framework decision covered data processed and stored by providers of a public communications network or publicly available electronic communications services and provided that these would be retained for a period of at least 12 months and no more than 36 months following

[501] ARTICLE 29 WORKING PARTY, OPINION 10/2001 ON THE NEED FOR A BALANCED APPROACH IN THE FIGHT AGAINST TERRORISM.
[502] European Council, Declaration on Combating Terrorism, 25 March 2004.
[503] *Id.* at 4.
[504] 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, Council Doc 8958/04 (Apr 28, 2004).
[505] The legal basis for the draft framework decision would be Articles 31(1) (c) TEU and 34(2) (b) TEU.

their generation.[506] The Article 29 Working Party criticised heavily this proposal[507] and stated that

> "the mandatory retention of all types of data on every use of telecommunication services for public order purposes, under the conditions provided in the draft framework decision, is not acceptable within the legal framework set in Article 8 ECHR."[508]

The Draft Framework decision was also challenged by the European Parliament, which contended that it contained measures that came both under the first and the third pillar.[509]

Almost a year later and after many debates on whether the measure fell under the first or the third pillar, the Commission "struck back"[510] and presented on 21 September 2005 a proposal for a directive on the retention of data processed in connection with the provision of public electronic communication services.[511] This proposal was once again criticised by the Article 29 Working Party,[512] and by the EDPS who noted that he was not convinced of "the necessity of the retention of traffic and location data for law enforcement purposes, as established in the Proposal."[513]

---

[506] *See* Clive Walker & Yaman Akdeniz, *Anti-terrorism Laws and Data Retention: War Is Over?*, 54 NORTHERN IRELAND LEGAL QUARTERLY 159, 169 (2003).

[507] *See* ARTICLE 29 WORKING PARTY, OPINION 9/2004 ON A DRAFT FRAMEWORK DECISION ON THE STORAGE OF DATA PROCESSED AND RETAINED FOR THE PURPOSE OF PROVIDING ELECTRONIC PUBLIC COMMUNICATIONS SERVICES OR DATA AVAILABLE IN PUBLIC COMMUNICATIONS NETWORKS WITH A VIEW TO THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL ACTS, INCLUDING TERRORISM. [PROPOSAL PRESENTED BY FRANCE, IRELAND, SWEDEN AND GREAT BRITAIN (COUNCIL DOC. 8958/04 – APRIL 28, 2004)] 5.

[508] *Id.*

[509] Committee on Civil Liberties, Justice and Home Affairs, Report of the European Parliament on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a 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 (8958/2004–C6-0198/2004–2004/0813(CNS)) (May 31, 2005), Rapporteur: Alexander Nuno Alvaro, A6-0174/2005 final.

[510] Eleni Kosta & Peggy Valcke, *Retaining the Data Retention Directive*, 22 COMPUTER LAW & SECURITY REPORT 370, 373 (2006); Mark Taylor, *The EU Data Retention Directive*, 22 COMPUTER LAW & SECURITY REVIEW 309 (2006).

[511] Proposal for a directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/ EC (September 21, 2005).

[512] ARTICLE 29 WORKING PARTY, OPINION 113/2005 ON THE 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 OF 21.09.2005).

[513] EUROPEAN DATA PROTECTION SUPERVISOR, OPINION ON THE 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).

After long negotiations between the Commission, the European Parliament and the Council the Directive was finally passed on 15 March 2006.

1.2 Aim and scope

Directive 2006/24/EC[514] (the 'Data Retention Directive') aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law (Article 1 (1)). It applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user, but does not apply to the content of electronic communications (Article 1 (2)).

The Directive does not include within its regulatory framework the prevention of crimes, but it requires the retention of data only for the purpose of the "investigation, detection and prosecution of serious crime." For this reason, Member States are obliged to ensure that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without "undue delay".[515] The lack of a definition of what constitutes 'serious crime' could prove to be problematic. The choice not to define the notion of 'serious crime' is to be criticised because it can result to an excessive broadening of the scope of the Directive, and therefore of the retention of data, for any crime that is to be characterised as 'serious' by each Member State.[516] To prevent such a risk, the Council urged[517] the Member States to "have due regard" to the crimes listed in

[514] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L105/54 of 13.4.2006.
[515] Article 8 of the Data Retention Directive.
[516] *See* HOUSE OF LORDS EUROPEAN UNION COMMITTEE, AFTER MADRID: THE EU'S RESPONSE TO TERRORISM 18 (5th Report of Session 2004-05). The Report notes that: "It may be difficult to draw a satisfactory line between serious and less serious crime, and a regular pattern of smaller crimes may sometimes amount to serious crime…"
[517] Council of the European Union, Statements, Council doc. 5777/06 ADD 1 (February 10, 2006).

Article 2 (2) of the Framework Decision on the European Arrest Warrant[518] and crime involving telecommunication when they implement the Directive to national law. However, this is not enough to alleviate the fear that data retention will be required for an extensive list of crimes according to the legislation of each Member State.

The Commission's Evaluation Report of the Data Protection Directive[519] proves that this fear is not unsubstantiated. In particular, ten Member States[520] have defined in their national legislation 'serious crime', with reference to a minimum prison sentence, to the possibility of a custodial sentence being imposed, or to a list of criminal offences defined elsewhere in national legislation; eight Member States[521] require data to be retained "not only for investigation, detection and prosecution in relation to serious crime, but also in relation to all criminal offences and for crime prevention, or on general grounds of national or state and/or public security"; and finally, four Member States[522] do not define 'serious crime' at all.[523]

Moreover, the Data Retention Directive adds a new paragraph 1 (a) to Article 15 (1) of the e-Privacy Directive according to which:

> "Paragraph 1 shall not apply to data specifically required [by the data retention directive] to be retained for the purposes referred to in Article 1(1) of that Directive."

This means effectively that Article 15 (1) of the e-Privacy Directive can be (still) the basis for the retention of data which fall outside the scope of the Data Retention Directive.[524]

---

[518] Council Framework Decision on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).
[519] 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, 18.4.2011.
[520] Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, Netherlands, and Finland.
[521] Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, and Slovenia.
[522] Cyprus, Malta, Portugal, and United Kingdom.
[523] Evaluation report on the Data Retention Directive, *supra* note 19, at 6.
[524] For the debate on the retention of 'unsuccessful call attempts' *see* Kosta & Valcke, *supra* note 510, at 373–374.

1.3 Types of data to be retained

The Directive lays down the obligation of the Member States to retain 'traffic' and 'location' data as well as any other related data necessary to identify the subscriber or user. The definition of 'traffic' and 'location' data is to be found in the e-Privacy Directive.[525] 'Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof[526]; 'location data' is understood as any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.[527]

However, Directive 2006/24/EC explicitly provides that no data revealing the content of the communication may be retained (Article 5 (2)). This distinction drawn by the Directive between traffic and location data on the one hand, and content data on the other, is certainly important because it safeguards the confidentiality of communications. Nevertheless, it is submitted that this distinction is not always so clear. Whereas in the context of the traditional telephone communications it is rather easy to separate content from traffic data, this is not always the case in the modern digital networks.[528] This is because, in practice, in the Internet environment content and traffic data are generated simultaneously. The example frequently used is that of a request operated with a search engine, such as Google. For instance, if we want to make a search on 'terrorism', our request will give the following result: 'http://www.google.it/search?hl=it&q=terrorism&btnG=Cerca+con+Google&meta=&aq=f&oq='. This information, however, which reveals already our interests, combined with our IP address constitutes information "relating to an identified or an identifiable natural person" in the words of the Data Protection Directive, and thus personal data. This conclusion, however, cannot be left unqualified. It has to be examined, further, whether IP addresses are personal data. The general position of the Article 29 Working Party on the issue is that:

---

[525] The fact that the Data Retention Directive refers to the ePrivacy Directive for the definition of 'traffic' and 'location' data is problematic, because it is not clear whether traffic data covers the same scope in the law enforcement framework of mandatory retention of traffic data as it does in the Directive on processing of personal data in the electronic communications sector. Law enforcement may be interested in the content of traffic data, which is quite different than using traffic data for billing purposes. On this issue, *see* Caroline Goemans & Jos Dumortier, *ENFORCEMENT ISSUES - Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-line Anonymity*, DIGITAL ANONYMITY AND THE LAW 161, 4.

[526] Article 2 (b) of Directive 2002/58/EC.

[527] Article 2 (c) of Directive 2002/58/EC.

[528] Goemans & Dumortier, *supra* note 525, at 4.

> "… unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side."[529]

However, this general statement is not without problems, in particular because IP addresses are normally dynamic, namely they may change for each session. Even dynamic IP addresses can be considered as data relating to an identifiable person. This is because, according to the Article 29 Working Party:

> "Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically "log" in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of Article 2 (a) of the Directive …"[530]

This thesis argues that dynamic IP addresses can be considered personal data when Internet access providers utilise different methods (recording of logs in, keeping of logbooks, e-mail accounts opened) to link the IP address assigned to a computer to a specific Internet user. This requires, however, a case-by-case analysis and rejects a general, unqualified assumption that all dynamic IP addresses constitute personal data.

The categories of data to be retained are laid down in Article 5 of the Directive. They consist of:

(a) data necessary to trace and identify the source of a communication;

(b) data necessary to identify the destination of a communication;

(c) data necessary to identify the date, time and duration of a communication;

(d) data necessary to identify the type of communication;

(e) data necessary to identify users' communication equipment or what purports to be their equipment; and

(f) data necessary to identify the location of mobile communication equipment.

---

[529] Article 29 Working Party, *Opinion 4/2007 on the Concept of Personal Data*, *supra* note 214, at 17.

[530] ARTICLE 29 WORKING PARTY, WORKING DOCUMENT PRIVACY ON THE INTERNET - AN INTEGRATED EU APPROACH TO ON-LINE DATA PROTECTION (5063/00/EN/FINAL, November 21, 2000).

1.4 Length of retention period

The Directive stipulates that the retention period will be between six months and two years starting from the date of the communication (Article 6). However, a Member State facing particular circumstances may request an extension of the maximum retention period. In this case, it is obliged to notify the Commission and inform the other Member States of the measures taken and state the grounds for introducing them (Article 12). It is puzzling that the Directive does not set a specific period for data retention but allows Member States for variations. This raises questions as to the level of harmonisation that it aims to achieve,[531] in that it cannot be excluded that a data retention period of six months in one Member State and of two years in another, might affect the competition between the service providers in the common market. According to the Commission's Evaluation Report the retention period stipulated in national laws varies from two years (one Member State), 1.5 years (one Member State), one year (ten Member States) six months (three Member States), to different retention periods for different categories of data (six Member States).[532] In this respect, the Commission admits that

> "the Directive provides only limited legal certainty and foreseeability across the EU for operators operating in more than one Member State and for citizens whose communications data may be stored in different Member States."[533]

Therefore, it finds it necessary to consider the possibility of further harmonising retention periods in the EU.[534]

[531] The House of Lords European Union Committee in its Report characterises the degree of approximation involved as "half-hearted at best." *See* House of Lords European Union Committee, *supra* note 516, at 18. Along these lines, also Kosta & Valcke, *supra* note 510, at 376.
[532] Evaluation report on the Data Retention Directive, *supra* note 19, at 14.
[533] Evaluation report on the Data Retention Directive, *supra* note 19, at 15.
[534] *Id.*

2. Data Retention Directive: A Privacy or a Data Protection Issue?

2.1 The conceptual confusions

The Data Retention Directive raises serious concerns regarding its compliance with fundamental rights requirements. The discussion has focused mainly on its implications on the right to privacy, the right to data protection, freedom of expression and the right to property.[535] The debate, in particular, on privacy and data protection illuminates the conceptual confusion, analysed in Chapter 1, regarding these two rights. The paradox of the Data Retention Directive is remarkable: while it is listed as a modification of EU data protection legislation;[536] it is far from clear what is the exact role of the right to data protection insofar as the fundamental rights' assessment of the Directive is concerned. Most commonly, commentators argue that it interferes (disproportionately?)[537] with the right to privacy.[538] Data protection is not left outside the game. However, in this respect, the general misconception discussed in Chapter 1, applies: the Directive is found to infringe privacy, because it is deemed to violate certain data protection principles,[539] according to the common perception that potential data protection violations are to be determined on the basis of the right to privacy.

The debate on whether the Data Retention Directive raises data protection or privacy issues, or both, is not merely theoretical. It has serious implications on the question of the compatibility of the Directive with fundamental rights. Only by posing

---

[535] Patrick Breyer, *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, 11 EUROPEAN LAW JOURNAL 365, 375 (2005). *See* also Ian Brown, *Communications Data Retention in an Evolving Internet*, 19 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 95 (2010).

[536] *See* above Article 11 of the Data Retention Directive, which essentially amends Article 15 (1) of the ePrivacy Directive by adding paragraph stipulating that Article 15 (1) of the latter does not apply to data retained under the Data Retention Directive. *See* also Cian Murphy, *Fundamental Rights and Security: The Difficult Position of the European Judiciary*, 16 EUROPEAN PUBLIC LAW 289, 300 (2010).

[537] Compare Bignami who contends that the Data Retention Directive adequately protects privacy. Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 CHICAGO JOURNAL OF INTERNATIONAL LAW 233 (2007).

[538] Breyer, *supra* note 535, at 370.

[539] *See* Opinion of the European Data Protection Supervisor on the 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) (2005/C 298/01) OJ C 298/1 of 29.11.2005, para 9. *See* also the Commission's Evaluation Report, at 28, which notes that: "Data retention constitutes a limitation of the right to private life and the protection of personal data which are fundamental rights in the EU."

the question of which fundamental right is at stake correctly, we can reach a concrete answer on the human rights' assessment of the Directive. Privacy and data protection may raise different issues, and this is the way they should be approached. Determining an interference with privacy, because there is interference with data protection –or vice-versa- is conceptually wrong. The right to data protection, as reconstructed in Chapter 2, can operate independently, therefore, it would be a fallacy to still persist in melding the two rights together.

The question of whether the Data Retention Directive violates the right to privacy or the right to data protection or both, is not the sole source of confusion concerning the Directive. The retention of communications' data covers several different types of processing: information retention – which further entails information collection and information storage-, and information use. There is a different assessment for each type of processing and this is evident in the lines that the Data Retention Directive itself draws:[540] it applies solely to the harmonisation of the obligations of the service providers to retain communications' data and *not* to the access to such data by the competent authorities of the Member States for law enforcement purposes.[541] In these terms, it makes the harmonisation of the obligations of service providers an issue of EU law, while the conditions for access to the data in order to fight terrorism and serious right a matter of national law. In particular, Article 4 of the Directive provides

> "Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided *only to the competent national authorities in specific cases and in accordance with national law*. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights."

Accordingly, this means that the Directive was adopted as a first pillar –common market- and not a third pillar –criminal justice- measure. These dichotomies did not only appear as a matter of inter-pillar litigation initially between certain Member

[540] These distinctions are not immune from criticism. *See The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)*, COMPUTERS, PRIVACY AND DATA PROTECTION : AN ELEMENT OF CHOICE 3, 12 (Serge Gutwirth et al., 2011).
[541] Article 1 of the Data Retention Directive (emphasis added).

States and the Commission in the negotiations of the Directive, and subsequently before the Court of Justice;[542] as it will be analysed below, they might also have implications on the fundamental rights' compliance of the Directive.

The Directive's Evaluation Report is illuminating also here. The authorities that have been granted access to telecommunications' data range from the police (in all Member States, except in Ireland and the United Kingdom), security or intelligence services or even the military (fourteen Member States), to tax and border authorities.[543] Only eleven Member States require judicial authorisation for each request for access to retained data, and another four require authorisation from a senior authority but not a judge.[544]

According to the Report, overall "over 2 million data requests were submitted each year, with significant variance between Member States, from less than 100 per year (Cyprus) to over 1 million (Poland).[545]

2.2 Applying the theory in data retention: What is privacy, what data protection?

As seen above, the Directive requires the retention of data revealing the source, the destination, the date, time, duration, the type and the location of the communication, alongside with any other related data necessary to identify the subscriber or user of electronic telecommunication services. 'Traffic' and 'location' data interfere with the confidentiality of the communications as they can reveal the location of individuals, their movements, the persons to whom they talk, the time and duration of their communications, the web sites that they are visiting, and information on the e-mails they sent, such as the time, the addressee and the size of possible attached files.[546] The issue posed, therefore, by the Data Retention Directive is, above

[542] *See* Case C-301/06 *Ireland v. European Parliament and Council*, Judgment of the Grand Chamber of 10 February 2009.
[543] Evaluation report on the Data Retention Directive, *supra* note 19, at 9.
[544] *Id.*
[545] *Id.*, at 21.
[546] *See* Judith Rauhofer, *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 322, 323 (2006).

all, a privacy problem.[547] The right to privacy is enshrined in Article 7 EUCFR which essentially repeats[548] the relevant provision of Article 8 (1) ECHR:[549] "Everyone has the right to respect for his or her private and family life, home and communications." In the present case, it is the privacy of individuals' communications that is at stake (communications' privacy).[550] The fact that 'traffic' and 'location' data are merely 'envelope' data and they do not touch upon the content of the communications is not crucial. 'Envelope' data can reveal an extensive amount of information about the individuals, concerning, for instance, among others, political activities, health condition, ideological, religious, and philosophical beliefs, and sexual preferences. Therefore, they interfere with the confidentiality of personal communications, even if they do not apply to their exact content. It would be mistaken, hence, to restrict the protection of confidentiality of communications merely in the content of these communications and exclude 'envelope' data. This is not only because 'envelop' data reveal already a lot about the individuals. It is because it introduces a very narrow understanding of the concept of personal privacy as secrecy. Notwithstanding this, as mentioned above, in the context of the Internet, there is no clear distinction between 'envelope' and 'content' data, as the 'envelope' reveals much of the content. The Data Retention Directive, thus, interferes with the confidential character of personal communications, and for this reason, the assessment whether this interference is permissible should be undertaken on the basis of the fundamental right to privacy.

What about the fundamental right to data protection? Are there any data protection issues raised by the Data Retention Directive? Leaving aside the common misconception, according to which, when privacy is interfered with, then there is an interference with data protection as well; the answer to this question is trickier, because it has to be established first, before assessing any potential interferences with data protection principles, whether 'traffic' and 'location' data are 'personal data'. 'Traffic' data may, *inter alia*, consist of data referring to

[547] As Breyer argues correctly: "The principal provision providing the individual with protection from the processing of telecommunications traffic data is Article 8 ECHR." Breyer, *supra* note 535, at 366.
[548] De Hert and Gutwirth note ironically: "The Charter contains an uninspired copy of Article 8 ECHR, namely Article 7..." De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197, at 81.
[549] Article 8 (1) ECHR provides: "Everyone has the right to respect for his private and family life, his home and his correspondence."
[550] Some authors, for instance, Roger Clarke refer to it as 'interception privacy'. I find this term self-contradictory, unduly narrow, and therefore inappropriate.

> "the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection", and to "the format in which the communication is conveyed by the network."[551]

'Location' data may refer to

> "the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded."[552]

It is not exactly straightforward that 'traffic' and 'location' data constitute information relating to any identified or identifiable natural person, according to Article 2 (a) of the Data Protection Directive. However, a closer look to the Data Retention Directive leaves no doubts: it mandates the retention of 'traffic' and 'location' data, as well as "the related data necessary to identify the subscriber or user"[553] of the electronic communications network or service. The combination of these data, to the extent that it relates to an identified and identifiable person, it can be considered as personal data.[554]

Having established that 'traffic' and 'location' data combined with any related data necessary to identify the subscriber or user constitute personal data and that their retention by the telecommunications' providers constitutes 'processing', it is time to investigate now, whether this is interfering with any data protection principles. The 'fair information principles' potentially affected by the Directive are purpose limitation, data security, and data minimisation. Further problems could be also be raised concerning the duration of the data retention period.

[551] Recital 15 of Directive 2002/58/EC.
[552] Recital 14 of Directive 2002/58/EC.
[553] Article 2 (2) (a) of Data Retention Directive.
[554] For a discussion whether IP addresses constitute personal data *see* above.

3. From the Theory to the Substance: Assessing the Data Protection Directive on the Basis of Privacy and Data Protection

3.1 Applying the 'privacy' test to the Data Retention Directive

As established above, "the principal provision providing the individual with protection from the processing of telecommunications traffic data"[555] is Article 7 EUCFR. The relevant analysis will take place on the specific processing that is covered by the scope of the Data Retention Directive, namely the retention (collection and storage) of data by the telecommunication service providers, and not the access to the data that is a matter of national law. The Article does not mention the permissible restrictions to the right to privacy. Article 52 (3) of the Charter provides more guidance:

> "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

The relevant provision in the Convention is Article 8 (2) ECHR. This reads as follows:

> "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."

As it has been mentioned, the European Court of Human Rights (ECtHR) has adopted a broad interpretation of the protective scope of Article 8 (1) ECHR and a narrow one of the restrictions provided for in the second paragraph, thus being consistent with its case law of reading the Convention as a "living instrument which … must be interpreted in the light of present day conditions."[556]

---

[555] Breyer, *supra* note 535, at 366.
[556] *Tyrer v UK (1978) Series A of the Publications of the European Court of Human Rights*, No 26, para 31.

According to the case-law of the Strasbourg Court, an interference with the right to privacy is justified only when it is in accordance with the law, it serves a legitimate purpose, and it is necessary in a democratic society. The analysis below will examine whether the Data Retention Directive satisfies those requirements.

a. Interference with the right to respect for private life

The Court has interpreted the notion of 'interference with the right to privacy' broadly. Thus, in *Leander v. Sweden* it held that the storing by a public authority of information relating to an individual's private life amounts to an interference with the right to respect for private life.[557] In *Amann v Switzerland* it reiterated this conclusion and added that 'the subsequent use of the stored information has no bearing on that finding'. In this case, the Court found that a card containing data relating to an individual's private life and stored by a public authority was sufficient to conclude that it amounted to an interference with the applicant's right to respect for his private life, without being necessary to speculate as to whether the information gathered was sensitive or not.[558] Furthermore, in *Klass v. Germany*, the Court reasoned that because a law permitting interception of mail created a "menace of surveillance" for all users of the postal service, and because that menace struck at freedom of communication, the law therefore constituted an interference with the right to privacy.[559]

In the light of the above mentioned decisions of the ECtHR, it can be concluded that the blanket retention of traffic data can be considered as an interference with the right to respect for private life, irrespective of whether these data will be used subsequently, and irrespective of whether these contain also 'sensitive' information.

[557] *Leander v. Sweden,* judgment of 26 March 1987, Series A no. 116, p. 22, para 48.
[558] *Amann v Switzerland* (Appl. No. 27798/95), judgment of 16 February 2000, paras 69-70.
[559] *Klass and Others v Germany*, (1978), Series A, No 28, para 40.

b. 'In accordance with the law'

According to the case-law of the Court, the requirement that an interference with the right to privacy must be 'in accordance with the law' covers two aspects. First, there must be a legal basis for the interference; secondly, the measure should be compatible with the 'rule of law'. This means that the measure should meet the standards of accessibility and foreseeability: it must be accessible to the persons concerned, and sufficiently precise to allow them to reasonably foresee its consequences.[560] In this respect, the ECtHR held in *Kruslin v France* that 'tapping and other forms of interception of telephone conversations represent a serious interference with private life and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated'.[561] Furthermore, in *Malone v United Kingdom* the Court stressed that the

> "law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to …secret and potentially dangerous interference with the right to respect for private life and correspondence."[562]

The data retention regime seems to satisfy the requirement of being 'in accordance with the law' as it is envisaged in an accessible, detailed, and democratically enacted law- Directive 2006/24/EC.[563] It has been argued that traffic data retention is incompatible with the requirement of foreseeability because it fails to distinguish between different categories of people, and does not provide a citizen with an accurately foreseeable basis by which to regulate his conduct.[564] This will be examined below under the proportionality test. It should be noted here, though, that the outcome of the 'in accordance with the law' test depends also on the quality of the laws of transposition of the Directive in domestic legislations.

---

[560] *Sunday Times v United Kingdom,* (1979), Series A, No 30, para 49.
[561] *Kruslin v France,* (1990), Series A, No 176-A, para 33.
[562] *Malone v United Kingdom,* (1984), Series A, No 82, para 66.
[563] Of the same view also Bignami who argues that the democratic character of the law is further enhanced by the fact that it was adopted under the first pillar where "the involvement of a directly elected legislature improves the transparency of rights-burdening rules", and the Working Party and the Data Protection Supervisor also contributed to the quality of the deliberative process. Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, *supra* note 537, at 249.
[564] PRIVACY INTERNATIONAL, MEMORANDUM OF LAWS CONCERNING THE LEGALITY OF DATA RETENTION WITH REGARD TO THE RIGHTS GUARANTEED BY THE EUROPEAN CONVENTION ON HUMAN RIGHTS 8–9 (October 10, 2003).

c. Legitimate aim

In order to be justified the interference with the right to privacy should also pursue one of the aims listed in paragraph 2 of Article 8 (i.e. 'national security', 'public safety', 'the economic well-being of the country', 'prevention of disorder or crime', 'protection of health or morals', and 'protections of the rights and freedoms of others'). The Strasbourg organs have rarely found that the aims invoked by the Contracting States are not in compliance with at least one of the aims listed in Article 8 (2).[565] Nevertheless, it should be stated here that while Article 8 (2) explicitly refers to the purpose of 'prevention of crime', the Directive speaks of 'investigation, detection, and prosecution of serious crime'. It could be argued that the investigation, detection, and prosecution of serious crime' falls in general either within the 'public safety' or within the 'prevention of crime' aim,[566] and can be considered as a legitimate one.

d. 'Necessary in a democratic society'

Article 8 (2) requires that the interference is 'necessary in a democratic society'. According to the ECtHR, this requirement is satisfied when the interference 'corresponds to a pressing social need' and is 'proportionate to the legitimate aim pursued.'[567] Nevertheless, national authorities enjoy a certain margin of appreciation, depending on a variety of factors, such as the importance of the legitimate aim or the seriousness of the interference involved.[568] In examining the necessity of a measure, the first test is that of effectiveness. The Directive's Evaluation Report can be helpful here. According to the Commission,

> "Member States generally reported data retention to be at least valuable, and in some cases indispensable, for preventing and combating crime, including the

[565] Lee Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, 6 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 247, 273 (1998); URSULA KILKELLY, THE RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE - A GUIDE TO THE IMPLEMENTATION OF ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 30 (Human rights handbooks, No. 1, 2001).
[566] Breyer, *supra* note 535, at 369; YUTAKA ARAI-TAKAHASHI, THE MARGIN OF APPRECIATION DOCTRINE AND THE PRINCIPLE OF PROPORTIONALITY IN THE JURISPRUDENCE OF THE ECHR 62 (2002).
[567] *Leander, supra* note 44, para 58.
[568] *Id.*

protection of victims and the acquittal of the innocent in criminal proceedings."[569]

The Commission then gives some examples from Member States where retained communications' data were useful for constructing evidence trails, starting criminal investigations and prosecuting crimes, but these cannot be accepted to prove the effectiveness of the blanket retention.[570]

A second criterion to be taken into account is whether there are less intrusive alternatives available. Finally, insofar as the proportionality requirement is concerned, the measure should not be disproportionate to the aim that it seeks to achieve.

In the light of these considerations, it seems difficult how the Data Retention Directive can satisfy the proportionality test when it stipulates the compulsory retention of traffic data of every individual, irrespective of whether he is considered to be under suspicion or not.[571] Blanket data retention, constitutes a permanent, general recording of citizens' behaviour.[572] The fact that this does not cover the content of the communication does not affect this conclusion, because, as explained above, traffic data can reveal a detailed picture of the communications, and the movements of individuals.[573] Furthermore, a blanket data retention is not proportionate because it fails to take into account specific types of communication (such as the attorney-client, patient-doctor communication), which the States already recognise as sufficiently special to warrant a higher degree of protection. Concerning the effectiveness of the

---

[569] Evaluation report on the Data Retention Directive, *supra* note 19, at 23.

[570] In his Opinion on the Commission's Evaluation Report, the EDPS notes: "...although the Commission has clearly put much effort into collecting information from the Member States' governments, the quantitative and qualitative information provided by the Member States is not sufficient to confirm the necessity of data retention as it is developed in the Data Retention Directive. Interesting examples of its use have been provided, however, there are simply too many shortcomings in the information presented in the report to allow general conclusions on the necessity of the instrument." *See* EUROPEAN DATA PROTECTION SUPERVISOR, OPINION ON THE EVALUATION REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT ON THE DATA RETENTION DIRECTIVE (DIRECTIVE 2006/24/EC) ¶ 44 (May 31, 2011).

[571] The Article 29 Working Party noted that: "the provisions of the Directive … have far reaching consequences for all European citizens and their privacy. The decision to retain communication data for the purpose of combating serious crime is an unprecedented one with a historical dimension. It encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish." *See* ARTICLE 29 WORKING PARTY, OPINION 3/2006 ON THE DIRECTIVE 2006/XX/EC 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, AS ADOPTED BY THE COUNCIL ON 21 FEBRUARY 2006 2.

[572] Breyer, *supra* note 535, at 370.

[573] Ian Brown & Douwe Korff, *Terrorism and the Proportionality of Internet Surveillance*, 6 EUROPEAN JOURNAL OF CRIMINOLOGY 119, 124 (2009). The authors note that "[t]here is little room for privacy when state investigators can see with whom we communicate, what we read and watch online, and where we travel via mobile phone use."

measure, there is no empirical knowledge at the moment, but it seems doubtful that a generalized data retention regime will in fact reduce the crime levels in the society.[574] Besides, it is not absolutely certain that other measures less privacy-intrusive do not exist. For instance, the Article 29 Data Protection Working Party has put forward as alternative measure to data retention, the so-called 'data preservation' or 'quick-freeze procedure.'[575] Under this procedure, "operators served with a court order are obliged to retain data relating only to specific individuals suspected of criminal activity as from the date of the preservation order."[576] This alternative was discarded at the EU level because

> "data preservation does not guarantee the ability to establish evidence trails prior to the preservation order, does not allow investigations where a target is unknown, and does not allow for evidence to be gathered on movements of, for example, victims of or witnesses to a crime"[577]

Finally, the maximum retention period of two years does not seem reasonable in the absence of any justification concerning its usefulness for the combating of crime. Thus, the Data Retention Directive seems to fail the proportionality test.[578] For this reason, it is interesting to anticipate the pronouncements of the Court of Justice on the issue. A challenge of the Directive based on the ground of violation of the right to privacy is possible both directly, under the procedure of Article 263 of the Treaty on the Functioning of the European Union (TFEU) (ex Article 230 EC), and indirectly through a preliminary reference submitted by a national court (Article 267 TFEU, ex Article 234 EC) on the validity of this measure with respect to fundamental rights as protected in the Community legal order and the principle of proportionality (Article 5

---

[574] Breyer, *supra* note 535, at 369. Breyer argues that there is a range of methods that criminal offenders can employ in order to prevent either the generation of traffic data or access to it by European authorities. For instance, they can use mobile-phone cards that have been registered in the name of another person or bought in a country that does not require registration.

[575] *See* Opinion of the European Data Protection Supervisor on the 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) (2005/C 298/01) OJ C 298/1 of 29.11.2005, 20; ARTICLE 29 WORKING PARTY, OPINION 4/2005 ON THE 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 OF 21.09.2005) 6.

[576] 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, 18.4.2011, 5.

[577] *Id.*

[578] *Contra see* Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, *supra* note 537, at 251. Bignami argues that a maximum retention period of two years appears reasonable, and the data retention scheme satisfies the demands of proportionality.

(4) of the Treaty on European Union (TEU), ex Article 5 EC). The Data Retention Directive has already been the matter of litigation before the Court of Justice in *Ireland v. European Parliament and Council*,[579] where the Directive was reduced to a legal basis (pillar) scrutiny. The Court, however, may have an opportunity to address the question of the fundamental rights compliance of the Directive through the preliminary ruling procedure, as a reference on the issue has been sent to Luxembourg by the Irish High Court.[580]

3.2 The Data Retention Directive under the scope of the right to data protection

The Data Retention Directive interferes primarily, as seen above, with the confidentiality of communications and therefore the right to privacy. As has been pointed out by the EDPS, though, "in addition" the Directive "has a huge impact on principles of data protection" recognised by EU law."[581] The EDPS notes, first of all, that the retention of the data is foreseen for "a period far longer than the periods that are usual for retention" by communications service providers.[582] Second, he warns against the potential loopholes in the security of the stored data.[583] The two final assertions of the EDPS regarding the impact of the Directive on the right to data protection are less clear concerning the fair information principles they refer to. The EDPS states that:

> "Under Directive 2002/58/EC, more in particular its Article 6, data may only be collected and stored for reasons directly related to the communication itself, including billing purposes. Afterwards, data must be erased (subject to exceptions). Under the present proposal, retention for the purpose of enforcement of criminal law is mandatory. The point of departure is thus contrary."[584]

---

[579] Case C-301/06 *Ireland v. European Parliament and Council*, Judgment of the Grand Chamber of 10 February 2009.
[580] *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* (2006), 3785. This case is been brought before the Irish High Court by Digital Rights Ireland. The plaintiff's summons are available at < http://www.mcgarrsolicitors.ie/wp-content/Files/Plenary%20Summons%20Scan.pdf> [accessed 28.5.2011].
[581] EDPS, *supra* note 58, para 11.
[582] *Id.*
[583] *Id.*
[584] *Id.* at para 11.

The last pronouncement of the EDPS, albeit slightly confusing, can be interpreted as referring to the access and use of the stored data by law enforcement authorities, rather than to their retention:

> "The introduction of the obligation to retain data, as foreseen by the proposal, leads to substantial databases and has particular risks for the data subject. One could think of the commercial use of the data, as well as of the use of the data for 'fishing operations' and/or data mining by law enforcement authorities or national security services."[585]

From the assertions of the EDPS, it can be deduced that apart from the questions on the duration of the data retention period, and the security of the stored data, that refer to the relevant data information principles; it is not quite clear what is the impact of the Data Retention Directive on the fundamental right to data protection. Let us start from the easier (?) questions. The period of retention of the communications is a data protection issue, to the extent that Article 6 (1) (e) of the Data Protection Directive stipulates that personal data should be kept "for no longer than is necessary for the purposes for which the data were collected or for which they are further processed." This constitutes an important fair information principle, as it expresses the proportionality value. That being said, it is very difficult to see how this principle can be violated to its essence, unless a retention of data for many years is at stake. The duration of the retention of the data has, therefore, to be judged alongside with other fair information principles to determine whether it is proportionate. As seen above, the duration of the retention period in the context of the Data Protection Directive has being taken into account in order to assess whether this interferes disproportionately with the right to communications' privacy. The principle is a matter of the right to data protection as well, but unless it is severely disregarded, we cannot talk about a violation of the right to data protection as such. Insofar as the Data Retention Directive is concerned, it does not seem that this principle has been violated. That does not imply, in any case, that the retention period of 6 months to 2 years is not considerable. It means that it is better, in the present case, to be assessed in the context of the right to privacy, rather as a data protection principle that has been violated as such.

[585] *Id.*

Data security is a further fair information principle that the Data Retention Directive might have an impact upon. The importance of the protection of the stored data from accidental loss or unauthorised access cannot be overemphasised. For this reason, the Data Direction Directive contains a number of provisions on the security of personal data. Article 7 requires that the providers of electronic communications services respect, as a minimum, the following data security principles:

(a) the retained data should be of the same quality and subject to the same security and protection as those data on the network;

(b) appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure should be in place;

(c) the data should be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and

(d) the data, except those that have been accessed and preserved, should be destroyed at the end of the period of retention.

The Directive, further, envisages that the application of the above mentioned provisions regarding the security of the stored data should be monitored by independent authorities within each Member State.[586] There is no reason to consider that these provisions are inadequate to ensure data security. On the contrary, it seems that the Directive takes this data information principle very seriously into account. There is, however, one small (at first sight) detail here that should not go unmentioned. The data security requirements of the Directive might impose a "considerable financial burden"[587] on the service providers. This is confirmed in the Evaluation Report where the Commission mentions that five major industry associations stated that the economic impact of the Directive was "substantial" or "enormous" for "smaller service providers", because the Directive leaves "broad room for manoeuvre."[588] The question is who will bear this burden. The issue might

[586] Article 9 of the Data Retention Directive.

[587] *See* Anna Tsiftsoglou & Spyridon Flogaitis, *Transposing the Data Retention Directive in Greece: Lessons from Karlsruhe* in VALUES & FREEDOMS IN MODERN INFORMATION LAW & ETHICS (4th International Conference of Information Law, May 21, 2011). The authors discuss the relevant costs in different countries therein. For instance, the cost for the retention of data is estimated to € 130 million in France in 2006 and € 150 million in the UK in 2008.

[588] Evaluation report on the Data Retention Directive, *supra* note 19, at 26. *See* http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF.

appear unimportant from a data protection point of view, but it seems at least ironic that EU citizens might be possibly called upon to "pay for their own surveillance."[589]

As seen above, the last two pronouncements of the EDPS regarding the impact of the Directive on the right to data protection are confusing. In particular, the first refers to the changes introduced to the ePrivacy Directive. Under this, data could only be collected and stored for reasons directly related to the communication itself, including billing purposes. Afterwards, they should, in principle, be erased. This principle has been reversed in the Data Retention Directive, where the retention for the purpose of enforcement of criminal law is being made mandatory. It is not stated clearly in the EDPS's Opinion which data protection principle is affected by this reversal. It seems, however, that the EDPS is referring here, in a rather confusing way, to the purpose limitation principle. This requires that personal information should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The use of communications data for law enforcement reasons is a purpose incompatible with their retention, initially foreseen solely for reasons directly related to the communication itself, such as for instance billing purposes. The Data Retention Directive interferes, therefore, with the purpose limitation principle. In fact, the Directive itself introduces an exception to this principle. According to the assertions made in Chapter 1, this is permissible, insofar as it complies with the following conditions: 1) it is provided by law 2) it pursues a legitimate aim 3) it is necessary in a democratic society 4) it conforms with the principle of proportionality and 5) it respects the 'hard core' or the 'essence' of the purpose limitation principle. The Data Retention Directive interferes

[589] Maria Kaifa-Gbanti, *Surveillance Models in the Security State & Fair Criminal Trial (in Greek)*, NOMIKI VIVLIOTHIKI 43 (2010). The German Constitutional Court positions itself on the issue as follows: "Within its discretion, which is broad in this connection, the legislature is not restricted to engaging private persons only if their occupation can directly cause dangers or they have direct liability for these dangers. Instead, it is sufficient in this connection if there is a close relationship in terms of subject-matter and in terms of responsibility between the person's occupation and the duty imposed. There are therefore no fundamental objections to the cost burdens incurred by the persons with a duty of storage. In this way, the legislature shifts the costs associated with the storage as a whole onto the market, corresponding to the privatisation of the telecommunications sector. Just as the telecommunications enterprises can use the new opportunities of telecommunications technology to make profits, they must also assume the costs of containing the new security risks that are associated with telecommunications and must include them in their prices." The Commission in its Evaluation Report notes that "there is no evidence of any quantifiable or substantial effect of the Directive on consumer prices for electronic communications services; there were no contributions to the 2009 public consultation from consumer representatives." *See* Evaluation report on the Data Retention Directive, *supra* note 19, at 26.

disproportionately with the fundamental right to data protection if one of these conditions is not satisfied.

Addressing these requirements, if one takes into account, all the more, the lack of any guidance by courts, is not an easy task. Moreover, the task might be deemed superfluous since a disproportionate interference have been found on the basis of the right to privacy, with which courts and judges are more accustomed. In any case, the retention of 'envelope' communications' data for criminal law enforcement, is not a purpose foreseen by individuals, that use telecommunications services and networks and provide their data to the relevant providers for contractual purposes (such as billing). This lack of foreseeability and transparency of the further processing can hardly by remedied by the fact that the Directive provides the basis for the retention of the data itself. Most EU citizens that use communications services and networks are probably not aware of the Data Retention Directive or its various national transposition laws in their respective Member States. But, even if they are, the further use of their communications' data for law enforcement purposes might have a chilling effect on their behaviour and the exercise of other fundamental freedoms. If they cannot predict with sufficient certainty which information about themselves is known to law enforcement authorities, and in which ways this can be used, they will be inhibited in exercising individual freedoms, such as freedom of speech or freedom of association. A processing for purposes such incompatible with their initial collection, as those introduced by the Data Retention Directive, is against the right to informational self-determination. This is why the EDPS warns that the obligation to retain data, laid down by the Directive, might lead to the creation of substantial databases and, therefore, have particular risks for the data subject. It is not entire certain, despite the seemingly strict conditions, that the data will not be used for commercial purposes, or for 'fishing operations' and data mining by law enforcement authorities or national security services. The scenario, while related *strict sensu* to the access and use of the data, and not their retention –which is a matter of EU law- is far from being hypothetical. The Bulgarian transposing law of the Data Retention Directive, which was eventually struck down by the Supreme Administrative Court,[590] stipulated that "the data would be retained by the providers and a directorate within the Ministry of Interior would have a direct access via computer terminal", and that

[590] Judgment of 11 December 2008.

"security services and other law enforcement bodies" would have access "to all retained data by Internet and mobile communication providers" without needing court permission.[591] Of course, it could be argued that such a result is only a matter of national law, since the EU Directive stipulates merely the collection and retention of the data and not their use. However, it should be stated that the path to such a use of the data is opened up already by the Directive and its provisions. Since the data are available for law enforcement purposes, Member States are free to decide, further, how they will be accessed and used by those authorities.[592]

The Commission in its Evaluation Report recognised the problems posed by the inability of the Directive to harmonise divergent practices on the fundamental rights to privacy and data protection. As the Commission has noted

> "the Directive does not in itself guarantee that retained data are being stored, retrieved and used in full compliance with the right to privacy and protection of personal data. The responsibility for ensuring these rights are upheld lies with Member States. The Directive only sought partial harmonisation of approaches to data retention; therefore it is unsurprising that there is no common approach, whether in terms of specific provisions of the Directive, such as purpose limitation or retention periods, or in terms of aspects outside scope, such as cost reimbursement."[593]

That the Member States bear responsibilities when implementing the Directive with regard fundamental rights goes without saying. But the Commission's statement tells only the half-truth. The analysis above showed that the mandatory blanket retention of communications' data constitutes a "huge interference"[594] with the right to privacy and with the purpose limitation principle. It is argued that part of the problem in these cases is found in the Data Retention Directive itself. The story might change with regard to further data protection principles, such as for instance, data security or proportionality of data retention periods. In these cases, Member States can construct their legislation in such a way so that these principles are safeguarded. But, the fact

[591] Article 5 of Regulation 40 on the categories of data and the procedure under which they would be retained and disclosed by companies providing publicly available electronic communication networks and/ or services for the needs of national security and crime investigation.
[592] *See* below the analysis of the Romanian Constitutional Court on the issue.
[593] Evaluation report on the Data Retention Directive, *supra* note 19, at 31.
[594] Peter Hustinx, *The Moment of Truth for the Data Retention Directive* (Taking on the Data Retention Directive, December 03, 2010).

that the Directive provides for the *availability* of telecommunications data for law enforcement purposes opens up the way for their abuse and misuse.[595]

4. Data Retention before the courts

4.1 The EU inter-pillar litigation

As mentioned above, there were vigorous debates between the EU institutions and the Member States at the time of the adoption of the Data Retention Directive regarding its legal basis, and in particular whether it fell under the Community competence or it was a measure to be adopted under the framework of police and judicial cooperation in criminal matters.

The case was not resolved even after the adoption of the Directive as a first pillar measure. Ireland supported by Slovakia, challenged it before the ECJ, on the ground that Article 95 EC (now 114 TFEU), which has as its object the establishment and the functioning of the internal matter, was not the appropriate legal basis, because the main aim of the Data Retention Directive is to facilitate the investigation, detection and prosecution of serious crime, including terrorism, and thus it should have been adopted under the third pillar. The Court in its judgment disagreed and held that the Directive was adopted on the appropriate legal basis, since both its aim and its content fell under Article 95 EC.[596]

It started by noting that after the Madrid and London terrorist attacks, several Member States,

> "realising that data relating to electronic communications constitute an effective means for the detection and prevention of crimes, including terrorism, adopted

[595] The Assistant EDPS, Giovanni Buttarelli characterised the Directive as "the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects." *See* Giovanni Buttarelli, *What Future for the Data Retention Directive* in EU COUNCIL WORKING PARTY ON DATA PROTECTION AND INFORMATION EXCHANGE (DAPIX - DATA PROTECTION) (Discussion on the Commission Evaluation report, May 04, 2011).
[596] *Ireland v. European Parliament and Council*, para 93.

measures with a view to imposing obligations on service providers concerning the retention of such data."[597]

These measures, not only "have significant economic implications for service providers in so far as they may involve substantial investment and operating costs",[598] but they also "differed substantially particularly in respect of the nature of the data retained and the periods of data retention".[599] The legislative and technical disparities between the national provisions governing the retention of data by service providers, were liable, according to the Court of Justice, to have "a direct impact on the functioning of the internal market",[600] and, thus, justified the adoption of harmonised rules by the Community legislature. The Court clarified that Article 95 EC was the correct legal basis for the adoption of these rules, since

> "the provisions of Directive 2006/24 are essentially limited to the activities of service providers and do not govern access to data or the use thereof by the police or judicial authorities of the Member States."[601]

As the Data Retention Directive does not harmonise the issue of access to data by the competent national law-enforcement authorities neither the use and exchange of those data between those authorities, it does not fall under the framework of police cooperation in criminal matters (former third pillar),[602] but under the Community (former first pillar). The Court of Justice did not refer to the human rights dimension of the Directive. The examination of this was dismissed with a short statement that

> "the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24." [603]

The decision of the ECJ is (obviously) not very helpful for the present analysis as the Court refrained to pronounce itself on the fundamental rights questions raised by the Directive. However, it is worth noting the insistence of the ECJ to a clear division between on the one hand, the retention and, on the other hand, the access and use of the data, which led to the conclusion that the former is an internal market issue while the latter a police and judicial cooperation matter.

---

[597] *Id.,* para 67.
[598] *Id.,* para 68.
[599] *Id.,* para 69.
[600] *Id.,* para 71.
[601] *Id.,* para 80.
[602] *Id.,* para 83.
[603] *Id.,* para 57.

4.2 Data retention before national courts

4.2.1 The German Constitutional Court decision

Unlike the Court of Justice of the EU, the German Constitutional Court did not show any deference before data retention. In its seminal decision,[604] the Court declared unconstitutional the law transposing the Directive into Germany, because it did not guarantee adequate data security or an adequate restriction of the purposes of use of the data, and it did not satisfy, in every respect, the constitutional requirements of transparency and legal protection.[605]

The Constitutional Court started its analysis by rejecting the need to submit a referral to the Court of Justice, since "a potential priority of Community law" was not relevant in this case. After this –not unquestionable- assertion, the Court went on to discuss the possible constitutional problems that the transposing law – not the Directive- raised in the Federal Republic of Germany. The Court, based, rightly, its analysis on the right to secrecy of telecommunications, enshrined in Article 10.1 of the German Constitution. In this respect, it distinguished between the storage of telecommunications by service providers and their subsequent access and use by law enforcement authorities. The Court opined that

> "the storage of telecommunications traffic data without occasion for six months for strictly limited uses in the course of prosecution, the warding off of danger and intelligence service duties is not in itself incompatible with Article 10 of the Basic Law."

Nevertheless, such storage constitutes "a particularly serious encroachment with an effect broader that anything in the legal system to date." This is because, according to the Court:

> "Even though the storage does not extend to the contents of the communications, these data may be used to draw content-related conclusions that extend into the users' private sphere. In combination, the recipients, dates,

---

[604] 1 BvR 256/08 of 2 March 2010 *available* at http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

[605] For an analysis *see* Christian DeSimone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, 11 GERMAN LAW JOURNAL 291 (2010); Wiebke Abel & Burkhard Schafer, *The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a Case Report on BVerfG, NJW 2008, 822*, 6 SCRIPT-ED 106 (2009).

time and place of telephone conversations, if they are observed over a long period of time, permit detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses. Depending on the use of the telecommunication, such storage can make it possible to create meaningful personality profiles of virtually all citizens and track their movements. It also increases the risk of citizens to be exposed to further investigations without themselves having given occasion for this. In addition, the possibilities of abuse that are associated with such a collection of data aggravate its burdensome effect. In particular since the storage and use of data are not noticed, the storage of telecommunications traffic data without occasion is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas."

That being said, the Court went on to recognise, surprisingly enough, that there are certain factors that make such retention of data acceptable under the Constitution. The first is that the storage "is realised not directly by the state, but by imposing a duty on the private service providers. In this way, the data are not yet combined at the point of storage itself, but remain distributed over many individual enterprises and are not directly available to the state as a conglomerate." The second, and more dubious one is that "precautionary storage of telecommunications traffic data considerably reduces the latitude for further data collections without occasion, including collections by way of European Union law."

In any case, such storage, according to the Court, is compatible with Article 10.1 of the Basic Law only if its formulation satisfies particular constitutional requirements on data security, purpose limitation, transparency and legal protection. The Court provided detailed guidance on all these issues to the legislator. Concerning the use of data pro-actively, in order to prevent criminal activity, the Court accepted that this may only be permitted, according to the principle of proportionality, "if there is a sufficiently evidenced concrete danger to the life, limb or freedom of a person, to the existence or the security of the Federal Government or of a *Land* or to ward off a common danger." The principle of proportionality also requires that:

> "there should be a fundamental prohibition of transmission of data, at least for a narrowly defined group of telecommunications connections which rely on particular confidentiality. These might include, for example, connections to persons, authorities and organisations in the social or ecclesiastical fields which

offer advice in situations of emotional or social need, completely or predominantly by telephone, to callers who normally remain anonymous, where these organisations themselves or their staff are subject to other obligations of confidentiality in this respect."

Leaving aside the Court's denial to submit a preliminary reference to the European Court of Justice, the judgment is to be welcomed for several reasons. First, it does not repeat the general confusion of whether the Directive is a matter of privacy or of data protection. The German Court is clear on the issue: it bases its decision on Article 10 of the Basic Law and the right to respect the secrecy of communications. In this respect, it leaves aside the right to data protection or informational self-determination that derives, according to the Census decision, from Article 1 of the Constitution and the right to dignity. The retention of traffic data affects above all the confidentiality of communications and the Court discusses it on this basis. Second, it does not accept the argument that traffic and content data are not the same, therefore the interference is not as grave in the present case.[606] Above all, its analysis on the principle of proportionality provides extremely useful guidance for the legislators and courts.

4.2.2 The Romanian Constitutional court decision

The decision of the Romanian Constitutional Court[607] on the law[608] transposing in Romania the Data Retention Directive is also interesting.[609] The Court identified several problems in the implementing law. First, it criticised it for requiring the retention of traffic and location data as well as "the related data necessary for the identification of the subscriber or registered user", without explicitly defining what it means by "related data". According to the Court, this lack of a precise legal provision

[606] *See* dissenting opinion of Judge Schluckebier on the issue.
[607] Decision No. 1258 of 8 October 2009. Unofficial translation by Bogdan Manolea and Anca Argesiu at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf.
[608] Law 298/2008.
[609] For a case-note *see* Cian Murphy, *Romanian Constitutional Court, Decision No. 1258 of 8 October 2009 Regarding the Unconstitutionality Exception of the Provisions of Law No. 298/2008 Regarding the Retention of the Data Generated or Processed by the Public Electronic Communications Service Providers, as Well as for the Modification of Law No. 506/2004 Regarding the Personal Data Processing and Protection of Private Life in the Field of Electronic Communication Area*, 47 COMMON MARKET LAW REVIEW 933 (2010).

that determines with accuracy the sphere of the data necessary to identify physical and legal users, opens up the possibility for abuses in the activity of retaining, processing and using the data stored by the electronic communication services and public networks providers. The Court also criticised the legislator for "ambiguous manner of drafting" with regards to the term "threats to national security", the prevention of which justifies access to the retained data.

Beyond these linguistic problems of the national transposition law, the Constitutional Court noted that

> "the continuous retention of personal data transforms the exception from the principle of effective protection of privacy right and freedom of expression, into an absolute rule."

In this respect, the users of electronic communication services or networks, are made

> "permanent subjects to intrusions into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communication, thus excluding the main communication means used nowadays."

Moreover, the Romanian Court focused on a further aspect of the data retention regime: that fact that it has an effect not only on the person that performs the communication, by sending for instance a message, but also on the receiver of that information. The called person is thus exposed, according to the Court, to the retention of the data connected to his private life, irrespective of his own act or a manifestation of will but only based on the behaviour of another person – of the caller- whose actions he cannot control to protect himself against bad faith or intent of blackmail, harassment etc. Even though he is a passive subject in the intercommunication relationship, the called person can become, despite his will, suspect in front of the law enforcement authorities. This intrusion in private life of third individuals was deemed by the Romanian Court as excessive.

Unlike the German Court, the Romanian Constitutional Court found the legal obligation of data retention with its continuous character and general applicability, more problematic than the data's "justified use" by law enforcement authorities. The former addresses equally

> "all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is

likely to overturn the presumption of innocence and to transform *a priori* all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes."

This line of argument is very interesting. Although, the present thesis does not subscribe to it, as it was argued above, the access and use of the data by law enforcement authorities does not describe the whole problem posed by the Data Retention Directive. The data can be accessed and used only because the Directive stipulates their retention for law enforcement purposes. Consequently, it would be hypocritical to assume that all fundamental rights issues are raised solely at the national level.

4.2.3 The Czech Constitutional court decision

On 22 March 2011 the Czech Constitutional court delivered its decision on the national law implementing the Data Retention Directive in the Czech Republic.[610] Following the judgments of the German and the Romanian Constitutional courts, it declared the implementing law unconstitutional.

The Court had, first, to decide whether it should submit a preliminary reference question to the ECJ on the validity of the Directive. Employing a similar argument with the German Court, it rejected this possibility on the basis that the content of the Data Retention Directive provided the Czech Republic with sufficient space to implement it in conformity with the constitutional order, since its individual provisions in fact only define the obligation to retain data. The legislator had certainly to respect the objective of the Directive when transposing it in national law, but the challenged provisions concerned

> "an expression of the will of the Czech legislator, which may vary to some extent as far as the choice of relevant means is concerned, while observing the Directive's objective, yet when making such choice, the legislator was at the same time bound to the constitutional order."[611]

The Czech Constitutional Court assessed the implementing law of the Directive on the basis of "the individual's fundamental right to privacy in the form of

[610] 2011/03/22 Pl. ÚS 24/10 *available* in English at http://www.concourt.cz/clanek/pl-24-10.
[611] *Id.,* para 25.

the right to informational self-determination."[612] The Court noted that although the obligation to retain traffic and location data does not apply to the content of individual messages

> "the data on the users, addresses, precise time, dates, places, and forms of telecommunication connection, provided that monitoring takes place over an extended period of time and when combined together, allows compiling detailed information on social or political membership, as well as personal interests, inclinations or weaknesses of individual persons."[613]

As *obiter dictum* the Constitutional Court expressed its doubts on whether an instrument of global and preventive retention of location and traffic data on almost all electronic communications "may be deemed necessary and adequate from the perspective of the intensity of the intervention to the private sphere of an indefinite number of participants to electronic communications",[614] and whether "it is at all desirable that private persons (service providers in the area of the Internet, telephone and mobile communication, i.e. in particular, mobile operators and commercial enterprises providing Internet access) should be entitled to retain all data on the communication provided by them."[615] This is indeed a very valuable comment that should not go unnoticed in the context of the discussion of the Data Retention Directive, as well as other instruments analysed below.

[612] *Id.,* para 37. Article 10 paragraph 3 and Article 13 of the Czech Constitutional Charter.
[613] *Id.,* para 44.
[614] *Id.,* para 55.
[615] *Id.,* para 57.

CHAPTER 5. The Information Storage Case.

> *"The problem with databases emerges from subjecting personal information to the bureaucratic process with little intelligent control or limitation, resulting in a lack of meaningful participation in decisions about our information."*[616]

Introduction

The computer database[617] has been eloquently described as "the biggest change brought about by the information technology revolution."[618] Indeed, multiple data can now be gathered, processed, tabulated and cross-referenced at speeds and with accuracy that would have been unthinkable in the past. In today's information society, where the collection, storage, use, collation and communication of vast amounts of personal data are central to the functioning of public services as well as private business, computer databases and computer networks are becoming almost ubiquitous.[619]

It goes without saying that databases are crucial for law enforcement. The storage and exchange of information through large-scale databases that interlink to each other is a very powerful apparatus for law enforcement authorities, in particular in the fight against terrorism. For this reason, a proliferation of cross-border information systems used for law enforcement purposes has been witnessed in the EU over the past few years.[620]

---

[616] Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, *supra* note 94, at 1422.

[617] Computer scientists define the 'database' as a "shared collection of logically related data (and a description of this data), designed to meet the information needs of an organization." *See inter alia* THOMAS CONNOLLY & CAROLYN BEGG, DATABASE SYSTEMS: A PRACTICAL APPROACH TO DESIGN, IMPLEMENTATION, AND MANAGEMENT (5th ed. ed. 2010).

[618] SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY ¶ 9.6.1 (September 2006), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.

[619] *Id.*

[620] *See* Geyer, *supra* note 498.

The information storage case aims to test the added value of the fundamental right to data protection with regard to the problems that arise from the EU-level databases. In particular, this Chapter discusses three databases that have attracted particular attention in the context of the EU's security strategy: the Schengen Information System (SIS) and more specifically the development of the second generation Schengen Information System (SIS II), the Visa Information System (VIS), and EURODAC. While SIS II pursues law enforcement and counter-terrorism purposes, VIS and EURODAC from their nature, they are significantly different databases with no obvious connection to counter-terrorism. In particular, they are not law enforcement tools, since they were not conceived as databases that could be accessed by law enforcement authorities in order to take the relevant executive action, as in the case of SIS II. In this regard, they have no direct connection with the EU's anti-terrorism strategy, as VIS on the one hand aims to support the common visa policy, and EURODAC, on the other hand, the common asylum policy. However, the major problem with regard to these databases is that the information they store can be very useful in the fight against terrorism and therefore law enforcement authorities require access to this.

The Chapter is structured as follows: First, it examines the relevant legal framework of each information system to the extent that it relates to the EU's counter-terrorism action. Subsequently, it discusses the potential privacy and data protection problems that each information system poses and engages into a substantive assessment of the interferences with these fundamental rights. The Information Storage case-study does not address the Europol and Eurojust databases, and the Customs Information System (CIS) database. Its main focus is to test the added value of the right to data protection in the storage and exchange of information through EU-scale databases.

1. The Schengen Information System

1. 1 Background: An overview of the Schengen co-operation

On 14 June 1985, five member states of the European Union -Belgium, Luxembourg, Germany, France, and the Netherlands- concluded in Schengen, a small village in Luxembourg, an intergovernmental agreement concerning the gradual abolition of controls of persons and goods at their internal borders.[621] This agreement was followed by the Implementing Convention (Convention Implementing the Schengen Agreement (CISA)),[622] which was signed in June 1990 and came into effect on 26 March 1995, by which time Italy, Portugal, Spain, and Greece had also joined the Schengen area.[623] In the following years, most of the remaining EU states signed up the Schengen Convention, alongside with the Nordic countries.[624]

The main purpose of the Convention was to abolish internal checks between signatory states while establishing a common external border where checks were to be carried out in compliance with a jointly agreed set of rules,[625] including common requirements for granting visas and closer cooperation between the authorities responsible for performing border controls.[626] The underlying principle was to facilitate free movement of people and goods within the Schengen area, while at the same time ensuring a high degree of security.[627] The rationale behind the Schengen

---

[621] The 1985 Schengen Agreement is published in OJ L 239/13 of 22.9.2000.

[622] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239/19 of 22.9.2000.

[623] Italy in 1990; Portugal and Spain in 1991; Greece in 1992; Austria in 1995.

[624] Denmark, Finland and Sweden in 1996 with Iceland and Norway as associate members. *See* also SCHENGEN, JUDICIAL COOPERATION AND POLICY COORDINATION (Monica den Boer, 1997); THE IMPLEMENTATION OF SCHENGEN: FIRST THE WIDENING, NOW THE DEEPENING (Monica den Boer, 1997).

[625] Article 6 of the Schengen Convention, which harmonised external border controls, read as follows: "1. Cross-border movement at external borders shall be subject to checks by the competent authorities. Checks shall be carried out for the Contracting Parties' territories, in accordance with uniform principles, within the scope of national powers and national law and taking account of the interests of all Contracting Parties."

[626] STEFANO BERTOZZI, SCHENGEN: ACHIEVEMENTS AND CHALLENGES IN MANAGING AN AREA ENCOMPASSING 3.6 MILLION KM^2 4 (CEPS Working Document No. 284, February 2008).

[627] Article 17 of the Schengen Agreement provided that: "In regard to the movement of persons, the Parties shall endeavour to abolish the controls at the common frontiers and transfer them to their external frontiers. To that end, they shall endeavour to harmonise, where necessary, the laws and administrative provisions concerning prohibitions and restrictions which form the basis for the controls and to take complementary measures to safeguard security and combat illegal immigration by national of States that are not members of the European Communities."

co-operation was that once a person has been allowed to enter the territory of one of the Schengen countries, he/ she may automatically travel further to any other Schengen country, without being checked again at the border of that country.[628] However, if border checks between two countries are reduced or eliminated, 'compensatory measures' that counterbalance the abolition of controls at the internal borders of the Schengen territory are necessary. This is because, the abolition of internal border controls, as explained above, means free circulation of persons within the Schengen area. However, it also implies that illegal immigrants and criminals can move freely. Since within the Schengen territory, illegal crossing of internal borders is in principle not controlled, an enhancement of external border controls as well as an increased sharing of information is needed in order to counter the undesirable effects of the removal of internal border controls. Furthermore, problems may arise also in the external borders with regard to the different Schengen states' policies concerning asylum and immigration. In this respect, the visa policies of the Schengen countries would remain without effect if even one Schengen country decided to apply a different policy, based, for instance, on a more permissive line. In that case, the obtaining of a visa for entry in that country would imply automatically the right to move also in every other country within the Schengen area, and would thus circumvent the visa policies of the rest of the states.

Therefore, the Schengen Convention laid down several 'compensatory measures' to the abolition of controls at the internal borders and the free movement of persons and goods in the Schengen territory.[629] These included among others the strengthening and harmonisation of the external border control, the harmonisation of visa policies, mutual assistance in criminal matters, and a strengthened police cooperation, based on the exchange of data through a common information system, a multinational database to be used by immigration, border control, judicial and police

---

[628] Jos Dumortier, *The Protection of Personal Data in the Schengen Convention*, 11 INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 93, 93 (1997).

[629] *See* Article 9 of the Schengen Agreement and Article 7 of the Schengen Convention. The main measures adopted by the Schengen member states include the following: the removal of checks at common borders, replacing them with checks at the external borders; common rules for crossing external borders and for controls at the external borders; separation in air terminals and ports of people travelling within the Schengen area from those arriving from countries outside the area; harmonisation of the rules regarding short- stay visas; harmonisation of the conditions governing the movement of aliens; rules for asylum seekers; police cooperation; mutual assistance in criminal matters; and the introduction of cross-border rights of surveillance and hot pursuit for police forces in the Schengen States.

authorities in any of the states which applied the Schengen Convention: the Schengen Information System (the SIS).[630]

The Schengen intergovernmental agreement was brought within the legal and institutional framework of the European Union via a Protocol attached to the Amsterdam Treaty.[631] This meant that from the moment of the entry into force of the Amsterdam Treaty, on 1st May 1999, the Schengen *acquis*[632] became part of the secondary Community and Union law and extended fully to all the fifteen States which were (then) members of the EU other than the United Kingdom and Ireland, and also separately to Norway and Iceland.

Nine of the ten member states that joined the European Union on 1 May 2004 are now also legally bound by the Schengen *acquis*, [633] and the Schengen area is now composed of twenty-five countries.[634]

2. The Schengen Information System (SIS)

2.1 Introduction: The SIS and SIRENE

At the heart of the Schengen co-operation and one of the most important 'compensatory measures', counterbalancing the suspension of the internal border controls within the Schengen area, is the Schengen Information System (SIS), a multinational database set up under the 1990 Schengen Convention which came into

[630] Article 92 of the Schengen Convention.
[631] Pieter Jan Kuijper, *Some Legal Problems Associated with the Communitarization of Policy on Visas, Asylum and Immigration Under the Amsterdam Treaty and Incorporation of the Schengen Acquis*, 37 COMMON MARKET LAW REVIEW 345, 346 (2000); Daniel Thym, *The Schengen Law: A Challenge for Legal Accountability in the European Union*, 8 EUROPEAN LAW JOURNAL 218 (2002); Eckart Wagner, *The Integration of Schengen into the Framework of the European Union*, 25 LEGAL ISSUES OF EUROPEAN INTEGRATION 1 (1998).
[632] The Schengen *acquis* consists of the Schengen Agreement, the Implementing Convention, the accession Protocols of the different latecomers, several Executive Committee decisions, and some Central Group decisions. See Council Decision 199/435/EC, OJ L 176 of 10.07.1999, including corrigendum in OJ L 9/1 of 13.01.2000.
[633] The Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia. Cyprus implements the Schengen *acquis* only partly. For Bulgaria (accession on 1 January 2007), there is a declaration setting the target date as 2011, and Romania (also accession on 1 January 2007) has not yet proposed any target date for joining the Schengen area.
[634] Belgium, France, Germany, Greece, Italy, Luxembourg, Netherlands, Portugal, Spain, Austria, Denmark, Finland, Iceland, Norway, Sweden, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, Slovenia, and Switzerland.

operation on 26 March 1995.[635] The SIS holds data on persons and objects and allows competent authorities in Member States to exchange this information with the further purpose of performing controls at external borders or on national territory and issuing visas and residence permits, as well as assisting police and judicial cooperation.

According to the Schengen Convention, the overall objective of the SIS is to strengthen and extend direct co-operation between police, immigration and customs authorities in the Schengen countries.[636] The specific purpose of the SIS is to "maintain public policy and public security" in relation to the movement of persons.[637] As the Commission explains

> "[t]he SIS is a common information system, whose aim is to allow the competent authorities in the Member States to cooperate, by exchanging information for the implementation of the various policies required in order to establish an area without internal border controls. It allows these authorities, through an automatic query procedure, to obtain information related to alerts on persons and objects. The information obtained is used, in particular, for police and judicial cooperation in criminal matters as well as for controls of persons at the external borders or on national territory and for the issuance of visas and residence permits. The SIS, therefore, is an indispensable component of the Schengen area for applying the Schengen provisions on the movement of persons and in ensuring a high level of security in this area. Consistency with a wide range of policies linked to control of external borders, visa, immigration and also police and judicial cooperation in criminal matters is, therefore, essential."[638]

The SIS is set up as a network of databases which consists of a central database (C.SIS), which is located in Strasbourg and national databases in each of the Member States (N.SIS) that are connected to C.SIS. The central SIS links the N.SIS networks of the Schengen countries. It comprises a data file that ensures that the data files of all the N. SIS are kept identical by online transmission of information.[639]

---

[635] Articles 92– 119 (Title IV) of the 1990 Schengen Convention.
[636] Article 92 of the Schengen Convention.
[637] Article 93of the Schengen Convention.
[638] Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II), COM(2005) 230 final, Brussels, 31.5.2005, p. 4.
[639] STEPHEN KARANJA, TRANSPARENCY AND PROPORTIONALITY IN THE SCHENGEN INFORMATION SYSTEM AND BORDER CONTROL CO-OPERATION 184 (2008).

The SIS is supported by the SIRENE[640] (Supplementary Information Request at the National Entry) system which provides the infrastructure for exchanging additional information to that held on the SIS, as well as facilitating the exchange of police information which takes place outside the SIS. Every Schengen Member State must set up a SIRENE office, which is responsible for the smooth operation of its N.SIS[641] in accordance with the provisions of the Schengen Convention.[642] In essence, the national SIRENE offices hold supplementary information in relation to all their national entries and make it available to the bureaux of other Schengen States if so required.

A particularly intriguing question concerned the allocation of a legal basis to the SIS after the communitarisation of the Schengen *acquis* by the Treaty of Amsterdam. As mentioned above, the SIS serves a dual purpose: It can be used for immigration purposes (since it covers data concerning persons who should not be admitted in the Schengen area for immigration reasons) on the one hand; but it can also be used for criminal law and policing purposes (because it contains data of persons who are wanted for extradition, or because they must still serve a criminal sentence or are wanted for other criminal law reasons) on the other hand. This meant that the allocation of a legal basis to the SIS was a highly controversial issue, especially because many Member States considered as 'anathema'[643] the possibility of an allocation of the SIS to both a first and a third pillar legal basis. Thus, they left the issue unregulated and an 'allocation by default' of the SIS to the third pillar took place.[644] However, the Treaty of Amsterdam required that any new measures 'building upon' the Schengen *acquis* had to be adopted on the correct legal bases. Thus, despite the failure to agree on the legal base for the SIS provisions, measures adopted subsequently were allocated to the correct legal basis. In this regard, also the

[640] Although the SIRENE is often described as the operational core of Schengen, no reference is made to it in the Schengen Convention. As JUSTICE points out in its report, 'since its inception, the SIRENE system has been surrounded by secrecy'. In fact, its operational structure was set out in a Manual which was confidential until 2003. See JUSTICE, THE SCHENGEN INFORMATION SYSTEM : A HUMAN RIGHTS AUDIT 19 (2000).

[641] Tromp, *Schengen's Final Days? The Incorporation of Schengen into the New EU, External Borders and Information Systems*, SCHENGEN, JUDICIAL COOPERATION AND POLICY COORDINATION, 164 (Monica den Boer, Maastricht : European Institute of Public Administration ed. 1997).

[642] Article 108 of the Schengen Convention.

[643] Kuijper, *supra* note 631, at 349.

[644] Steve Peers, *Key Legislative Developments on Migration in the European Union: SIS II*, 10 EUROPEAN JOURNAL OF MIGRATION AND LAW 77, 79 (2008).

procedure for updating the SIRENE Manual was set out in both first and third pillar legislation from 2004.[645]

2.2 The SIS and counter-terrorism

After the September 2001 and in particular after the Madrid 2004 terrorist attacks, new functions were introduced to the SIS in order to provide for the fight against terrorism. The two legislative measures that were adopted pursuant to Spain's initiative, namely Regulation 871/2004[646] and Council decision 2005/211/JHA,[647] aimed to enhance the functions of the SIS and improve its capabilities in order to make it a more powerful tool in the fight against terrorism.[648]

The measures adopted, included the grant of wider access to certain types of data entered in the SIS to judicial[649] and law enforcement authorities, among which the European Police Office (Europol) and the national members of Eurojust;[650] the extension of the categories of missing objects about which alerts may be entered;[651] the recording of transmissions of personal data;[652] and the enactment of provisions concerning the exchange of all supplementary information through the SIRENE authorities in the Member States.[653]

Both the Regulation and the Decision recognise the need to develop a new, second generation SIS, the 'SIS II', "with a view to the enlargement of the European

---

[645] The first pillar measure is Council Regulation (EC) No 378/2004 of 19 February 2004 on procedures for amending the Sirene Manual OJ L 64/5 of 2.3.2004; *See* also Commission Decision 2006/758/EC of 22 September 2006 on amending the Sirene Manual OJ L 317/41 of 16.11.2006.

[646] Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism OJ L 162/29 of 30.4.2004.

[647] Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism OJ L 68/44 of 15.3.2005.

[648] Recital 4 of the Regulation and the Council decision refers to the Conclusions of the Laeken European Council of 14 and 15 December 2001 and in particular Conclusions 17 (cooperation between specialised counter-terrorism services), 43 (Eurojust and police cooperation with regard to Europol) and the Action Plan of 21 September 2001 against terrorism that called for an enhancement of the SIS' capabilities.

[649] Article 1 (3) of Regulation 871/2004 and Article 1 (8) of Council decision 2005/211/JHA.

[650] Article 1 (9) of Council decision 2005/211/JHA.

[651] Article 1 (6) of Regulation 871/2004 and Article 1 (10) of Council decision 2005/211/JHA.

[652] Article 1 (2) of Regulation 871/2004 and Article 1 (2) and (7) of Council decision 2005/211/JHA.

[653] Article 1 (1) of Regulation 871/2004 and Article 1 (1) of Council decision 2005/211/JHA. *See* also BROUWER, DIGITAL BORDERS AND REAL RIGHTS, *supra* note 269, at 81.

Union and allowing for the introduction of new functions, while benefiting from the latest developments in the field of information technology."[654]

2.3 From SIS to SISone4ALL and SIS 1+

One of the most important challenges faced by the Schengen Information System concerned the enlargement of the EU with the accession of the ten new Member States on 1 May 2004. The SIS was a system with limited capabilities: it was not able to serve technically more than 18 countries. The need, thus, for the development of a second generation SIS was pressing. However, a number of delays in launching the new system were encountered.[655] This led to the disappointment of the new Member States that had invested considerable resources and were expecting to join the Schengen area by October 2007.[656]

Since completion of SIS II by this date was clearly out of reach, a quick alternative solution that would enable the new Member States to join the system as soon as possible was adopted. In October 2006 Portugal put forward a proposal for a so-called 'SIS one4all', that would allow the SIS to be adapted in order to include the new Member States. The proposal was met with distrust especially by the old Member States,[657] but, on 5 December 2006 the Justice and Home Affairs Council, after re-affirming that "the development of the SIS II remains the absolute priority", decided to implement SISone4all to integrate nine of the Member States which joined the European Union in May 2004 into SIS 1+ temporarily. The aim of the SISone4ALL project was to facilitate the process leading to the lifting of internal border controls with the Member States concerned between December 2007 and March 2008.[658] In

---

[654] Recital 2 of the Council Regulation and the Council Decision.
[655] *See* HOUSE OF LORDS EUROPEAN UNION COMMITTEE, SCHENGEN INFORMATION SYSTEM II (SIS II) ¶ 22 (9th Report of Session 2006–07).
[656] *Id.* at 25.
[657] *Id.* at 26.
[658] SCHENGEN JOINT SUPERVISORY AUTHORITY, ACTIVITY REPORT – DECEMBER 2005 – DECEMBER 2008 9. Bertozzi characterises the Portuguese proposal for SISone4all as a "patchwork solution", that nevertheless succeeds in "giving Member States and the Commission more time to complete the development of SIS II, including the testing phases and "switch scenarios"." Bertozzi, *supra* note 626, at 20. The House of Lords European Union Committee is also critical towards the EU institutions: "Since the requirement to develop a new generation of the SIS was apparent many years ago, in the light of the planned enlargement of the EU, there was an opportunity for long-term strategic planning of the project, which could have avoided the delays and reduced the costs which have affected the SIS II project. This opportunity was missed. There are lessons to be learned by the EU as regards the

accordance with Council Decision 2007/471/EC of 12 June 2007,[659] the new Member States were able to enter data into the SIS and use SIS data from 1 September 2007.

However, the SISone4all is only a temporary solution and the migration from the Schengen Information System (now, SIS 1+) to the second generation Schengen Information System (SIS II) should take place as soon as possible. For this reason, in October 2008 the Council adopted Regulation 1104/2008[660] and Decision 2008/839/JHA[661] on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II). Article 11(2) of the Regulation and the Decision provided that the migration of the Member States participating in SIS 1+ to SIS II using the interim migration architecture, would be completed by 30 September 2009 at the latest. However, in September 2009 the Commission recognised that a number of issues identified during the testing of SIS II led to delay in the implementation of the activities set out in Regulation 1104/2008 and in Decision 2008/839/JHA.[662] Therefore, taking into account the time required to resolve these outstanding issues, it held that the date for migration from SIS 1+ to SIS II, set for September 2009, was no longer realistic.[663] Due to further delays in the completion of the SIS II system two further Council Regulations, amending Regulation 1104/2008[664] and Decision 2008/839/JHA[665] were adopted in 2010. The

---

planning and development of other large-scale multinational information systems." House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 27.

[659] Council Decision 2007/471/EC of 12 June 2007 on the application of the provisions of the Schengen *acquis* relating to the Schengen Information System in the Czech Republic, the Republic of Estonia, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic OJ L 179/46 of 7.7.2007.

[660] Council Regulation (EC) No 1104/2008 of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) OJ L 299/43 of 8.11.2008.

[661] Council Decision 2008/839/JHA of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), OJ L 299/43.

[662] Report from the Commission to the Council and the European Parliament on the Development of the Second Generation Schengen Information System (SIS II), Progress Report January 2009-June 2009, COM(2009) 555 final, 5; Report from the Commission to the Council and the European Parliament on the Development of the Second Generation Schengen Information System (SIS II), Progress Report July 2009- December 2009, COM(2010)221 final; and, Report from the Commission to the Council and the European Parliament on the Development of the Second Generation Schengen Information System (SIS II), Progress Report January 2010- June 2010, COM(2010) 633 final.

[663] Commission Decision 2009/720/EC of 17 September 2009 laying down the date for the completion of migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) OJ L 257/26 of 30.9.2009; and Commission Decision 2009/724/JHA of 17 September 2009 laying down the date for the completion of migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) OJ L 257/41 of 30.9.2009.

[664] Council Regulation (EU) No 541/2010 of 3 June 2010 amending Regulation (EC) No 1104/2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) OJ L 155/19 of 22.6.2010.

new timeframe for the migration to SIS II is now foreseen to be completed by 31 March 2013 or, if an alternative technical scenario will be used, by 31 December 2013.

3. The Second Generation Schengen Information System (SIS II)

3.1 Introduction

Already as early as in October 1997, the Schengen Executive Committee had declared the plan to set up a new SIS generation with modernized information technologies, broader competences and additional performance elements.[666] The main purpose for the development of the SIS II was twofold: on the one hand, to make the system technically able to serve more than 18 countries, in order to accommodate the inclusion of the EU's new Member States; on the other hand, to introduce new functionalities in the system and to provide for additional technical features, in particular for the inclusion of biometric data.[667] However, the delays in launching the new system, which is still –at the time of the writing- not operational,[668] and the need

---

[665] Council Regulation (EU) No 542/2010 of 3 June 2010 amending Decision 2008/839/JHA on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) OJ L 155/23 of 22.6.2010.

[666] SCH/Com-ex (97) 24, OJ L 239/442 of 22.9.2000. It should be noted that while this decision of the Schengen Executive Committee forms part of the Schengen *acquis* (as it is the case with all decisions of the Executive Committee) and is therefore publishable, it was not published until September 2000, meaning thus that it was classified up to this date as 'confidential'. *See* also Torsten Stein, *European and German Security Policy, Especially Border Controls, with Regard to International Terrorism*, 35 ISRAEL YEARBOOK ON HUMAN RIGHTS 231, 233 (2005).

[667] In its Communication on the development of a common policy on illegal immigration, smuggling and trafficking of human beings, the Commission stated the importance given at the Laeken (see Presidency Conclusions of the Laeken European Council, 14–15 December 2001, SN 00300/01, point 42) and Seville (see Presidency Conclusions of the Seville European Council, 21–22 June 2002, SN 13463/02, point 30) European Councils as well as in its Comprehensive Plan (Comprehensive Plan to combat illegal immigration and trafficking of human beings, 2002/C142/02, OJ C142/23 14/06/2002) to establishing the second generation of the Schengen Information System (SIS II) to better fight against terrorism. *See* Communication from the Commission to the European Parliament and the Council in view of the European Council of Thessaloniki on the development of a common policy on illegal immigration, smuggling and trafficking of human beings, external borders and the return of illegal residents COM(2003) 323 final.

[668] As a commentator explains the SIS II project has encountered "substantial delays, an escalating budget, political crises and criticisms." JOANNA PARKIN, THE DIFFICULT ROAD TO THE SCHENGEN INFORMATION SYSTEM II: THE LEGACY OF "LABORATORIES" AND THE COST FOR FUNDAMENTAL RIGHTS AND THE RULE OF LAW (CEPS, April 2011); JOANNA PARKIN, THE SCHENGEN INFORMATION SYSTEM AND THE EU RULE OF LAW (INEX Policy Brief, No. 13, June 2011). *See* also ANAÏS FAURE

for the new Member States to join the system as soon as possible led to the adoption of the quick alternative solution of the SISone4ALL.

On 31 May 2005, the Commission introduced its proposals for the adoption of three legislative measures to establish the SIS II: a (then first pillar) Regulation concerning the immigration aspects of the system to be adopted under Title IV of the EC Treaty (visas, asylum immigration and other policies related to the free movement of persons)[669] (hereinafter the 'SIS II Regulation' or the 'immigration Regulation'); another, separate (first pillar) Regulation concerning access to the system by vehicle registration authorities to be based on Title V (Transport) of the EC Treaty[670] (hereinafter the 'vehicles' Regulation'); and, a (then third pillar) Council Decision concerning use of the system for policing and criminal law purposes to be based on Title VI of the EU Treaty[671] (hereinafter the 'SIS II Decision'). The separate proposals were necessary due to the different legal bases and decision-making procedures concerned.[672] However, as it is stressed in the Recitals of both the SIS II Regulation and the Council Decision

> "the fact that the legislative basis necessary for governing SIS II consists of separate instruments does not affect the principle that SIS II constitutes one single information system that should operate as such."[673]

The three measures were discussed as a package, and the two Regulations were adopted on 20 December 2006, while the third pillar Decision was adopted only on 12 June 2007.[674]

ATGER, THE ABOLITION OF INTERNAL BORDER CHECKS IN AN ENLARGED SCHENGEN AREA: FREEDOM OF MOVEMENT OR A SCATTERED WEB OF SECURITY CHECKS? (CHALLENGE Research Paper No. 8, March 2008).

[669] Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II) COM (2005) 236 final, 31 May 2005.

[670] Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates COM (2005) 237 final, 31 May 2005.

[671] Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II) COM (2005) 230 final, 31 May 2005.

[672] Peers, *Key Legislative Developments on Migration in the European Union: SIS II*, *supra* note 644, at 81.*See* also footnote 38 therein where he explains the decision- making procedures under the different pillars and the opt-outs for the UK, Ireland and Denmark. *See* also House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 41.

[673] Recital 4 of the SIS II Regulation and the Decision.

[674] The delay in adopting the Decision was due to national parliamentary scrutiny reserves from certain Member States (such as Denmark and Sweden). *See* Vasiliki Christou, *The Council Decision of 12 June 2007 on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II)*, 14 COLUM. J. EUR. L. 649 (2008).

Below the basic features of the immigration Regulation that constitutes alongside with the Regulation on vehicles[675] and the Decision the legal basis of the SIS II will be briefly presented, but the bulk of the analysis will focus on the examination of the Council Decision as this regulates the use of the SIS II database for law enforcement purposes and in particular for the fight against terrorism. Nevertheless, it should be mentioned that the structure and a number of provisions of the Decision and the immigration Regulation are almost identical.

3.2 The Regulation on the establishment, operation and use of the second generation Schengen Information System (SIS II)[676]

The SIS II Regulation constitutes the legal base for the "conditions and procedures for the entry and processing in SIS II of alerts in respect of third- country nationals, the exchange of supplementary information and additional data for the purpose of refusing entry into, or a stay in, a Member State."[677] Chapter I of the SIS II Regulation sets out the general provisions dealing with the purpose and scope, definitions, technical architecture and costs of SIS II (Articles 1–5). Chapter II lays down the responsibilities of the Member States, which include setting up, operating and maintaining the N.SIS II. (Articles 6–14) Chapter III provides for the responsibilities of the 'Management Authority' of SIS II (Articles 15–19). Chapter IV sets out the key rules on the grounds for issuing immigration alerts, the types of data kept, access to those alerts by various authorities and the conservation period for data (Articles 20–30). It is worth noting that Article 26 of the Regulation introduces a new category of third- country nationals to be entered in SIS II for the purpose of refusing entry or stay. This refers to third- country nationals "who are the subject of a restrictive measure intended to prevent entry into or transit through the territory of Member States, ... including measures implementing a travel ban issued by the Security Council of the United Nations." In essence in this category of alert fall third-

[675] Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates OJ L 381/1 of 28.12.2006.
[676] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381/4 of 28.12.2006.
[677] Article 2 (1) of the SIS II Regulation.

country nationals that are either subject to UN or EU- autonomous listing.[678] In Chapter V of the Regulation provides for the general data-processing rules (Articles 31–39).

Chapter VI of the Regulation lays down a number of data protection rules (Articles 40–47). In particular, Article 40 bans the storage of 'sensitive' information such as racial and religious information as defined in EC data protection legislation (and also in the Council of Europe data protection Convention). Article 41 provides that a person's right of access to SIS II data concerning him or her shall be exercised in accordance with the law of the Member State in which that access is invoked. National law may provide that the national supervisory authority will decide on whether the data may be transmitted. A Member State which has not issued the alert in question must first consult the Member State which issued the alert before releasing the data. However, the Regulation stipulates that information shall not be communicated to the data subject if this is indispensable for the performance of a lawful task in connection with an alert or for the protection of the rights and freedoms of third parties.[679] Furthermore, any person has the right to have factually incorrect data corrected or unlawfully stored data deleted.[680] The Regulation also provides for a right to information in accordance with the Data Protection Directive.[681] This means that the third country nationals who are subject to a SIS II alert, must be informed of the identity of the controller of their data, the purposes of the data processing and any further information such as the recipients of the data, the conditions and consequences of not replying to questions asked, and the existence of the rights of access and rectification, insofar as the further information is necessary in the circumstances 'to guarantee fair data processing'.[682] This information need not be provided in three cases: where the data was not obtained from the data subject; where the provision of

[678] On listing of individuals suspected for terrorism in the EU *see inter alia* ECKES, *supra* note 443. On EU Court's response on the issue *see* Sara Poli & Maria Tzanou, *The Kadi Rulings: A Survey of the Literature*, 28 YEARBOOK OF EUROPEAN LAW 533 (2009); Maria Tzanou, *Case-note on Joined Cases C-402/05 P & C-415/05 P Yassin Abdullah Kadi & Al Barakaat International Foundation v Council of the European Union & Commission of the European Communities*, 10 GERMAN LAW JOURNAL 121 (2009); Maria Tzanou & Sufyan Droubi, *Case -note on Case T-318/01 Omar Mohammed Othman v Council of the European Union and Commission of the European Communities, Judgment of the Court of First Instance of 11 June 2009 (Seventh Chamber)*, 47 COMMON MARKET LAW REVIEW 1233 (2010).

[679] Article 41 (4) of the SIS II Regulation.

[680] Article 41 (5) of the SIS II Regulation.

[681] Article 42 (1) of the SIS II Regulation which refers to Articles 10 and 11 of the Data Protection Directive.

[682] Peers, *Key Legislative Developments on Migration in the European Union: SIS II*, *supra* note 644, at 97.

information would be impossible or require disproportionate effort; where the data subject already has the information; or where national law allows for the right of information to be restricted, "in particular in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences."[683] Article 43 of the Regulation provides for a right of review before the courts or authorities of any Member State as regards the right of access, correction or deletion or as regards obtaining information or compensation. Finally, Articles 44 and 45 regulate the supervision of the N.SIS II and the Management Authority respectively.

Chapter VII contains rules concerning liability and sanctions for breach of the Regulation (Articles 48–49) and Chapter VIII lays down a number of rules concerning monitoring and statistics, the comitology process, the repeal of all parts of the Schengen *acquis*, a transitional period during which alerts are transferred from SIS to SIS II, and the decision on when SIS II will begin operations (Articles 50–55).

3.3 The Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II)[684]

i. Scope and Purpose of SIS II

Council Decision 2007/533/JHA, constitutes the "necessary legislative basis" for governing SIS II in respect of matters falling within the scope of police and judicial cooperation in criminal matters.[685]

According to Article 1 (2) of the Decision, the purpose of SIS II is

[683] Article 42 (2) (c) of the SIS II Regulation.
[684] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205/63 of 7.8.2007.
[685] Recital 3 of the SIS II Decision. It should be stated that at the time of the adoption of the Decision (in June 2007), the EU constitutional architecture was based on the pillar structure. Therefore, the Decision covered the third pillar measures (concerning police and judicial cooperation) of SIS II, while the immigration Regulation covered the first pillar matters (concerning visas, immigration, external border controls). This particularity of the SIS II is maintained- at least for the time being- even after the entry into force of the Lisbon Treaty as from the 1st December 2009, which abolished the pillar structure of the EU.

"to ensure a high level of security within the area of freedom, security and justice of the European Union including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the EC Treaty relating to the movement of persons in their territories, using information communicated via this system."[686]

Two objectives concerning SIS II can be discerned: The first is a more general one and regards the exchange of information for the "maintenance of public security and public policy", while the second is more specific and regards the exchange of information for the purposes of controls on persons and objects. This means that SIS II is not limited to police and judicial cooperation by supporting the controls of persons and objects (as it was the case with the old SIS), but it might be developed also to be used as a tool to support police and judicial cooperation in a more general way.[687]

The widening of the purpose of the SIS II is not without problems. The objective of "maintaining public security" seems unduly broad[688] and creates uncertainty regarding the possibilities of use of the SIS II for the exchange of information between police and judicial authorities in practice.[689]

The European Council had noted already since 2002 that the potential of SIS should be maximised within the framework of police cooperation beyond its compensatory role under the first generation system.[690] In this respect, it recognised that

"the idea of using the SIS data for other purposes than those initially foreseen, and especially for police information purposes in a broad sense, is now widely

---

[686] *See* also Recital 5 which provides that: "SIS II should constitute a compensatory measure contributing to maintaining a high level of security within the area of freedom, security and justice of the European Union by supporting operational cooperation between police and judicial authorities in criminal matters."

[687] *See* SCHENGEN JOINT SUPERVISORY AUTHORITY, OPINION ON THE PROPOSED LEGAL BASIS FOR SIS II 11.

[688] BROUWER, DIGITAL BORDERS AND REAL RIGHTS, *supra* note 269, at 93.

[689] ALICE GARSIDE, THE POLITICAL GENESIS AND LEGAL IMPACT OF PROPOSALS FOR THE SIS II: WHAT COST FOR DATA PROTECTION AND SECURITY IN THE EU? 5 (Sussex Migration Working Paper no. 30, March 2006).

[690] Note from Presidency to Working Party on SIS Requirements on SIS, Council Doc. 5968/02, 5.2.2002, 2.

agreed upon and even follows from the Council conclusions after the events of 11 September 2001."[691]

This implies that the SIS II is developing from a tool providing informational assistance with regard to border controls into a much more complex, investigative instrument that can be used by the police authorities in each Member State for various purposes. Such a development might transform SIS from a compensatory measure for the removal of border controls to a law enforcement and intelligence instrument.[692]

The Schengen Joint Supervisory Authority ('Schengen JSA') who is responsible for monitoring the SIS and its successors' compliance with data protection norms, noted this change with concern in its report of 2002 with regard to the SIS II proposals:

"the JSA has warned that, as they stand, these proposals would result in a fundamental change to the nature of the system … the SIS II looks set to become a multi-purpose investigation tool'.[693]

ii. Content

a. Operational Management

The issue of who would be responsible for the operational management of SIS II[694] proved particularly contentious during the negotiations for the adoption of the legal framework of SIS II, as the Commission initially proposed to reserve this role for itself. The Member States, however, objected to this idea and a different solution

[691] *Id.*

[692] In his Oral Evidence before the House of Lords, Mr Smith, Information Commissioner noted that: "[SIS II] is becoming an investigative tool, not a replacement for removal of border controls and some of the things like access by Europol also feed into that. Europol is very much an analytical intelligence investigative type of organisation, so how will they use their access? We have this underlying concern of function creep, I think we have used that term here before. There is scope for function creep here and we are concerned that there may be inadequate control over that." *See* House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, at 98. *See* also BROUWER, DIGITAL BORDERS AND REAL RIGHTS, *supra* note 269, at 106.

[693] SCHENGEN JOINT SUPERVISORY AUTHORITY, REPORT JAN 2002 – DEC 2003 17.

[694] According to Article 15 (8) of the Decision the operational management of Central SIS II consists of "all the tasks necessary to keep Central SIS II functioning 24 hours a day, seven days a week, in particular the maintenance work and technical developments necessary for the smooth running of the system."

had to be found. According to the text of the Decision, for an initial transitional period of no more than five years, the Commission will be responsible for the operational management of Central SIS II and of parts of the communication infrastructure.[695] However, the Commission, in order to ensure a smooth transition to SIS II, may delegate some or all of these responsibilities to national public sector bodies in two different countries.[696] In the long term, a 'Management Authority' entrusted with the responsibility of administering SIS II will be established.[697]

b. Categories of alert

The SIS database contains a number of so-called 'alerts', which are essentially requests by the State that issued the alert to the other Schengen countries to take a certain action.[698] The SIS II Decision defines 'alerts' as the set of data entered in the system in order to allow the competent authorities "to identify a person or an object with a view to taking specific action."[699] The Decision provides for the following categories of alerts that can be object to a report in the SIS II: a) data on persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes will be entered at the request of the judicial authority of the issuing Member State;[700] b) data on missing persons who need to be placed under protection;[701] c) data on persons sought to assist with a judicial procedure, in particular witnesses, persons summoned or persons sought to be summoned to appear before the judicial authorities in connection with criminal proceedings, persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings, and persons who are to be served

[695] Recital 9 of the SIS II Decision.
[696] The management of SIS II will be delegated to France and Austria, which are currently responsible respectively for the main site in Strasbourg and the back-up site in Sankt Johann im Pongau. Those Member States will, however, pursuant to Article 15 (7) be held accountable for their management of the system in accordance with EU laws. In particular, they will be subject to the control mechanism of the Court of Justice, the Court of Auditors and the European Data Protection Supervisor, as this provided for by EU law.
[697] According to a Joint Statement of the European Parliament, the Council and the Commission (Statement 235/06, in the monthly summary of Council acts for Dec. 2006, available at http://register.consilium.europa.eu/pdf/en/06/st17/st17121.en06.pdf) an Agency will be established in order to serve as the Management Authority of SIS II.
[698] Dumortier, *supra* note 628, at 97.
[699] Article 3 (1) (a) of the SIS II Decision.
[700] Article 26 of the SIS II Decision.
[701] Article 32 of the SIS II Decision.

with a summons to report in order to serve a penalty involving deprivation of liberty;[702] and, data on persons subject to discreet checks or specific checks.[703] The SIS also stores data on objects (vehicles, boats, aircrafts and containers) for the purposes of discreet or specific checks,[704] as well as for the purposes of seizure or use as evidence in criminal proceedings.[705]

The SIS operates in a 'hit/ no hit' basis which allows the competent authorities in the Member States to check rapidly whether a person being checked is mentioned in the database or not.[706] In the case of a 'hit' (a positive response), the SIS (according to the type of the alert entered to it) will indicate the action that has to be undertaken (for example, arrest).[707] This means that if a consulting officer gets a 'hit' in the NSIS, he/she must carry out the action requested by the reporting Schengen country (for example, put the person under arrest) and immediately inform his/her national SIRENE, which will take the necessary steps to contact the reporting country and to provide supplementary information if needed. [708]

c. Categories of data

The data stored in the system for the different categories of alert included under the Schengen Convention for the –old- SIS 'alphanumeric' information (letters and numbers) comprising (as regards individuals) data on: names (surname and forenames); "specific objective physical characteristics not subject to change"; date and place of birth; sex; nationality; whether the persons are armed or violent; the reason for the alert; and the action to be taken.[709]

The SIS II Decision provides for a number of further data to be included in the second generation system. Those include additional alphanumeric data, such as multiple nationalities; the authority issuing the alert, a reference to the decision giving

[702] Article 34 of the SIS II Decision.
[703] Article 36 of the SIS II Decision.
[704] *Id.*
[705] Article 38 of the SIS II Decision.
[706] *See* Sergio Carrera, *What Does Free Movement Mean in Theory and Practice in an Enlarged EU?*, 11 EUROPEAN LAW JOURNAL 699, 718 (2005).
[707] *See* Dumortier, *supra* note 628, at 95.
[708] Article 3 (b) of the SIS II Decision.
[709] Article 94 (3) of the Schengen Convention.

rise to the alert; and links to other alerts issued in SIS II.[710] More importantly, however, according to the SIS II Decision biometric data will be stored in the system, in particular fingerprints and photographs.[711]

This introduces a major change in the nature of the SIS, which is transformed from a 'hit/no hit' system to an identification tool. In other words, SIS II might be searchable on the basis of the biometric data it contains, i.e. photographs and fingerprints without needing additional data on the person concerned such as name and surname. The inclusion of biometric data into SIS II means also that now all three EU centralised databases that hold information on individuals (SIS II, VIS, EURODAC) will be using biometric identifiers.[712]

d. Retention period

According to Article 44 of the Decision, alerts on persons entered in SIS II will be kept "only for the time required to achieve the purposes for which they were entered." As a general principle, the need to keep alerts on persons entered in SIS II must be reviewed after a period of three years.[713] In the case of alerts on persons to be subject to discreet checks the review period is one year.[714] Alerts must be automatically erased after the review period,[715] except where the Member State that issued the alert has communicated, based on a comprehensive individual assessment, the extension of the alert to CS-SIS.[716]

e. Access to the data

The authorities that have access to SIS II data fall in two broad categories: On the one hand, those who are responsible for border controls; on the other hand, those

[710] Article 20 (3) of the SIS II Decision.
[711] Article 20 (3) (e) and (f).
[712] See point 1.7.2. of the Hague Programme where the European Council held that biometric identifiers and data are necessary for the fight against terrorism.
[713] Article 44 (2) of the SIS II Decision.
[714] *Id.*
[715] Article 44 (4) of the SIS II Decision.
[716] Article 44 (5) of the SIS II Decision.

carrying out police and customs checks.[717] Access to SIS II data is also granted to national judicial authorities in the performance of their tasks, as provided for in national legislation.[718]

As seen above, the Council decision 2005/211/JHA, adopted in the aftermath of the Madrid terrorist attacks, had already given to Europol and Eurojust access to SIS data for the purpose of the fight against terrorism. The SIS II Decision also grants access to SIS II data to Europol and Eurojust.[719] According to Article 41 (1), Europol will "within its mandate have the right to access and search directly," data entered into SIS II of persons wanted for arrest for surrender or extradition purposes, of persons and objects for discreet checks and of objects for seizure or use as evidence in criminal proceedings. If a search by Europol reveals the existence of an alert in SIS II, Europol must inform the Member State which issued the alert.[720] The Decision provides, however, that the use of information obtained from a search in the SIS II will be subject to the consent of the Member State concerned.[721] Furthermore, Europol cannot communicate such information to third countries and third bodies without the consent of the Member State concerned.[722] The Decision also imposes a number of obligations on Europol, among which, to record every access and search made by it, to limit access to data entered in SIS II to specifically authorised staff and to allow the Europol Joint Supervisory Body to review its activities regarding the exercise of its right to access and search data entered in SIS II.[723]

Article 42 of the SIS II Decision grants access to the national members of Eurojust and their assistants to search "within their mandate" data entered in SIS II, of persons wanted for arrest for surrender or extradition purposes, of missing persons, of persons sought to assist with a judicial procedure and on objects for use as evidence in criminal proceedings. The Decision makes Eurojust's access to SIS II subject to certain conditions similar to those laid down for Europol.[724] Finally, Article 43 of the

---

[717] Article 40 (1) of the SIS II Decision.
[718] Article 40 (2) of the SIS II Decision.
[719] According to the Opinion of the Schengen Joint Supervisory Authority on the Proposed Legal Basis for SIS II, "allowing such organisations access will have consequences for the character of the SIS II, as the information obtained from the system is more likely to be put to operational use by these organisations." *See* Schengen Joint Supervisory Authority, *Opinion on the Proposed Legal Basis for SIS II*, *supra* note 687.
[720] Article 41 (2) of the SIS II Decision.
[721] Article 41 (3) of the SIS II Decision.
[722] *Id.*
[723] Article 41 (5) of the SIS II Decision.
[724] Article 42 (2) – (7) of the SIS II Decision.

SIS II Decision reiterates the existing rule also under SIS[725] that "users may only access data which they require for the performance of their tasks."

Overall, the provisions of the SIS II Decision introduce essentially two different types of authorities that have access to SIS II data: On the one hand, these that have access in order to fulfil their own particular tasks, such as for instance border control authorities that have access for a specific purpose, relating to an alert, or police officers; and on the other hand, authorities such as Europol and Eurojust,[726] for which there is no further specification of the purpose of the access.[727] All the more, although access to SIS II data is granted to Europol and Eurojust to the extent that this is necessary "for the performance of their tasks;" this condition does is not so satisfactory from the point of view of legal certainty as it seems, considering that Europol and Eurojust's tasks might evolve over time.[728] For this reason, it would have been preferable if the tasks for the performance of which Europol and Eurojust can use SIS II data had been more explicitly and restrictively defined by the Decision and in any case subjected to stricter conditions.[729]

Even if one accepts that the Decision restraints Europol and Eurojust's access to SIS II data by allowing it only with relation to certain alerts (Articles 26, 36 and 38 for Europol; and, Articles 26, 32, 34, and 38 for Eurojust), and therefore those two agencies are not given access to information that falls outside their competence; the fact remains that there is still a significant quantity of SIS II data, which Europol and Eurojust should not have access to.[730] For instance, Article 26 of the Decision allows alerts for arrest to be entered in the SIS II on the basis of the European Arrest

---

[725] The rule is found in Article 101 (3) of the Schengen Convention.

[726] *See* PETER HOBBING, AN ASSESSMENT OF THE PROPOSALS OF REGULATION AND DECISION WHICH DEFINE THE PURPOSE, FUNCTIONALITY AND RESPONSIBILITIES OF THE FUTURE SIS II (Briefing Paper for Directorate C of the European Parliament, IP/C/LIBE/OF/2005-168, February 15, 2006).

[727] As the EDPS has put it eloquently in his Opinion: "Among all the authorities having access for their own purposes, [Europol and Eurojust] benefit from an access granted in the most open terms." *See* Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)230 final); the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005)237 final) (2006/C 91/11) OJ L C 91/38 of 19.4.2006, para 4.2.3.

[728] *Id.*

[729] The Schengen JSA has noted: "there ought to be clarification of the specific tasks for which Europol, Eurojust (and any other organisations) require access to the SIS II." *See* JSA opinion on the development of SIS II, SCHAC 2504/04, 4.

[730] Schengen Joint Supervisory Authority, *Opinion on the Proposed Legal Basis for SIS II*, *supra* note 687, at 9.

Warrant,[731] but the range of offences covered by this extends well beyond those offences for which Europol (and Eurojust) are competent.[732] In this respect, the House of Lords Select Committee on European Union expressed concern that the provisions granting access to SIS II data to Europol and Eurojust will lead to a significant change in the powers of these agencies since their respective instruments do not provide in fact for such a possibility.[733]

f. Exchange of information with third parties

According to the SIS II Decision, the general rule is that "data processed in SIS II shall not be transferred or made available to third countries or to international organisations."[734] However, the Decision provides by way of derogation for the possibility of exchange of certain passport data[735] with Interpol,[736] subject to safeguards and conditions guaranteeing an adequate level of protection.[737]

This does not seem to be the end of the story. As mentioned above, pursuant to Article 41 (2), Europol can use the information obtained from a search in the SIS II "subject to the consent of the Member State concerned." If, however, the Member State allows the use of such information, the handling thereof will be governed by the Europol Convention. Europol is free to communicate further such information to third countries and third bodies with the consent of the Member State concerned. As the Europol Data Protection Officer explained to the House of Lords Select Committee on European Union this means in essence that if there is an alert, Europol will contact the Member State concerned and ask for permission to use the alert and, if necessary, ask for supplementary information. The information that Europol will get from the Member State will be considered by Europol as a Member State contribution to Europol's system, hence it is no longer Schengen information but it becomes Europol

[731] See Council Framework Decision on the European arrest warrant and the surrender procedures between Member States 2002/584/JHA of 13 June 2002 OJ L 190/1 of 18.7.2002.
[732] See Article 8 of the Council Framework Decision on the European Arrest Warrant.
[733] House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 115.
[734] Article 54 of the SIS II Decision.
[735] This is data on the passport number, the country of issuance and the document type of stolen, misappropriated, lost or invalidated passports entered in SIS II.
[736] *See* also Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol OJ L 27/61 of 29.1.2005.
[737] Article 55 of the SIS II Decision. *See* also Recital 18.

information and from then on it will be handled according to Europol's Convention.[738] This information can, therefore, be transferred, under the terms of the Europol Convention, to third states or third parties with which Europol has agreements in place for the exchange of personal data.[739] The Decision expressly stipulates that such a transfer can only take place with the consent of the Member State concerned, but one may wonder whether this is merely a typical requirement since the Member State has already given its consent for the handling of the data by Europol.

g. Interlinking of alerts

A new feature of the Second Generation Schengen Information System is the possibility to interlink the alerts entered in the system.[740] This means essentially that when an alert on a person is entered in SIS II, a link to further alerts on other persons or objects can be added as well.[741] The effect of such a link shall be to establish a relationship between the two alerts.[742] According to the SIS II Decision, links between alerts can be created "only when there is a clear operational need."[743] Links between alerts may not affect the rights of access of the relevant authorities. This means that authorities with no right of access to certain categories of alerts cannot be able to see the link to an alert to which they do not have access.[744] The Decision also stipulates that if a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or international obligations, it may take the necessary measures to ensure that there can be no access to the link from its national authorities.[745]

The interlinking of alerts is not merely an enhanced technological feature of the new system. It is aimed to make SIS II a powerful investigation tool in the hands of law enforcement authorities that can have an even more completed knowledge on

---

[738] House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 108.
[739] Europol has operational agreements in place with Canada, Croatia, Eurojust, Iceland, Interpol, Norway, Switzerland and the United States.
[740] Article 52 of the SIS II Decision.
[741] BROUWER, DIGITAL BORDERS AND REAL RIGHTS, *supra* note 269, at 101.
[742] Article 52 (1) of the SIS II Decision.
[743] Article 52 (4) of the SIS II Decision.
[744] Article 52 (3) of the SIS II Decision.
[745] Article 52 (6) of the SIS II Decision.

individuals entered in SIS II, including their relationships with other family members, for instance.[746]

3.4 SIS II data protection rules: The applicable legal framework

As the House of Lords European Union Select Committee has eloquently observed, the data protection regime applicable to the SIS II rules is "unduly complex."[747] This is due to the fact that SIS II is governed by "a myriad of legal instruments,"[748] between which, the distribution of *lex specialis* and the *leges generales* seems a confusing and cumbersome exercise[749] that goes completely against a clear and accessible data protection legal framework.

This complexity is attributed essentially to the SIS II particular nature that is a single information system based on two -not to mention three- different legal bases (the immigration Regulation, the Decision, and the Regulation on vehicles). Each of these instruments have their own data protection provisions ('*lex specialis*'), which are complemented by a different general data protection legislation ('*lex generalis*') for each sector (Commission, Member States acting in former first pillar, Member States acting in police and judicial cooperation). This means that apart from the data protection regime established in the SIS II legislation, the following instruments are also applicable –according to the nature of the processing- to data processed in the SIS II system: the Data Protection Directive, Regulation 45/2001 and the Data Protection Framework Decision.[750] In this respect, on the one hand, what concerns the processing of data coming into the SIS II immigration Regulation (such as for instance, the processing of data on third country nationals to be refused entry) falls within the scope of the Data Protection Directive, and to the extent that Community institutions (i.e. the Commission) are involved Regulation 45/2001 applies. On the other hand, data processing through SIS II for law enforcement purposes under the

[746] An example of interlinking of alerts given by Brouwer is an alert of the husband that is convicted criminal to be refused entry that can be linked with an alert on the wife that is a suspected terrorist. *See* BROUWER, DIGITAL BORDERS AND REAL RIGHTS, *supra* note 269, at 102.
[747] House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, at 130.
[748] House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655.
[749] Memorandum by JUSTICE, *Id.* at 132.
[750] For a detailed analysis of the scope and content of these legislative instruments, see Chapter 4.

Decision, falls within the scope of the Council of Europe Data Protection Convention and the Data Protection Framework Decision.

This structure raises the question of how to deal with the specialised sets of rules in their relationship to general law.[751] In this regard, the EDPS proposed in his Opinion that the *lex specialis* must always be in conformity with the *lex generalis*; it elaborates and specifies the *lex generalis* but cannot be conceived as an exception from it. As to the question of which rule should be applied in specific cases, the EDPS suggested that the general principle is that "the *lex specialis* applies in priority, but wherever it is silent or unclear, reference should be made to the *lex generalis*."[752] This seems a satisfactory solution, but problematic situations might still arise in case of potential conflicts between *lex specialis* and *lex generalis*.[753]

Furthermore, the specific rules on data protection and data processing contained, on the one hand, in the SIS II Regulation and, on the other hand, in the SIS II Decision on cooperation in criminal law and policing "have almost as many differences as they have similarities."[754] For instance, the 'right of information' (the right of a person to know that a file with his personal data has been established, along with who has established the file and for what purpose) constitutes an important safeguard of the SIS II Regulation,[755] but is nowhere to be found in the SIS II Decision. This division raises issues of transparency, equality and legal certainty of the SIS II database legislation, especially if one takes into account the fact that this purports to be a *single* information system,[756] (inevitably) based on two legal bases.[757] However, the result seems to be that individuals, the data of whom are stored in the SIS II, and authorities that use the system will be faced with a considerable confusion on exactly which rules apply in every situation.

In this regard, many commentators have argued that the entry into force of the Lisbon Treaty would solve this problem because of the collapsing of the pillars, which could provide "an extra motive to extend the application of the EC Directive 95/46 to

---

[751] In the words of the EDPS, "the legal framework is so complex that it is very likely to engender some confusion in the practical application." EDPS, *supra* note 105, para 2.2.4.
[752] EDPS, *supra* note 105, para 2.2.1.
[753] This scenario seems rather hypothetical, but as the House of Lords Select Committee observes in its Report: "We have asked a number of witnesses how potential conflicts are to be resolved, and have received as many answers as there are witnesses." *See* House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, at 116.
[754] *Id.*, para. 112.
[755] Article 42 of the SIS II Regulation.
[756] Emphasis added.
[757] *See* Recital 4 of the SIS II Regulation and the SIS II Decision.

the general field of EU law."[758] This is as from 1st December 2009 a reality, but the problem of divergent data protection rules governing SIS II stills exists and will continue to exist for at least five more years according to Protocol 36 on transitional provisions.[759] The same Protocol limits, in addition, the jurisdiction of the Court of Justice to provide interpretation of former third pillar legislation. Nevertheless, as already discussed in Chapter 4, an extension of the Data Protection Directive in order to apply in the area of police and judicial cooperation is not possible, since this expressly excludes from its scope the processing of data for law enforcement purposes.[760]

So, what is the *lex generalis* for the SIS II Decision? At the time of its adoption, in June 2007, the Data Protection Framework Decision was not into force as it was only adopted in November 2008. Therefore, Article 57 of the Decision envisages the application of the Council of Europe Data Protection Convention as *lex generalis* to the SIS II data protection rules. However, Recital 21 of the Decision explicitly provides that the general rules in the Data Protection Framework Decision, once adopted, will apply to SIS II instead of the Council of Europe rules. It should be concluded, therefore, that the aspect of SIS II that falls in the field of police and judicial cooperation in criminal matters, as soon as it becomes operational, will be governed by the provisions of the Data Protection Framework Decision[761] as its *lex generalis*. SIS II, however, has its own *lex specialis*. The analysis below will assess critically these specific SIS II data protection provisions.

3.5 A Substantive Assessment of the data protection principles of SIS II

i. The purpose limitation principle

The 'purpose limitation principle', which establishes that personal data must be collected for specified, explicit and legitimate purposes and not further processed

[758] Meijers Committee Written submission to House of Lords, House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, at 15.
[759] *See* Steve Peers, *The "Third Pillar Acquis" After the Treaty of Lisbon Enters into Force* (2009).
[760] Article 3 (2) of the Data Protection Directive. For a more detailed analysis *see* Chapter 4.
[761] For a more detailed discussion of the Framework Decision and its problems *see* Chapter 4.

in a way incompatible with those purposes,[762] is a fundamental principle of the EU data protection regime. This is because an individual's informed consent to the collection and processing of his/her personal data is dependent on the information about the purpose and use of those data.[763]

With regard to the storage of personal information to databases, the importance of the purpose limitation principle for safeguarding the transparency and the legality of the use of the data and consequently of the individuals' fundamental rights cannot be overemphasised. Within this context, the principle of purpose limitation prescribes that the scope and purpose of a database should strictly define the group of users who may lawfully access the database and process the data held on it. This principle commands that there be a strict nexus between the purpose of a data collection and the use that can be made of the data.[764]

Article 46 (1) of the SIS II Decision provides that "the Member States may process the data referred to in Articles 20, 26, 32, 34, 36 and 38 only for the purposes laid down for each category of alert referred to in those Articles." Furthermore, access to data will only be authorised "within the limits of the competence" of the designated national authorities and to duly authorised staff.[765] The Decision requires that each Member State will send to the Management Authority a list of its competent authorities which are authorised to search directly the data contained in SIS II. The list must specify, for each authority, which data it may search and for what purposes. The Management Authority will ensure the annual publication of the list in the *Official Journal of the European Union*.[766] Finally, the Decision lays down a number of restrictions on the copying of SIS II data,[767] and establishes that any use of data which does not comply with paragraphs 1 to 6 will be considered "as misuse under the national law of each Member State."[768]

However, a first problematic aspect regarding the purpose limitation principle is found in Article 46 (5). This stipulates that with regard to alerts in respect of

---

[762] Article 6 (1) (b) of the Data Protection Directive.
[763] Joseph Cannataci & Jeanne Pia Bonnici Mifsud, *The End of the Purpose-specification Principle in Data Protection?*, 24 INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 101, 101 (2010).
[764] JUSTICE Report to House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 10.
[765] Article 46 (4) of the SIS II Decision.
[766] Article 46 (8) of the SIS II Decision. See also Article 101 (4) for the arrangement under the Schengen Convention.
[767] Article 46 (2) and (3) of the SIS II Decision.
[768] Article 46 (7) of the SIS II Decision.

persons wanted for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks, the processing of information for further purposes, other than those for which it was entered in SIS II is allowed, where this is

> "linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence."

Prior authorisation from the Member State issuing the alert must be obtained for this purpose. This provision that does not exist neither under the current SIS rules[769] nor in the SIS II Regulation[770] has been probably introduced in the name of fighting terrorism, but it goes against the purpose limitation principle as it is practically impossible for the individual to know which further authorities have gained access to his personal data. What is even more problematic is that paragraph 5 of Article 46 does not describe in a clear and sufficiently precise way the particular conditions which would allow a use of the SIS II data for further purposes. One can recognise that the Decision speaks of a further use of the data in the case of an imminent and serious threat, hence not any threat, however the rest of the conditions set out in paragraph 5 seem to be taking a slippery slope path, starting from a threat to public policy and public security, serious grounds of national security, and going to serious crime, whatever that means for each Member State. Of course, prior authorization of the reporting Member State is required for the further use of the data but again it is not indicated in what circumstances this should be given or denied.[771]

A further problem concerning the purpose limitation principle regards the possibility of interlinking of alerts established in Article 52 of the Decision. Linking alerts means in essence merging purposes; data contained into SIS II with relation to one alert are used for the purposes of other alerts too. It therefore becomes completely impossible for the data subject to foresee the use of his/her data, as SIS II becomes a tool of informational assistance, of investigative support and of executive action all at

---

[769] *See* Article 102 of the Schengen Convention which permits merely a "change from one type of report to another" if this is justified "by the need to prevent an imminent serious threat to public order and safety for serious reasons of State security or for the purposes of preventing a serious offence."
[770] *See* Article 31 of the SIS II Regulation.
[771] *See* House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 94.

the same time.[772] As the European Data Protection Supervisor correctly pointed out in his Opinion on SIS II, interlinking of alerts can have a major impact on the rights of the person concerned,

> "since the person is no longer 'assessed' on the basis of data relating only to him/her, but on the basis of his/her possible association with other persons. Individuals whose data are linked to those of criminals or wanted persons are likely to be treated with more suspicion than others."[773]

ii. The data quality principle

The Schengen Information is a database used for law enforcement purposes. This essentially means that if a 'hit' is found concerning an alert entered into the SIS system, then the law enforcement authorities of a Member State (police, judicial authorities) must take the necessary action prescribed by the relevant alert. It therefore goes without saying that the information contained into SIS II should be accurate, adequate and up-to date (data quality principle)[774] in order to ensure a fair operation of the system. If inaccurate data are stored in SIS II, the risk of unjustifiable decisions being taken by Member States' authorities against individuals that are found in the system only by mistake will increase.

The question therefore of the quality of the SIS II data, besides being of great interest to the Member States, in that the relevant decisions taken on the basis of a SIS II alert are based on mutual trust and mutual cooperation,[775] raises also important data

---

[772] ARTICLE 29 WORKING PARTY, OPINION 6/2005 ON THE PROPOSALS FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (COM (2005) 236 FINAL) AND A COUNCIL DECISION (COM (2005) 230 FINAL) ON THE ESTABLISHMENT, OPERATION AND USE OF THE SECOND GENERATION SCHENGEN INFORMATION SYSTEM (SIS II) AND A PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL REGARDING ACCESS TO THE SECOND GENERATION SCHENGEN INFORMATION SYSTEM (SIS II) BY THE SERVICES IN THE MEMBER STATES RESPONSIBLE FOR ISSUING VEHICLE REGISTRATION CERTIFICATES (COM (2005) 237 FINAL) 16.

[773] Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) COM(2005)230 final); the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005)237 final) 2006/C 91/11, OJ C 91/38 of 19.4.2006, 10.

[774] On the data quality principle *see* Chapters 1 and 2.

[775] In its Report on SIS, JUSTICE noted the complaints of Belgian police regulating entry at external borders and international airports about the difficulties they encountered when trying to judge whether

protection issues.[776] The SIS II Decision envisages that it is the responsibility of the Member State issuing the alert to ensure that the data are accurate, up-to-date and entered in SIS II lawfully.[777] In this respect, only that Member State is authorised to modify, add to, correct, update or delete data which it has entered. The problematic aspect that the Decision does not regulate though seems to be the question of how the accuracy and lawfulness of an entry by a Schengen reporting state is to be safeguarded. Article 7 (2) specifies that the SIRENE Bureaux in each Member State will be responsible for coordinating the verification of the quality of the information entered in SIS II. However, this mere mention of the responsible for data quality national authority does not remedy the situation as the absence of a centralised check of the lawfulness and accuracy of entries makes the system still vulnerable to mistaken or unwarranted data which might have serious consequences on the fundamental rights of individuals.

Another problem is that the information entered into SIS II by a Member State will most probably be used by a different Member State, which will be required to take action as a result of an alert. However, the lack of procedural measures to verify SIS II information before taking action "undermines the system's ability to function lawfully as an instrument for executive action."[778] In an attempt to ensure further the SIS II data quality – or most probably to deepen the mutual trust between the Schengen Member States- the Decision provides that if a Member State other than the reporting one has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it can, through the exchange of supplementary information, inform the reporting Member State at the earliest opportunity and in any case not later than 10 days after the said evidence has come to its attention. In this case, the Member State that issued the alert must check the communication and, if necessary, correct or delete the item in question without delay.[779] If the Member States are unable to reach agreement within two months, the Decision provides that the Member State that

---

a person seeking entry matched a person "of the same or similar name and year on the SIS, as entered by another Schengen state." *See* JUSTICE, *supra* note 640, at 37.

[776] Not to mention other fundamental rights issues, for instance due-process questions. As JUSTICE pointed out in its Report concerning the SIS (above n 38, 37), in cases where only names appear in the system "there is an obvious temptation for border guards to err on the side of safety, even when the details do not exactly match the applicants for entry, and to reject individuals to avoid being blamed for wrongly admitting them." *Id.*

[777] Article 49 (1) of the SIS II Decision.

[778] Garside, *supra* note 689, at 4.

[779] Article 49 (3) of the SIS II Decision.

suggested the inaccuracy of the alert must submit the matter to the European Data Protection Supervisor who, jointly with the national supervisory authorities concerned, will act as mediator.[780] This procedure, however, it seems to have more as its principal aim to settle down possible cases of distrust between Member States, rather than to take into account possible infringements to individuals' fundamental rights. In a situation that a person complains that he is not the person wanted by an alert, the Decision simply foresees that the Member States must exchange supplementary information. If the outcome of the check is that there are in fact two different persons then the complainant must be informed accordingly.[781]

iii. Individual rights and remedies

a. The right of information

As pointed out above, the right of information, namely the right of the data subject to be informed that an alert on him or her exists and thus his/her data is being held in SIS II is not provided for at all in the SIS II Decision. This right is enshrined in the SIS II Regulation, which stipulates in Article 42 that third-country nationals who are the subject of an alert must be informed in accordance with Articles 10 and 11 of the Data Protection Directive. This information must be provided in writing, together with a copy of or a reference to the national decision giving rise to the alert. However, even in the Regulation the right of information is made subject to extensive exemptions and limitations.[782]

The absence of a right to information from the SIS II Decision is problematic because the data held on SIS II that fall under the Decision are probably of more

[780] Article 49 (4) of the SIS II Decision. Under the Schengen Convention Article 106 (3) provides that such disputes are to be submitted to the Joint Supervisory Authority for an opinion. It should be noted here that the original proposal for SIS II provided only for an optional referral to the EDPS.
[781] Article 49 (5) of the SIS II Decision.
[782] See Article 42 (2) of the immigration Regulation which provides that the right to information 'shall not be provided: (a) where (i) the personal data have not been obtained from the third-country national in question; and (ii) the provision of the information proves impossible or would involve a disproportionate effort; (b) where the third country national in question already has the information; (c) where national law allows for the right of information to be restricted, in particular in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences'.

sensitive nature than immigration data, since they refer in essence to alerts for surrender or extradition purposes or for the placement under surveillance and specific checks, for missing persons etc. Furthermore, the absence of a right to information in the Decision renders also meaningless the exercise of other rights of the data subject such as the right of correction or deletion of unlawfully stored data. Those rights cannot be effectively exercised unless the right of information is first granted. An individual cannot even be aware that he has an interest in exercising a right of access unless he knows that his personal data is held on SIS II and knows of the consequences of this, pursuant to the right to information.[783]

The SIS II *lex specialis* may be silent on a right to information, but what happens with the *lex specialis*, i.e. the Data Protection Framework Decision? This indeed stipulates in Article 16 that Member States must ensure that the data subject is informed regarding the collection or processing of personal data by their competent authorities, in accordance with national law. Can this provision be applied in order to remedy the absence of such a right in the SIS II Decision? In my view, the answer is probably to the negative, because the non existence of an information right in the SIS II Decision reflects the choice of the EU legislator, who nevertheless decided to provide for such a right in the immigration Regulation. Therefore, it seems that in the present case the *lex generalis* cannot be used to correct the deficiencies of the *lex specialis*, thus eventually depriving the individuals of an absolutely fundamental right if one takes into account the vast amounts of data held in the SIS II.

b. The right of access

Article 58 of the SIS II Decision lays down the right of access, correction of inaccurate data and deletion of unlawfully stored data. The exercise of this right, however, must be in accordance with the law of the Member State before which it is invoked.[784] This qualification seems already to be undermining the right of access,

[783] House of Lords Report, above n 52, para 113.
[784] Article 58 (1) of the SIS II Decision.

since it leaves too much discretion to the Member States to decide how they will regulate it.[785]

Furthermore, the right to access is made subject to exceptions. In particular, it must be refused to the data subject "if this is indispensable for the performance of a lawful task in connection with an alert or for the protection of the rights and freedoms of third parties."[786] While denial of access to information is understood on the grounds of the protection of the rights and freedoms of others; the first proviso appears unduly broad since, in principle, information stored in SIS II would almost always be indispensable for the performance of any lawful task of Member States' law enforcement authorities. The fact that the provisions do not distinguish between lawful tasks of law enforcement agencies of different importance is very problematic, because this could cover in essence every possible task of the law enforcement agencies. JUSTICE in its Memorandum to the House of Lords European Union Select Committee proposes that

> "a balancing requirement obliging Member States to weigh the infringement of the data subject's right of access to the SIS data against the likely effects of access to data on the criminal justice system and crime detection and investigation' should be established."[787]

I do not agree. A balancing test seems rather unsure and uncertain to determine whether the individual will be granted access to his data, especially if one takes into account that it will be the law enforcement authorities of each Member State that will be carrying out this balancing task. I would find preferable a harmonised solution that restricts the right to access only, for instance, in the specific cases provided for by the Data Protection Framework Decision, namely where such a restriction, with due regard for the legitimate interests of the person concerned, constitutes a necessary and proportional measure: a) to avoid obstructing official or legal inquiries, investigations or procedures; b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties; c) to protect public security; and d) to protect national security.[788] These criteria are also very broad, but at least still more specific than the "indispensable for the performance

[785] *See* JUSTICE, Report to House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 57.
[786] Article 58 (4) of the SIS II Decision.
[787] JUSTICE, Report to House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 59.
[788] See Article 15 (2) of the Data Protection Framework Decision.

of a lawful task" or an *ad hoc* balancing exercise. In any case, the principle of proportionality should play a central role and in this respect a denial of access to the SIS II data should be deemed disproportionate where the police or law enforcement authorities in general are performing a lawful, albeit insignificant, task even if only a denial of access to the SIS II data would ensure that that task was fulfilled.[789]

c. Remedies

Article 59 of the Decision provides that any person can bring an action before the courts or the authority competent under the law of any Member State to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him. The Member States undertake mutually to enforce the final decisions handed down in these cases.

iv. Supervision: EDPS and National Supervisory Authorities

The SIS II Decision provides for a system of data protection supervision which distinguishes between national supervision of the N.SIS II by the national supervisory authorities and supervision of the Management Authority by the EDPS, each acting within the scope of its respective competences. In particular, Article 60 envisages that each Member State must ensure that an independent authority (the national supervisory authority) monitors independently the lawfulness of the processing of SIS II personal data on their territory and its transmission from their territory, and the exchange and further processing of supplementary information via the SIRENE system. The EDPS will perform the same function for the Management Authority;[790] during the transitional period where the Commission will delegate its responsibilities, it must ensure that the EDPS can fully exercise his tasks in respect of national public-sector bodies.[791] According to Article 62, the EDPS and the national supervisory

[789] JUSTICE, Report to House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 59.
[790] Article 61 of the SIS II Decision.
[791] Article 63 of the SIS II Decision.

authorities must cooperate actively in the framework of their responsibilities and must ensure coordinated supervision of SIS II.[792]

The Decision does not set out the exact powers of the national data protection authorities, but refers vaguely only to a monitoring power. Does this mean that national supervisory authorities will have solely this power? Under the Schengen Convention national supervisory authorities have the power to inspect or access data in the national section of SIS, but it not clear from the Decision whether this will be the also the case with regards to SIS II. The same concerns apply also with relation to the powers of the EDPS that does not seem to enjoy full supervisory powers.

4. The VISA Information System (VIS)

4.1 Legal framework

4.1.1 Background

Unlike SIS and SIS II, the Visa Information System database (VIS) has no obvious connection with the EU's counter-terrorism strategy as it is an EU-large database created to support the common visa policy. Ironically enough, however, as an author points out, the decision to establish the Visa Information System was "a

[792] In particular Article 62 of the SIS II Decision provides that: "'2. They shall, each acting within the scope of its respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Decision, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.
3. The national supervisory authorities and the European Data Protection Supervisor shall meet for that purpose at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Management Authority every two years."

direct consequence of the terrorist attacks of 11 September."[793] Already since the extraordinary JHA Council meeting on 20 September 2001, the Home Affairs and Justice Ministers agreed that the application procedures for the issue of visas[794] should be dealt with maximum rigour and called upon the Commission to make proposals for the establishment of a network for information exchanges concerning visas issued by the Member States.[795] The Seville European Council of 21- 22 June 2002 considered the establishment of a common identification system for visa data as a "top priority."[796] In its Conclusions of 20 February 2004 on the development of the VIS, the Council noted that, among other purposes, the database would aim to contribute towards improving internal security and combating terrorism.[797]

The Council Decision establishing a system of exchange of visa data between Member States, 'the Visa Information System' was adopted on 8 June 2004 on the basis of Article 66 EC.[798] The Decision gives the Commission the mandate to develop the VIS and constitutes the required legal basis to allow for the inclusion of the necessary appropriations for its development through EC financing.[799] According to the Decision, the Visa Information System will be based on a centralised architecture and consist of a central information system, 'the Central Visa Information System' (CS-VIS), an interface in each Member State, 'the National Interface' (NI-VIS) which will provide the connection to the relevant central national authority of the respective Member State, and the communication infrastructure between the Central Visa

---

[793] Anneliese Baldaccini, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, 10 EUROPEAN JOURNAL OF MIGRATION AND LAW 31, 39 (2008).

[794] Article 5 of Council Regulation 2317/95 defines 'visa' as "authorization given by or a decision taken by a Member State which is required for entry into its territory with a view to: an intended stay in that
Member State or in several Member States of no more than three months in all; transit through the territory or the airport transit zone of that member state or several Member States." *See* Council Regulation (EC) No 2317/95 of 25 September 1995 determining the third countries whose nationals must be in possession of visas when crossing the external borders of the Member States OJ L 234/1 of 3.10.1995.

[795] Extraordinary Council Meeting of 20 September 2001, Justice, Home Affairs and Civil Protection, Doc. 12019/01 (Presse 327), para. 26.

[796] Presidency Conclusions Seville European Council 21 and 22 June 2002, DOC/02/13.

[797] Council Conclusions on the development of the Visa Information System (VIS), Doc. 6535/04, 20 February 2004.

[798] Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213/5 of 15.6.2004.

[799] The Decision follows the Conclusions of the European Council of 19-20 June 2003 in Thessaloniki, which deemed it necessary that orientations should be determined with regard to the planning for the development of the VIS, together with the appropriate legal basis permitting its establishment and the engagement of the necessary financial means. *See* Thessaloniki European Council, 19-20 June 2003: Presidency Conclusions and Recital 3 of Council Decision 2004/512/EC.

Information System and the National Interfaces.[800] The Central VIS, the National Interface in each Member State, and the communication infrastructure between the Central VIS and the National Interfaces are to be developed by the Commission, while the national infrastructures are to be adapted and developed by the Member States.[801] The system will be designed to provide for the connection of at least 12,000 users in 27 Member States and at 3,500 consular posts.[802]

Citizens from 134 countries require visas to enter the EU. This means that it had been possible for an applicant rejected by one country's consulate to continue applying to other consulates. Once the VIS is in place this will not be possible. Information on previous applications and reasons for rejection will be available through the new system. The inclusion of fingerprint data is intended to allow the exact verification of somebody's identity.

The VIS was due to become operational by spring 2009. On 24 June 2009, following the request of the Council and the European Parliament, the Commission introduced a legislative package proposing the setting up of an Agency for the long-term operational management of the SIS II, VIS, EURODAC and other large-scale IT systems in the area of freedom, security and justice. According to the proposals, the core mission of the Agency would be to fulfil the operational management tasks for SIS II, VIS and EURODAC, keeping the systems functioning 24 hours a day, seven days a week. In addition to these operational activities, the Agency will also be responsible for adopting the necessary security measures, reporting, publishing statistics, monitoring of research, SIS II and VIS related training and information issues. It will ensure data security and integrity as well as compliance with data protection rules.

4.1.2 The VIS Regulation

In order to implement the Decision, a Regulation (the 'VIS Regulation') defining the purpose, the functionalities and the responsibilities of the information

[800] Article 1 (2) of the VIS Decision.
[801] Article 2 of the VIS Decision.
[802] Communication from the Commission to the Council and the European Parliament – Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS), COM(2003) 771 final, 11 December 2003, p. 26.

system, and establishing the procedures and conditions for the exchange of data between Member States on short-stay visa applications was adopted on 9 July 2008.[803] According to the Regulation, the purpose of the VIS is to improve the implementation of the common visa policy, consular cooperation and consultation between the central visa authorities by:

- facilitating the visa application procedure;
- preventing 'visa shopping';
- facilitating the fight against fraud;
- facilitating checks at external border crossing points and in the territories of the Member States;
- assisting in the identification of persons that do not meet the requirements for entering, staying or residing in a Member State;
- facilitating the application of the Dublin II Regulation for determining the Member State that is responsible for the examination of a third-country national's asylum application and for examining said application; and
- contributing to the *prevention of threats* to Member States' *internal security*.[804]

The data to be recorded in the VIS include not only alphanumeric data (on the applicant and on the visas requested, issued, refused, annulled, revoked or extended), but also biometric identifiers such as photographs and applicants' fingerprint data. Links to previous visa applications and to the application files of persons travelling together are also included in the VIS.[805]

Access to the VIS for entering, amending or deleting data, will be reserved exclusively to duly authorised staff of the visa authorities; while access for consulting data, will be reserved to visa authorities and authorities competent for checks at the external border crossing points, immigration checks and asylum, and will be limited to the extent the data is required for the performance of their tasks.[806] The Regulation stipulates that each Member State must communicate to the Commission a list of the competent authorities whose staff are authorised to enter, amend, delete or consult

[803] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218/60 of 13.8.2008.
[804] Article 2 of the VIS Regulation (emphasis added). *See* also Valsamis Mitsilegas, *Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance*, WHOSE FREEDOM SECURITY AND JUSTICE? EU IMMIGRATION AND ASYLUM LAW AND POLICY 359, 391 (Elspeth Guild et al., 2007).
[805] Article 5 of the VIS Regulation.
[806] Article 3 of the VIS Regulation.

data in the VIS, along with the details of the central authority designated as responsible for the processing of that data. The Commission will annually publish an updated consolidated list of these authorities, where there are amendments thereto.[807] The Regulation lays down the purpose limitation and proportionality principles, according to which, the authorities with access to VIS must ensure that its use is limited to that which is necessary, appropriate and proportionate for carrying out their tasks.[808] Furthermore, they must ensure that in using VIS, the visa applicants and holders are not discriminated and that their human dignity and integrity are respected.[809]

The Regulation provides that competent visa authorities will consult the VIS for the purpose of examining applications and decisions to issue, refuse, extend, annul or revoke a visa, or to shorten a visa's validity period.[810] They are authorised to carry out searches using the application number, surname, surname at birth, first names, sex, date, place and country of birth, information on the travel document, name and address of the person issuing an invitation or liable to pay living costs during the stay, fingerprints, number of the visa sticker and dates of issuance of previous visas. If the search using any of the above data indicates that data on the applicant is recorded in the VIS, the visa authority will be given access to the application file and linked application files.[811]

According to the Regulation, for the sole purpose of verifying the identity of the person, the authenticity of the visa and/or whether the person meets the requirements for entry, stay or residence in a Member State, the competent authorities will have access to search with fingerprint data.[812] If that person's fingerprints cannot be used or the search with the fingerprints fails, the relevant authorities may search the VIS with the name, sex, date and place of birth and/or information taken from the travel document. These may be used in combination with the nationality of the person.[813]

[807] Article 6 of the VIS Regulation.
[808] Article 7 (1) of the VIS Regulation.
[809] Article 7 (2) of the VIS Regulation.
[810] Article 4 (3) of the VIS Regulation.
[811] Article 15 of the VIS Regulation.
[812] Article 18 of the VIS Regulation.
[813] Article 19 of the VIS Regulation.

The Regulation stipulates that each application file will be stored in the VIS for a maximum of five years. Only the Member State responsible will have the right to amend or delete data it has transmitted to the VIS.[814]

Concerning the operational issues, the Regulation provides, as in the case of SIS II, that after a transitional period, during which the Commission will be in charge, the Management Authority will be responsible for the operational management of the Central VIS and the national interfaces. In addition, the Management Authority will be in charge of the supervision, security and the coordination of relations between Member States and the service provider.[815] The Central VIS will be located in Strasbourg, France, and the back-up Central VIS in Sankt Johann im Pongau, Austria. The VIS will be connected to the national system of each Member State via the national interface in the Member State concerned.

Data stored in the VIS are not to be communicated to third countries or international organisations unless indispensable for attesting a third-country national's identity in individual cases. The communication may be made when a set of conditions are met, with due respect to the rights of refugees and persons requesting international protection.[816]

Article 3 of the VIS Regulation provides access to VIS data for the prevention, detection and investigation of terrorist and other serious criminal offences. According to this provision, the designated authorities of the Member States may in a specific case and following a reasoned written or electronic request access the data kept in the VIS if there are reasonable grounds to consider that their consultation "will substantially contribute to the prevention, detection or investigation of terrorist

[814] Article 23 of the VIS Regulation
[815] Article 26 of the VIS Regulation.
[816] Article 30 of the VIS Regulation. Article 30 (2) and (3) stipulate that: " By way of derogation…, the data …may be transferred or made available to a third country or to an international organisation … if necessary in individual cases for the purpose of proving the identity of third-country nationals, including for the purpose of return, only where the following conditions are satisfied:
(a) the Commission has adopted a decision on the adequate protection of personal data in that third country in accordance with Article 25(6) of Directive 95/46/EC, or a readmission agreement is in force between the Community and that third country, or the provisions of Article 26(1)(d) of Directive 95/46/EC apply; (b) the third country or international organisation agrees to use the data only for the purpose for which they were provided; (c) the data are transferred or made available in accordance with the relevant provisions of Community law, in particular readmission agreements, and the national law of the Member State which transferred or made the data available, including the legal provisions relevant to data security and data protection; and (d) the Member State(s) which entered the data in the VIS has given its consent.
3. Such transfers of personal data to third countries or international organisations shall not prejudice the rights of refugees and persons requesting international protection, in particular as regards non-refoulement."

offences and of other serious criminal offences." Also, Europol may access the VIS within the limits of its mandate and when necessary for the performance of its tasks. Data obtained from the VIS cannot be transferred or made available to a third country or to an international organisation.[817] However, in an exceptional case of urgency, such data may be transferred or made available to a third country or an international organisation exclusively for the purposes of the prevention and detection of terrorist offences and of other serious criminal offences and under the conditions set out in that Decision.[818]

4.1.3 The VIS Regulation data protection rules

The data protection regime of the VIS Regulation has many similarities with the SIS II one, however, the Regulation provides in many respects for a higher level of protection. This combined with the fact that the *lex generalis* of the VIS Regulation is the Data Protection Directive, since the Regulation falls under the former first pillar in the pre-Lisbon era, leads to the (preliminary) conclusion that the rights of the data subjects are adequately protected in the VIS Regulation.

The VIS Regulation provides for both a right to information and a right of access to data for the data subjects. Insofar as the right to information is concerned, the Regulation requires that the responsible Member State will provide the persons concerned with information on the identity and contact details of the controller responsible for the processing of the data, the purposes for which the data will be processed within the VIS, the categories of the recipients of the data, the period of retention of the data and the right to access, correct and delete the data, and that the collection of the data is mandatory for the examination of the application.[819]

Insofar as the right of access is concerned, the Regulation stipulates that any person must be entitled to: obtain communication of the data relating to him/her recorded in the VIS and of the Member State that transmitted it to the VIS; and, request that inaccurate data relating to him/her be corrected or that unlawfully

[817] Article 3 (3) of the VIS Regulation.
[818] *Id.*
[819] Article 37 of the VIS Regulation.

recorded data be deleted.[820] The data subject may bring an action or a complaint before the competent courts of that Member State if he/she is refused the right of access to, or the right of correction or deletion of, data relating to him/her.[821]

As in the case of SIS II, the Regulation shares out the supervisory task between national supervisory authorities and the EDPS. National Supervisory Authority will monitor the lawfulness of the processing of personal data by Member States,[822] the European Data Protection Supervisor will be responsible for the monitoring of the activities of the Management Authority.[823] The EDPS and the national supervisory authorities are to cooperate actively, in particular to coordinate the management of the VIS and the national interfaces.[824]

Some of the criticisms raised with regard to the data protection regime of the SIS II, in particular those concerning the exact scope of the supervision, both by the national supervisory authorities and the EDPS, apply here as well. However, the fact that the Data Protection Directive is the *lex generalis* in the present case, raises hopes that some of the deficiencies identified in the VIS data protection regime will be remedied by the application of the Directive.

4.2 Access to VIS for law enforcement purposes. A 'function creep'?

4.2.1 The VIS Council Decision

i. Background

As seen above, apart from improving the implementation of the common visa policy, one of the purposes of VIS was also to contribute towards internal security and to combating terrorism. In its meeting of 7 March 2005 the Council stated that "in order to achieve fully the aim of improving internal security and the fight against

[820] Article 38 of the VIS Regulation.
[821] Article 40 of the VIS Regulation.
[822] Article 41 of the VIS Regulation.
[823] Article 42 of the VIS Regulation.
[824] Article 43 of the VIS Regulation.

terrorism," Member State authorities responsible for internal security should be guaranteed access to the VIS, "in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats."[825]

On 23 June 2008 the Council adopted a Decision allowing the access for consultation of the Visa Information System by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.[826] The Decision was adopted on the basis that

> "it is essential in the fight against terrorism and other serious crimes for the relevant services to have the fullest and most up-to-date information in their respective fields in order to perform their tasks. The Member States' competent national services need information if they are to perform their tasks. The information contained in the VIS *may be necessary* for the purposes of preventing and combating terrorism and serious crimes and should therefore be available for consultation' by the designated authorities,"[827] and "by Europol that has a key role in the field of cross-border crime investigation and in supporting Union-wide crime prevention, analyses and investigation."[828]

This justification provided in the Decision for a measure that has serious implications on fundamental rights can be characterised, at best, as extremely weak.[829] That the information contained in the VIS "may be necessary" for counter-terrorism does not justify by no means granting access to VIS for law enforcement purposes. In this respect, it is very regrettable that there was no impact assessment study concerning access to VIS by law enforcement authorities. As the EDPS rightly pointed out in his Opinion on the VIS Decision,[830]

---

[825] Council of the European Union, Conclusions meeting Council Competitiveness 7 March 2005, doc. 6811/05.
[826] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218/129 of 13.8.2008.
[827] *See* Recital 3 of the VIS Decision (emphasis added).
[828] *See* Recital 4 of the VIS Decision.
[829] Tzanou, *The EU as an Emerging "Surveillance Society": The Function Creep Case Study and Challenges to Privacy and Data Protection*, *supra* note 467, at 419.
[830] Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and

> "such a significant change of the system could invalidate the results of the impact assessment study (which addressed the use of the system for the original purpose only)."[831]

Furthermore, granting access to former first pillar databases to law enforcement agencies, however justified one accepts that it may be for the purpose of fighting terrorism, has significant consequences. The VIS is an information system developed in view of the application of the European visa policy and not as a law enforcement tool,[832] therefore a study assessing the necessity and proportionality of such a measure for the purpose of fighting terrorism was indispensable.

ii. Access to VIS

The Decision provides that VIS will be accessed by designated authorities of the Member States. For this purpose, every Member State must keep a list of the designated authorities and notify them to the Commission and the General Secretariat of the Council. The Commission will publish these declarations in the *Official Journal of the European Union*.[833] Access to the VIS for consultation can be exercised also by authorities responsible for internal security from Member States which are not part of the VIS.[834]

Access to VIS data is limited for the specific purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA on the European arrest warrant. The Decision stipulates that

> "it is essential to ensure that the duly empowered staff with a right to access the VIS is limited to those who 'have a need to know' and possess appropriate knowledge about data security and data protection rules."[835]

---

investigation of terrorist offences and of other serious criminal offences (COM (2005) 600 final) (2006/C 97/03), OJ C 97/6 of 25.4.2006.

[831] Opinion of the EDPS on the VIS Decision, above n 216, 2.

[832] Baldaccini, *supra* note 793, at 41.

[833] Article 3 of the VIS Decision.

[834] Article 6 of the VIS Decision. The VIS Regulation does not apply to the United Kingdom and Ireland. Denmark has decided to implement it.

[835] Recital 6 of the VIS Decision.

iii. Conditions for access to VIS

Article 5 of the Decision lays down clearly the conditions for the access to VIS data. In order to exclude routine access, this provision allows for the processing of VIS data only on a case-by-case basis. Such a specific case exists in particular when the access for consultation is connected to a specific event or to a danger associated with serious crime, or to a specific person in respect of whom there are serious grounds for believing that he will commit or has committed terrorist offences or other serious criminal offences or he has a relevant connection with such a person. In this regard, the designated Member States' authorities and Europol may search the data contained in the VIS when they have reasonable grounds to believe that such a search will provide information that will substantially assist them in preventing, detecting or investigating serious crime.[836]

Consultation of the VIS means searching any of the following VIS data in the application file: (a) surname, surname at birth (former surname(s)); first name(s); sex; date, place and country of birth; (b) current nationality and nationality at birth; (c) type and number of the travel document, the authority which issued it and the date of issue and of expiry; (d) main destination and duration of the intended stay; (e) purpose of travel; (f) intended date of arrival and departure; (g) intended border of first entry or transit route; (h) residence; (i) fingerprints; (j) type of visa and the number of the visa sticker; (k) details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay.[837]

In the event of a hit consultation of the VIS will give access, in addition to the data referred above, also to: (a) any other data taken from the application form; (b) photographs; (c) the data entered in respect of any visa issued, refused, annulled, revoked or extended.[838]

Access to VIS data by Europol is also circumscribed by strict conditions. In particular, Europol is granted access within the limits of its mandate and when necessary for the performance of its tasks. For an analysis of a general nature and of a strategic type,[839] Europol must render anonymous the VIS data prior to processing and retain them in a form in which identification of the data subjects is no longer possible. Finally, processing of information obtained by Europol from access to the VIS must

[836] Article 5 of the VIS Decision. *See* also Recital 8.
[837] Article 5 (2) of the VIS Decision.
[838] Article 5 (3) of the VIS Decision
[839] See Article 10 of the Europol Convention.

be subject to the consent of the Member State which has entered that data in the VIS.[840]

iv. Data protection rules

Article 8 in connection with Recital 9 of the VIS Decision specifies that the Data Protection Framework Decision applies as *lex generalis* alongside the specific data protection regime of the VIS Decision.[841]

With regard to Europol, the Decision provides that the processing of personal data by it must be in accordance with the Europol Convention and the rules adopted in implementation thereof and supervised by the independent joint supervisory body established by Article 24 of the Convention.

It then sets out the purpose limitation principle, according to which personal data obtained from the VIS must "only be processed for the purposes of the prevention, detection, investigation and prosecution of terrorist offences or other serious criminal offences."[842]

Moreover, the Decision states that personal data obtained from the VIS must not be transferred or made available to a third country or to an international organisation. However, this is subject to exceptions. In particular, in an exceptional case of urgency such data may be transferred or made available to a third country or an international organisation, "exclusively for the purposes of the prevention and detection of terrorist offences and of other serious criminal offences and subject to the consent of the Member State that entered the data into the VIS and in accordance with the national law of the Member State transferring the data or making them available."[843]

[840] Article 7 of the VIS Decision.
[841] Recital 9 of the VIS Decision provides that: "once the proposed Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters has entered into force it should apply to the personal data which are processed pursuant to this Decision."
[842] Article 8 (3) of the VIS Decision.
[843] Article 8 (4) of the VIS Decision.

The national supervisory authorities of the Member States are entrusted with the task of monitoring the lawfulness of the processing of personal data by the designated authorities.[844]

Finally, the Decision requires that before being authorised to process data stored in the VIS, the staff of the authorities having a right to access the VIS receive appropriate training about data security and data protection rules and be informed of any relevant criminal offences and penalties.[845]

4.2.2 Access to VIS data for law enforcement purposes and data protection

It is true that the VIS Decision attempts to circumscribe with a number of data protection safeguards the access to VIS data by law enforcement authorities. However, this measure is still very problematic from the point of view of the right to personal data protection. The concerns about the access to the system by Europol, raised with regard to SIS II, apply here as well, maybe with even greater magnitude.

The keystone purpose limitation principle is, once again in the present case, undermined. This time the problem seems even more serious: law enforcement authorities are granted access to databases that have no law enforcement purposes whatsoever. The Visa Information System database cannot function by its nature as a "multifunctional tool." This database is very different from SIS which pursues also law enforcement purposes, and includes alerts upon which certain executive action should be adopted. On the contrary, VIS was designed to be used only for the implementation of EU visa policy, and not for the fight against terrorism. Once the purposes of a large-scale information system, where huge amounts of data are stored are not clearly and restrictively defined, then the system is opened up for any possible purpose. It goes without saying that this 'function' or 'competence creep', where personal data collected for one specific purpose and in order to fulfil one function, are used for completely different purposes, which are totally unrelated to the ones for which they were initially collected constitutes a breach to the purpose limitation principle.

[844] Article 8 (6) of the VIS Decision.
[845] Article 8 (8) of the VIS Decision.

The need for law enforcement authorities to benefit from the best possible tools to identify the perpetrators of terrorist acts or other serious crime cannot be disregarded. Furthermore, it should be acknowledged that the Decision granting access to VIS for law enforcement purposes sets out a number of data protection safeguards and in particular envisages only access on a case-by-case basis and not routinely. However, it is submitted that the adoption of the VIS Decision itself violates the purpose limitation principle. Granting access to VIS in order to combat terrorism and serious crime is not a purpose that travellers who agreed to their data being processed in order to obtain a visa can foresee. What is more, since information systems are built for a specific purpose, with safeguards, security, conditions for access determined by this purpose, granting access for a purpose different from the original one would not only infringe the principle of purpose limitation, but could also render the above mentioned elements inadequate or insufficient.[846] It is very questionable, therefore, to what extent measures that introduce exceptions to the purpose limitation principle, such as the VIS Decision which allows law enforcement authorities and Europol access and use of the VIS data for other purposes than for which these data were collected and processed, can be adopted in the context of the fight against terrorism.

Finally, granting access to visa data for law enforcement purposes implies that third-country nationals are placed under a general suspicion[847] of being potential terrorists or criminal offenders.[848] In this respect, it should be recalled that the ECJ in *Huber* held in relation to the centralised database operated by the German authorities and containing information on non-German citizens that:

> "the fight against crime… necessarily involves the prosecution of crimes and offences committed, *irrespective of the nationality* of their perpetrators. It follows that, as regards a Member State, the situation of its nationals cannot, as regards the objective of fighting crime, be different from that of Union citizens

[846] *See* in this respect Opinion of the EDPS on the VIS Decision, above n 214, at 4.
[847] *See* Ryszard Cholewinski, *The Criminalisation of Migration in EU Law and Policy*, WHOSE FREEDOM SECURITY AND JUSTICE? EU IMMIGRATION AND ASYLUM LAW AND POLICY 301 (Anneliese Baldaccini et al., 2007).
[848] *See* TERRORISM AND THE FOREIGNER : A DECADE OF TENSION AROUND THE RULE OF LAW IN EUROPE (Elspeth Guild & Anneliese Baldaccini, 2007); Valsamis Mitsilegas, *Contrôle Des Étrangers, Des Passagers, Des Citoyens : Surveillance Et Anti-terrorisme*, 58 CULTURES ET CONFLITS 155 (2005).

who are not nationals of that Member State and who are resident in its territory."[849]

The VIS database, by its nature, concerns primarily non-EU citizens, as it will store the data of visa applicants. The fight against terrorism and crime, however, as the ECJ has emphasised in *Huber*, cannot be carried out on the basis of distinctions between EU and non-EU citizens.

5. EURODAC

5.1 Legal framework

EURODAC, which stands for *European Dactyloscopie*, is the European fingerprint database for identifying asylum seekers and irregular border-crossers established by Council Regulation 2725/2000 of 11 December 2000.[850] The objective of the creation of the EURODAC system was to facilitate the application of the Dublin Regulation[851] (before Dublin Convention),[852] which makes it possible to determine the Member State responsible for examining an asylum application, by comparing the fingerprints of asylum seekers and illegal immigrants.[853] EURODAC, which became operational on 15 January 2003, enables Member States to identify asylum applicants and persons who have been apprehended while unlawfully crossing

[849] Case C-524/06 *Huber v Bundesrepublic Deutschland*, paras 78-79. *See* GLORIA GONZÁLEZ FUSTER ET AL., HUBER, MARPER AND OTHERS: THROWING NEW LIGHT ON THE SHADOWS OF SUSPICION 2 (INEX Policy Brief, No. 11, June 2010); D. Martin, *Comments on Förster (Case C-158/07 of 18 November 2008), Metock (Case C-127/08 of 25 July 2008) and Huber (Case C-524/06 of 16 December 2008)*, 11 EUROPEAN JOURNAL OF MIGRATION AND LAW 95 (2009). *See* also Chapter 4.

[850] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316/1 of 15.12.2000.

[851] Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national OJ L 50/1 of 25.2.2003.

[852] Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities OJ C 254/1 of 19.8.1997. The Convention was signed in Dublin on 15 June 1990.

[853] Article 1 (1) of the EURODAC Regulation.

an external frontier of the Community.[854] The system is based on the assumption that asylum seekers must apply for asylum in the first EU country in which they arrive and may be returned to another Member State if it can be proven that they have either passed through the border of another Member State or already lodged an application for asylum in that Member State. Thus, by comparing fingerprints, Member States can determine whether an asylum applicant or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State, or whether an asylum applicant entered the Union territory unlawfully.[855] EURODAC stores fingerprints of every applicant for asylum and of every alien who is apprehended in connection with the irregular crossing of an external border of a Member State, over the age of 14 years old.[856]

EURODAC is a database aimed to support the implementation of the common asylum policy by preventing "asylum shopping."[857] In particular, the computerised system allows for the identification of third-country nationals who may have already lodged asylum applications in the EU and whose data were already enrolled by one Member State, and thus when a Member State receives a hit reply, proving that an asylum seeker has applied for asylum before in another Member State, it will request the other Member State to take back the asylum applicant.

The EURODAC system consists of: a) the Central Unit equipped with a computerised fingerprint recognition system; b) a computerised central database in which the EURODAC data are processed for the purpose of comparing the fingerprint data of applicants for asylum and of illegal immigrants; and c) means of data transmission between the Member States and the central database.[858]

---

[854] Evelien Brouwer, *Eurodac: Its Limitations and Temptations*, 4 EUROPEAN JOURNAL OF MIGRATION AND LAW 231 (2002).
[855] *See* JONATHAN AUS, SUPRANATIONAL GOVERNANCE IN AN "AREA OF FREEDOM, SECURITY AND JUSTICE": EURODAC AND THE POLITICS OF BIOMETRIC CONTROL (Sussex European Institute Working Paper No 72, 2003).
[856] Article 4 and Article 8 of the EURODAC Regulation.
[857] *See* Recital 3 of the EURODAC Regulation. *See* also BROUWER, DIGITAL BORDERS AND REAL RIGHTS, *supra* note 269, at 118.
[858] Article 3 of the EURODAC Regulation.

5.2 EURODAC and counter-terrorism: Access to EURODAC for law enforcement purposes?

5.2.1 The proposal for a Council Decision on access to EURODAC for law enforcement purposes

i. Background

Following the general trend, started with VIS, the Member States have agreed that EURODAC should also be made accessible for law enforcement purposes in order to fight terrorism. A commitment to this effect had been made by the Interior Minister of the EU's six largest Member States at their G6 meeting in Heiligendamm, Germany, on 22-23 March 2006.[859] Furthermore, the 18-months Presidency Programme on Police and Customs Cooperation of 2007 stated:

> "[f]requently, asylum-seekers and foreigners who are staying in the EU unlawfully are involved in the preparation of terrorist crimes, as was shown not least in the investigations of suspects in the Madrid bombings and those of terrorist organisations in Germany and other Member States (for instance, two of the five accused in German proceedings against the terrorist group "Al Tawhid", which prepared attacks against Jewish institutions in Berlin and Düsseldorf, were asylum-seekers.) Since January 2003, the fingerprints of asylum-seekers and persons who have entered the EU illegally have been stored in EURODAC. The police and law enforcement authorities therefore need greater access to EURODAC, because in many cases this is the only way of identifying suspected offenders or of detecting aliases of suspects. Access to EURODAC can help provide the police and law enforcement authorities of the Member States with new investigative leads making an essential contribution to preventing or clearing up crimes."[860]

---

[859] *See* HOUSE OF LORDS EUROPEAN UNION COMMITTEE, BEHIND CLOSED DOORS: THE MEETING OF THE G6 INTERIOR MINISTERS AT HEILIGENDAMM (40th Report of Session 2005–06).

[860] Council of the European Union, Common 18-months Presidency Programme on Police and Customs Co-operation, Council Doc. 5291/07, 12 January 2007, 6. *See* also Elspeth Guild, *International Terrorism and EU Immigration, Asylum and Borders Policy: The Unexpected Victims of 11 September 2001*, 8 EUROPEAN FOREIGN AFFAIRS REVIEW 331 (2003).

Along the same lines, the Council held on 25 May 2007 that, in order to fully achieve the aim of improving security and to enhance the fight against terrorism, access under certain conditions to EURODAC should be granted to Member States' police and law enforcement authorities, as well as Europol.[861] The Ministers therefore invited the Commission to present "as soon as possible" an amendment to the EURODAC Regulation in order to allow for police access to the database.[862]

ii. The proposed Council Decision on access to EURODAC for law enforcement purposes

On 10 September 2009[863] the Commission adopted a proposal concerning access to EURODAC data by Member States law enforcement authorities and Europol for law enforcement purposes.[864] The proposal was justified by the Commission on the basis that

> "[f]ingerprint data is especially useful information for law enforcement purposes, as it constitutes an important element in establishing the exact identity of a person. The usefulness of fingerprint databases in fighting crime is a fact that has been repeatedly acknowledged."[865]

Fingerprint data of asylum seekers are collected and stored in the Member State in which the asylum application was filed, as well as in EURODAC. In fact, the Commission points out that in most Member States the law enforcement authorities have direct or indirect access to their national databases that contain the fingerprints of asylum seekers for the purpose of fighting crime.[866]

---

[861] Council of the European Union, Draft Council Conclusions on access to Eurodac by Member State police and law enforcement authorities as well as Europol, Council Doc. 10002/07, 25 May 2007.
[862] *Id.*
[863] On the same date the Commission introduced in the same package an Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], COM(2009) 342 final.
[864] Proposal of 10 September 2009 for a Council decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes , COM(2009) 342 final.
[865] *Id.* at 2.
[866] *Id.*

According to the Commission though, while Member States successfully access asylum seekers fingerprints on a national level, access to asylum seekers fingerprint databases of other Member States is more problematic. This is because there is a structural information and verification gap since there exists no single system which enables law enforcement authorities to determine the Member State that has information on an asylum seeker.[867] If a query of a national Automated Fingerprint Identification Systems (AFIS) using the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and crossborder crime (Prüm Decision) does not result in a 'hit', it is not certain that no information is available in a Member State.[868] In this respect, according always to the Commission's proposal, law enforcement authorities may not only remain "ignorant about whether or not information is available at all and in which Member State, but often also whether this information relates to the same person."[869] This means, pursuant to the proposal, that

> "without any action at EU level, the action of law enforcement authorities may become prohibitively expensive or may seriously jeopardise the application of the law because no further efficient and reasonable action to determine a person's identity can be taken."[870]

Moreover, the absence of the possibility for law enforcement authorities to access EURODAC to combat terrorism and other serious crime was reported as a shortcoming by the Commission in one of its Communications to the Council and the European Parliament.[871]

The proposal sets out the conditions, according to which, designated authorities of the Member States as well as Europol can request a comparison of fingerprint data with those stored in the EURODAC database. Access to EURODAC data is permitted where a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences; b) the comparison is necessary in a specific case; and, c) there are reasonable grounds to consider that such comparison with EURODAC data will

---

[867] *Id.*
[868] *Id.*
[869] *Id.*
[870] *Id.*
[871] Commission Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 24 November 2005 COM(2005) 597.

substantially contribute to the prevention, detection or investigation of any of the criminal offences in question.[872] In case of a successful comparison resulting in a 'hit' reply from EURODAC, all data held in the EURODAC system regarding the fingerprint will be transmitted to the relevant authorities.

Concerning the data protection rules, it is stipulated that the provisions of the Data Protection Framework Decision are applicable to the processing of personal data under the EURODAC proposal.[873] The proposal contains a number of data protection provisions regarding data security,[874] the prohibition of transfers of data to third countries,[875] and the obligation to monitor the logging and all data processing operations carried out in the EURODAC system.[876] Finally, it envisages that data obtained from EURODAC will be erased after a period of one month, if they are not required for a specific ongoing criminal investigation.[877]

iii. Criticisms

The proposal is problematic for several reasons. First, here again we have to deal with a function creep case. When adopted, the Regulation establishing EURODAC did not contemplate police access to EURODAC; the fingerprints were collected for the very specific purpose of determining which Member State is responsible for examining an asylum application, and in any case for facilitating the application of the Dublin Regulation. To be used for a completely different purpose, by law enforcement authorities to fight terrorism and crime, goes clearly against the purpose limitation principle and the legitimacy of the processing.

Access to EURODAC data by law enforcement authorities has, however, consequences that go beyond concerns on interferences with the right to data

[872] Article 7 of the Proposal for a Council Decision on the access of law enforcement authorities to EURODAC. For the conditions of access for Europol *see* Article 8.
[873] Article 10 (1) of the Proposal for a Council Decision on the access of law enforcement authorities to EURODAC.
[874] Article 11 of the Proposal for a Council Decision on the access of law enforcement authorities to EURODAC.
[875] Article 12 of the Proposal for a Council Decision on the access of law enforcement authorities to EURODAC.
[876] Article 13 of the Proposal for a Council Decision on the access of law enforcement authorities to EURODAC.
[877] Article 10 (4) of the Proposal for a Council Decision on the access of law enforcement authorities to EURODAC.

protection. The proposal for a Council Decision not only concerns individuals in principle not suspected of any crime, but what is more important, it targets particularly vulnerable groups in society, such as asylum seekers who, are in need of higher protection because they flee from persecution.[878] Furthermore, granting access to EURODAC data to law enforcement authorities might have a discriminatory impact on asylum seekers or illegal cross-borders[879] whose data are stored in the EURODAC database, in that they might be subject database to "a greater level of surveillance" than others in the population,[880] particularly as there is a general presumption that a disproportionate criminal activity might result from this group.

Finally, as the EDPS highlighted in his Opinion, the Commission's proposal raises questions with regards to its necessity since there already exists a number of legal instruments,[881] concerning access to centralized databases by law enforcement authorities that –in some cases- have not yet been fully implemented.

iv. The situation after Lisbon

With the entry into force of the Treaty of Lisbon, and in particular the Treaty on the Functioning of the European Union, which abolished the pillar system, and merged the former first and third pillars, the proposal for a Council Decision on law enforcement access to EURODAC lapsed.[882] According to the Communication on the

[878] *See* Opinion of the European Data Protection Supervisor on the Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes (2010/C 92/01) OJ C 92/1 of 10.4.2010, para 17.
[879] *Id.*
[880] Baldaccini, *supra* note 793, at 44.
[881] For instance, the Prüm Decision, provides that Member States shall grant each other an automated access *inter alia* to national Automated Fingerprint Identification Systems (AFIS). Also, 'Swedish' Framework Decision 2006/960/JHA facilitates the exchange of information (fingerprints and supplementary information) which is held by or is available to law enforcement authorities in the Member States.
[882] Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version) of 11.10.2010 COM(2010) 555 final, 3.

consequences of the entry into force of the Treaty of Lisbon for ongoing interinstitutional decision-making procedures,[883] such proposal should be formally withdrawn and replaced with a new proposal under the new framework of the TFEU with the participation of the European Parliament in the decision-making process.

However, due to the criticisms raised against such a controversial measure and the Commission's desire to progress on the negotiations on the asylum package and facilitating the conclusion of an agreement on the EURODAC Regulation, the Commission decided to withdraw –at least temporarily- from the EURODAC Regulation those provisions referring to the access to the database for law enforcement purposes.[884] According to the Commission, this would enable "the swifter adoption of the new EURODAC Regulation" and would "facilitate the timely set up of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice",[885] since that Agency is planned to be also responsible for the management of EURODAC.

6. Biometric data

As seen above, all three EU centralised databases (will) store biometric data:[886] SIS II[887] and VIS[888] fingerprints and photographs, and EURODAC fingerprints.[889] The notion of biometrics although mentioned explicitly,[890] is not further explained in any

[883] Communication from the Commission to the European Parliament and the Council, Consequences of the entry into force of the Treaty of Lisbon for ongoing interinstitutional decision-making procedures COM(2009) 665 final, 2.12.2009.
[884] Amended proposal for a EURODAC Regulation, 3.
[885] *Id.*
[886] *See* Paul De Hert et al., *Machine-readable Identity Documents with Biometric Data in the EU-Overview of the Legal Framework*, 21 KEESING JOURNAL OF DOCUMENTS & IDENTITY 3 (2006).
[887] Article 20 (2) (e) and (f) of the SIS II Decision.
[888] Article 5 (1) (b) and (c) of the VIS Regulation.
[889] *See* Angela Liberatore, *Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union*, 13 EUROPEAN JOURNAL ON CRIMINAL POLICY AND RESEARCH 109, 115 (2007).
[890] Recital 14 of the SIS II Decision provides: "SISII should permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned." Recital 10 of the VIS Regulation reads as follows: "To ensure reliable verification and identification of visa applicants, it is necessary to process biometric data in the VIS."

of their respective instruments. Biometrics[891] (from the Greek *βίος*, life and *μέτρον*, measurement, in essence, features that can be measured)[892] are normally used to identify individuals based on their distinguishing[893] physiological (or behavioural) characteristics.[894] Physiological characteristics include, among others, fingerprints, retinal and iris pattern, hand and finger geometry, facial recognition. Examples of behavioural characteristics are voice patterns and gait analysis.

Biometric data can be used in two different ways when stored in IT systems: they can provide for a 'one-to-one' search, using the data to confirm identity, by comparing, for example the fingerprints of a person against those contained in the database;[895] but they can also provide for a 'one-to-many' search, where the data is used to identify a person by, for instance, comparing his fingerprints with all other fingerprints stored in the system.[896]

As mentioned above, SIS currently operates as an alphanumerical database that contains data which allow only for two results: hit or no hit ('one-to-one' search). The inclusion of biometrics in SIS II will allow for more effective and different types of searches to take place in the system in order to identify individuals.[897] The possibility of 'one-to-many' searches will transform the nature of the SIS from a database used for control purposes to one which can be used for investigative

---

[891] For a discussion on the fundamental rights posed by biometrics *see* PAUL DE HERT, BIOMETRICS: LEGAL ISSUES AND IMPLICATIONS (Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission, January 2005).

[892] JOINT RESEARCH CENTRE- INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (DG JRC), BIOMETRICS AT THE FRONTIERS: ASSESSING THE IMPACT ON SOCIETY - FOR THE EUROPEAN PARLIAMENT COMMITTEE ON CITIZENS' FREEDOMS AND RIGHTS, JUSTICE AND HOME AFFAIRS (LIBE) 35 (Technical Report Series).

[893] As Corien Prins explains "[t]he application of biometric technology is based on the empirically verifiable notion that nature does not repeat itself and that, therefore, certain traits are unique." Corien Prins, *Making Our Body Identify for Us: Legal Implications of Biometric Technologies*, 14 COMPUTER LAW & SECURITY REVIEW 149, 160 (1998).

[894] EVELIEN BROUWER, DATA SURVEILLANCE AND BORDER CONTROL IN THE EU: BALANCING EFFICIENCY AND LEGAL PROTECTION OF THIRD COUNTRY NATIONALS (Challenge, liberty and security Paper, 2005), *available at* http://www.libertysecurity.org/article289.html.

[895] *See* House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, paragraph 57; Dennis Broeders, *The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants*, 22 INTERNATIONAL SOCIOLOGY 71, 88 (2007).

[896] MITSILEGAS, EU CRIMINAL LAW, *supra* note 475, at 240.

[897] Recital 14 of the Decision provides that: "SIS II should permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. In the same perspective, SIS II should also allow for the processing of data concerning individuals whose identity has been misused in order to avoid inconveniences caused by their misidentification, subject to suitable safeguards, in particular the consent of the individual concerned and a strict limitation of the purposes for which such data can be lawfully processed."

purposes, enabling so-called 'fishing expeditions' in which people registered in the SIS II database will form the suspect population.[898]

In *S and Marper v UK,*[899] the ECtHR distinguished between different types of biometric data, cellular samples and DNA profiles on the one hand, and fingerprints on the other. Its pronouncements on fingerprints are very interesting for the present analysis. First, the Court stated that fingerprints "do not contain as much information as either cellular examples or DNA profiles."[900] Furthermore, it recalled its case-law, according to which, the retention of fingerprints and photographs following an arrest did not constitute an interference with the right to private life, as these biometric data did not contain any "subjective appreciations which called for refutation."[901] In any case, the Court held that fingerprints contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances, and therefore, their retention can be regarded as constituting an interference with the right to respect for private life.[902] It should be reminded here that the Court's analysis focused mainly on the storage of fingerprints for criminal investigations purposes. In the context of the present discussion, VIS, EURODAC (and to an extent SIS II) store biometrics for totally unrelated to criminal prevention purposes.

The added value of biometrics is found allegedly in their unique identifying capabilities.[903] Identification on the basis of biometric data is presumed to be reliable beyond any doubts.[904] In this respect, biometric identifiers stored in centralised databases are expected to significantly improve the possibilities for police searches.[905] As experts explain, however, biometrics present a reliable identification process "in as much as they provide a strong link between physical persons with their identity

---

[898] Baldaccini, *supra* note 793, at 38.
[899] *See S and Marper v UK, supra* note 262.
[900] *Id.* at ¶ 78.
[901] *Kinnunen v. Finland*, Appl. no. 24950/94, Commission decision of 15 May 1996.
[902] *S and Marper v UK*, paras 84-86.
[903] ARTICLE 29 WORKING PARTY, WORKING DOCUMENT ON BIOMETRICS 10 (12168/02/EN, August 01, 2003). *See* also ARTICLE 29 WORKING PARTY, OPINION NO 7/2004 ON THE INCLUSION OF BIOMETRIC ELEMENTS IN RESIDENCE PERMITS AND VISAS TAKING ACCOUNT OF THE ESTABLISHMENT OF THE EUROPEAN INFORMATION SYSTEM ON VISAS (VIS).
[904] *See* Juliet Lodge, *EJustice, Security and Biometrics: The EU's Proximity Paradox*, 13 EUROPEAN JOURNAL OF CRIME, CRIMINAL LAW AND CRIMINAL JUSTICE 533 (2005).
[905] In this regard, the June 2003 European Council of Thessaloniki invited the Commission to prepare proposals for a 'coherent approach' in the EU on biometric identifiers to result in 'harmonised solutions for documents for third country nationals, EU citizens' passport and information systems'. See Presidency Conclusions, Thessaloniki European Council, 19–20 June 2003, para 11.

data."[906] While (full) biometric data are normally very reliable, their identification capacities may be reduced for a number of reasons, such as, for instance, when databases store data templates,[907] rather than the full ('raw') biometric data.[908] Using biometrics as sole identification key entails a high risk of false identification or false non-identification (false rejection rate or false acceptance rate).[909] The so- called 'false rejection rate' of the various biometric identifiers, which is estimated between 0.5 and 1 %, is very high if one takes into account the millions of people to be recorded in the three EU large-scale databases.[910] In the case of fingerprints, experts estimate that "circa five per cent of people would not be able to register and deliver a readable fingerprint."[911] This is considered significant when implementing databases of millions of people.

Furthermore, as it has been pointed out by the European Data Protection Supervisor (EDPS), the use of biometrics as a unique means of identification can have serious consequences for those who are wrongly identified, given the tendency of authorities to overestimate the reliability of biometric data.[912] The following case is illuminating at this point: a US lawyer, was jailed for two weeks because the FBI successfully matched his fingerprint with one found in the Madrid terrorist bombing (on the plastic bag which contained the detonator). However, in the end it was demonstrated that the matching process was flawed and resulted to a misinterpretation.[913] The use of databases, such as SIS II and VIS as 'biometrics search engines' may provide a powerful tool for law enforcement authorities, but it can have serious consequences concerning the accuracy of the results they produce.[914]

---

[906] Joint Research Centre- Institute for Prospective Technological Studies (DG JRC), *supra* note 892, at 13.
[907] A template is normally a set of numbers that the 'raw data' are processed into, through the use of an algorithm. *See Id.* at 12.
[908] The Joint Research Centre Report for the LIBE Committee notes: "Biometric identification is a statistical process. Variations in conditions between enrolment and acquisition as well as bodily changes (temporary or permanent) mean that there is never a 100% match." *Id.* at 36.
[909] Memorandum by the Meijers Committee (11 October 2006), House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, at 13.
[910] *Id.*
[911] Joint Research Centre- Institute for Prospective Technological Studies (DG JRC), *supra* note 892, at 58.
[912] Opinion of the European Data Protection Supervisor on the SIS II Proposals, *supra* note 112, at 7.
[913] *Id.*
[914] *Id.* *See* also Article 22 (a) that lays out a special rule for the photographs and fingerprints to be included into SIS II. This biometric data will only be entered following a "special quality check" in order to ascertain the fulfilment of a minimum data quality standard.

The storage of biometric data poses further problems as well. It increases the risk of security breaches and unauthorised accesses to the databases, combined with the possibility of misuse or manipulation of biometric data by criminal organisations, and the possible increase of identity theft.[915] Finally, there is a high risk that the inclusion of biometric identifiers might develop the EU databases in systems used for 'fishing' and data mining expeditions.[916] This means, that on the one hand, these could be potential used by police authorities, to 'fish around' different information about suspected individuals, especially in the context of the fight against terrorism; and on the other hand, they can be used in order to search for individuals that 'fit' a certain profile that the law enforcement authorities already have.

According to Article 22 (b) and (c) of the SIS II Decision, initially the biometric data entered in the system will only be used to "confirm the identity" of a person who has been located as a result of an alphanumeric search made in SIS II. Later, however, and as soon as this becomes technically possible, fingerprints may also be used to identify a person on the basis of his biometric identifier ('one to many' searches).

7. The Privacy - Data Protection debate in the context of databases

As Daniel Solove notes, "since their creation, computer databases have been viewed as problematic"; they "certainly present a privacy problem",[917] but it is not so clear what the nature of this problem is.

The notion of privacy as such, despite its vagueness, is not so helpful in assessing the problems of computer databases. It is not exactly clear why an individual's private and family life is invaded upon when his data are entered in SIS II. Certainly, having your personal data stored in such a database has serious implications, all the more because they are registered in connection of an alert that has to be executed. But what is the privacy problem exactly? The same concerns apply to VIS and EURODAC. Even if the visa information is accessed by law enforcement

[915] Memorandum by the Meijers Committee, House of Lords European Union Committee, *Schengen Information System II (SIS II)*, *supra* note 655, at 13.
[916] Oral Evidence by Guild *Id.* at 82.
[917] Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, *supra* note 94, at 1394–1395.

authorities, the interferences on the right of privacy of the individuals concerned are not so obvious.[918]

The nature of the problem posed by databases is better described by the data protection law. All three EU-scale databases process personal data. The problems they pose concern different data protection principles: purpose limitation, data security, data quality, the due process rights of individuals that have their data stored in such systems, independent supervision. The underlying problem behind databases is not exactly a privacy one. As Solove have correctly put it, it is

> "a problem of our inability to participate meaningfully in the processing of our personal information."[919]

This is a problem dealt by data protection law. In its –necessarily- procedural character it seems that the right to data protection has an added value in the present case. It conceptualises in a clear and precise manner the different problems posed by databases and through the information principles, it gives guidelines on how these should be dealt with. At first sight, one could argue that it plays the role of the *lex specialis* of the right to privacy, since it materialises in the different information principles privacy concerns.[920] Data protection, however, seems to go further. As discussed in Chapter 1, its underlying value is not only privacy. Data protection, as a right, aims to pursue further values, such as transparency of processing, meaningful participation of the data subject, data security, non-discrimination, proportionality. This is why it is particularly valuable in the context of computer databases. Because the problems they pose have to do more with the asymmetry of power between data

[918] This is with the exception of biometric data that raise serious privacy concerns as they are highly sensitive data. *See* Roger Clarke, *Biometrics' Inadequacies and Threats, and the Need for Regulation*. However, it does not mean that all biometric data are necessarily sensitive data in every case. For a relevant discussion *see* Article 29 Working Party, *Working Document on Biometrics*, *supra* note 903, at 10.

[919] Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, *supra* note 94, at 1461. Solove argues that "the European Union Privacy Directive would go far towards addressing the [database] privacy problem as I have characterized it."

[920] As Brown and Korff have put it: "The right to privacy relates to the right to respect for private life, guaranteed by Article 8 of the European Convention on Human Rights (ECHR), but is also shorthand for a more specific right, usually referred to in terms of 'data protection'. This is increasingly recognized as a right *sui generis* (e.g. in Article 8 of the EU Charter on Fundamental Rights) and is not only concerned with protecting individuals from intrusions into their privacy or private life, but more broadly against the improper collecting, storing, sharing and use of their data. It addresses the central issue in the 'information society' of the extent of control by 'data controllers' over individuals – tellingly referred to as 'data subjects' – through possession of their data." Brown & Korff, *supra* note 573, at 120.

'controllers' and data subjects. For this reason, the above analysis focused on the problems that SIS II, VIS, and EURODAC pose on specific data protection principles.

8. Interoperability of SIS II, VIS and EURODAC and the Proposed Agency for the Operational Management of large-scale IT systems in the AFSJ

On 24 November 2005, the Commission issued a Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs.[921] The purpose of this Communication was, according to the Commission,

> "to highlight how, beyond their present purposes, these systems can more effectively support the policies linked to the free movement of persons and serve the objective of combating terrorism and serious crime."[922]

This could be made possible by establishing 'interoperability' between SIS II, VIS and EURODAC. The Commission defined 'interoperability' as

> "the ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge."[923]

The Commission, furthermore, clarified that 'interoperability' is a technical rather than a legal or political concept, and it is disconnected from the question of whether the data exchange is legally or politically possible or required. The Communication did not go on further details on the proposed interoperability on the basis that technical and organisational issues were raised.[924] However, it noted that the existing systems in the Area of Freedom, Security and Justice are under-exploited,[925] and that bringing the daily management of these systems together "in a single organisation would also bring about significant synergy effects."[926]

---

[921] Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs COM(2005) 597 final, 24.11.2005.
[922] *Id.* at 2.
[923] *Id.* at 3.
[924] *Id.* at 5.
[925] *Id.*
[926] *Id.*

As it has been noted by some commentators, the idea of interoperability of databases is not new, but it goes back to 1977.[927] Only it is now that the technological developments would allow for such synergies to be built. This is why the Commission characterises interoperability as a technical possibility. Essentially, it presumes that since the relevant technology exists, it can be used to enhance the capabilities of the existing systems. The EDPS in his Comments on the Commission's Communication was critical on this approach. If technical means are used just because they are available, it seems that "it is the means that justify the end and not the other way around."[928] Interoperability might be a technical issue, but it raises serious legal and political questions. As it has been put astutely,

> "[a]lthough the interoperability of police and justice databases will be realised technically, it must be sanctioned legally after ... [a] sensitive political debate."[929]

From the point of view of the fundamental right to data protection, a potential interoperability of SIS II, VIS and EURODAC raises concerns since it could create "interconnected databases" and introduce a new use by providing new possibilities of access to them.[930] This interferes with the purpose limitation principle as the interlinking of three databases designed for distinct purposes might provide a fourth one aggregating the irrelevant with each other purposes.[931]

On 24 June 2009, the Commission adopted a legislative proposal establishing an Agency responsible for the operational management of large-scale IT systems in the area of freedom, security and justice which was replaced by an amended proposal on 19 March 2010 taking into account the new legal framework after the Lisbon Treaty.[932] The Agency, which will have legal personality, will be responsible for the long-term operational management of the SIS II, the VIS and EURODAC (keeping

---

[927] *See* the relevant discussion in Paul De Hert & Serge Gutwirth, *Interoperability of Police Databases Within the EU: An Accountable Political Choice?*, 20 INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 21, 23 (2006).

[928] EUROPEAN DATA PROTECTION SUPERVISOR, COMMENTS ON THE COMMUNICATION OF THE COMMISSION ON INTEROPERABILITY OF EUROPEAN DATABASES 2 (March 10, 2006).

[929] De Hert & Gutwirth, *Interoperability of Police Databases Within the EU*, *supra* note 927, at 25.

[930] European Data Protection Supervisor, *Comments on the Communication of the Commission on Interoperability of European Databases*, *supra* note 928, at 4.

[931] European Data Protection Supervisor, *Comments on the Communication of the Commission on Interoperability of European Databases*, *supra* note 928.

[932] Amended Proposal for a Regulation (EU) No ……/…… of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (presented by the Commission pursuant to Article 293(2) of the Treaty on the Functioning of the European Union) COM(2010)93 final 2009/0089/P (COD), 19.3.2010.

the systems functioning 24 hours a day, seven days a week, thus ensuring a continuous, uninterrupted flow of data exchange).[933] The Commission explained that such an Agency was found to be, among the different options, the most "feasible alternative for carrying out the tasks of a "Management Authority" for these systems in the long term."[934] As the Commission's Proposal notes "combining the systems in a joint Agency will make it possible to exploit synergies and share facilities and staff."[935]

The envisaged Agency will not affect the specific rules governing the purpose, access rights, security measures and further data protection requirements applicable to the three EU databases.[936] Its main governing body will be a Management Board "with an adequate representation of the Member States and the Commission", including the other non-EU countries that participate in the Schengen *acquis*.[937] According to Article 25 of the proposed Regulation, the applicable data protection legal framework for the information processed by the Agency will be Regulation 45/2001.

Whether the new Agency will introduce interoperability and its problems through the back door, it remains to be seen when the Regulation is adopted and the Agency starts working in practice. A function creep risk can be avoided as the EDPS has noted in his Opinion with regard to the Commission's proposal, if "the scope of (possible) activities of the Agency is limited and clearly defined."[938] Clear and precise safeguards need to be put in place so that the Agency does not introduce a *de facto* interoperability.

---

[933] *Id.*
[934] *Id.*
[935] *Id.*
[936] *Id.*
[937] *Id.*
[938] Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and on the proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty (2010/C 70/02) OJ C 70/13 of 19.3.2010, para 26.

The Information Transfer Case.

Introduction

As discussed above, the centrepiece of the EU data protection legislation, the Data Protection Directive pursues two objectives: on the one hand, the harmonisation of national data protection rules, on the other hand, the free movement of personal data.[939] The two purposes are placed at equal footing; this means that the free movement of data constitutes an important aspect of the European conception of the notion of personal data protection.

While personal data can flow freely between the Member States of the European Union, ironically, the story changes when they cross the EU's external borders and move to third countries with different privacy regimes. That data are deemed to cross borders in today's globalised world is more than evident, either this is taking place for the purposes of international trade, or for the fight of international terrorism and crime. For this reason, transborder data flows are allowed to third countries with the necessary requirement that these should ensure in principle an 'adequate' level of protection of personal data.[940]

The information transfer case aims to test the added value of the fundamental right to data protection in cross- border data flows. In particular, this Chapter discusses two of the most controversial instances of data processing in the context of counter-terrorism: the transfer of PNR and SWIFT data to the US counter-terrorism and law enforcement authorities. The Chapter is structured as follows: The First Part focuses on the EU-US PNR Agreements. It examines their background and their chronology, addresses the different privacy regimes of the EU and the US, and presents the domestic EU PNR legislative proposals. It goes on to discuss the potential privacy and data protection issues that they both pose, and takes a closer look to the questions of datamining and profiling of airline passengers. The Second Part turns to the SWIFT case. It examines the sequence of events that led to the first TFTP Agreement, its rejection by the European Parliament, and the conclusion of a

[939] Article 1 (2) of the Data Protection Directive.
[940] Article 25 of the Data Protection Directive.

new Agreement. It addresses the nature of the fundamental rights' problems posed by the Agreement and engages into a substantive analysis of the relevant infringements.

Chapter 6. Passenger Name Record

1. PNR Data: What is it about?

> *"As you know, passenger name record information is that which is collected by the travel industry or the airlines when a person makes an airline reservation. It's basic information. It's nothing that's particularly confidential by its very nature. It's things like your name, passport number, frequent flyer number, credit card information and contact information like telephone and address. What we do is we take this information and we run it against lists of known and suspected terrorists. We use it to analyze links that may arise or connections that may arise between travellers and others who are known to be terrorists so that we can identify those of the 80 million air passengers who come to the United States every year who we need to take a closer look at. It is the ability to use this information to identify hidden connections that makes it so valuable as a tool to keep out dangerous people."*[941]

1.1 Defining Passenger Name Record (PNR)

According to the European Commission, 'Passenger Name Record' (PNR) is a computerized "record of each passenger's travel requirements which contains all information necessary to enable reservations to be processed and controlled by the booking[942] and participating airlines[943]."[944] PNR data sets may contain "as many as 60 data fields",[945] including name, address, e-mail, contact telephone numbers, passport information, date of reservation, date of travel, travel itinerary, all forms of payment information, billing address, frequent flyer information, travel agency and travel

[941] US Homeland Security Secretary Michael Chertoff's Address before the Civil Liberties Committee of the European Parliament, Brussels 14 May 2007, *available at* http://useu.usmission.gov/dossiers/data_privacy/may1407_chertoff_ep.html.
[942] "Booking airline" denotes the airline with which the passenger made his original reservations or with which additional reservations were made after commencement of the journey.
[943] "Participating airline" means any airline on which the booking airline has requested space, on one or more of its flights, to be held for a passenger.
[944] Commission Decision 2004/535/EC 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), para 4.
[945] HOUSE OF LORDS EUROPEAN UNION COMMITTEE, THE EU/US PASSENGER NAME RECORD (PNR) AGREEMENT ¶ 12 (21st Report of Session 2006–07).

agent, travel status of passenger (such as confirmations and check-in status), ticketing field information (including ticket number, one-way tickets and Automated Ticket Fare Quote), date of issuance, seat number, seat information, general remarks, no show history, baggage information, go show information, OSI (Other Service-related Information), and SSI/SSR (Special Service Information/Special Service Requests). PNR can further contain information on individuals who are not travelling by air,[946] such as, for instance, the details (e-mail address, telephone number) for contacting a person (e.g. a friend or a family member).[947] PNR data may also reveal religious or ethnic information (for example from the meal preferences of the passenger),[948] affiliation to a particular group,[949] as well as medical data (for example medical assistance required by the passenger, or any disabilities or health problems that are made known to the airline).[950] Few airlines hold PNR data in their own databases; those are normally stored centrally in the databases of the "Computerized Reservation Systems" ("CRS").[951] There are currently three "CRS's" operating worldwide: Amadeus, Sabre, and Travelport.[952] PNR data are never deleted from the "CRS's", once created, they are archived and retained indefinitely.[953]

PNR data are normally distinguished from APIS data (Advanced Passenger Information System) which include information, such as: names, gender, date of birth, nationality, type of travel document, country of issuance, and expiry date.[954] The basic difference is that APIS data comprise normally the biographical information included in the machine-readable part of a passport,[955] and is therefore considered more accurate than PNR, that is "unverified information provided by passengers for

---

[946] Richard Rasmussen, *Is International Travel Per Se Suspicion of Terrorism? The Dispute Between the United States and European Union over Passenger Name Record Data Transfers*, 26 WIS. INT'L L.J. 551, 553 (2009).
[947] ARTICLE 29 WORKING PARTY, OPINION 6/2002 ON TRANSMISSION OF PASSENGER MANIFEST INFORMATION AND OTHER DATA FROM AIRLINES TO THE UNITED STATES.
[948] *Id.*
[949] *Id.*
[950] *Id.*
[951] Edward Hasbrouck, *What's in a Passenger Name Record?*, THE PRACTICAL NOMAD.
[952] *Id.* According to Hasbrouck, of the four "CRS" that used to operate worldwide before, two (Worldspan and Galileo) merged in 2007 in Travelport, but continue to operate two distinct technology platforms under different brand names. Among them, only Amadeus is based in Europe.
[953] *Id.*
[954] *See* Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004, p. 24.
[955] House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, *supra* note 945, paragraph 11.

enabling reservations and carrying out the check-in process."[956] APIS data are most commonly used for identification purposes in border controls,[957] while PNR data are intended to detect criminal or terrorist activity.[958]

1.2 Why is Airline Passengers' Surveillance Needed? Uses of PNR data

Michael Chertoff, US Secretary of Homeland Security, noted in an article in Washington Post, in 2006:

> "If we learned anything from Sept. 11, 2001, it is that we need to be better at connecting the dots of terrorist-related information."[959]

In fact, it cannot go unmentioned that nine of the nineteen hijackers of September 11, 2001 were identified as threat risks by the Airline Passenger Screening Programme operating at that time in the US,[960] but were nevertheless allowed to board the planes.[961] 'Connecting the dots',[962] therefore, is crucial to identify terrorists and prevent future terrorist attacks.[963] Law enforcement authorities should not merely act proactively;[964] they should, more importantly, focus on people.[965] The question is not

---

[956] Commission Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 492 final, 3.

[957] According to the Commission (*supra* note 17, 4) "API data are [...] primarily used as an identity management tool."

[958] *See* 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 (2006/2193(INI)), P6_TA(2006)0354.

[959] Michael Chertoff, *A Tool We Need to Stop the Next Airliner Plot*, WASHINGTON POST (2006).

[960] CAPPS I. *See* below.

[961] House Select Committee on Homeland Security: Subcommittee on Econ. Sec., Infrastructure Prot. & Cybersecurity Hearing on Air Passenger Pre-Screening, 109th Cong. (June 29, 2005) (statement of James Dempsey, Exec. Dir. Ctr. For Democracy & Tech). *See* also Stephen Dummer, *COMMENT: Secure Flight and Dataveillance, A New Type of Civil Liberties Erosion: Stripping Your Rights When You Don't Even Know It*, 75 MISS. L.J. 583, 584 (2006).

[962] *See* K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1 (2003).

[963] Mehmet Ozcan & Fatma Yilmaz, *Pendulum Swings in Between Civil Rights and Security: EU Policies Against Terrorism in the Light of the PNR Case*, 1 USAK Y.B. INT'L POL. & L. 51, 54 (2008).

[964] Taipale, *supra* note 962, at 4.

[965] Timothy Ravich, *Is Airline Passenger Profiling Necessary?*, 62 U. MIAMI L. REV. 1, 2 (2007). Ravich criticises the anti-terrorism techniques employed until recently as inefficient, because they were focusing on objects instead of people: "On August 10, 2006 British intelligence presented a terrorist plot to blow up ten airplanes by detonating common liquids. In response, the Transportation Security Administration ("TSA") banned certain carry-on items. In May 2007 TSA unveiled "FIDO", a hand-held scanner capable of detecting liquid explosives inside sealed bottles. Although providing an important layer of security, carry-on restrictions and explosives detecting equipment exemplify why profiling is necessary to safeguard commercial aviation. Reaction-based national aviation security

anymore about screening the baggage of passengers, it is about screening the passengers themselves.

The pre-screening of passengers is carried out through the help of PNR data. It is normally argued that unlike API data that are used as an identity verification tool, PNR are used as a criminal intelligence tool.[966] As the US Department of Homeland Security (DHS) explains, "PNR information is a critical tool used [...] in such screening of travellers to identify individuals of interest who are planning to travel to the United States."[967] But, what is the exact role of PNR data in the detection of "individuals of interest"? In its 2010 Communication on the global approach to transfers of PNR data to third countries, the European Commission identified three different uses of PNR: First, the "re-active" use in investigations and prosecutions. PNR is utilised to unravel networks after a crime has been committed.[968] Second, the "real time" use, where PNR is used in order to prevent a crime, survey or arrest persons before a crime has been committed or because a crime has been or is being committed. In such cases PNR are necessary for running against predetermined fact-based risk indicators in order to identify the previously "unknown" suspects and for running against various databases of persons and objects sought.[969] Third, the "pro-active" use for trend analysis and creation of fact-based travel and general behaviour patterns, which can then be used in real time use.[970] The uses of PNR data are, therefore, classified chronologically: past-present-future. In this way, however, especially the present and future uses seem to be intertwined in an unduly circular relationship: PNR are used to create patterns (future) which will be subsequently used to identify "unknown" suspects (present), which in their turn may generate further patterns (future), etc. Besides the above chronological classification of PNR uses, the Commission's discussion on the specific uses of PNR data is even more confusing:

---

policy focused myopically on objects instead of people is backward looking and flowed, "the equivalent of fighting the last war.""

[966] Commission Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries, s*upra* note 18, 4.

[967] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY OFFICE, A REPORT CONCERNING PASSENGER NAME RECORD INFORMATION DERIVED FROM FLIGHTS BETWEEN THE U.S. AND THE EUROPEAN UNION 7 (December 18, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf.

[968] Commission Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries, s*upra* note 18, 5.

[969] *Id.*

[970] *Id.*

> "The uses of PNR are mainly the following: (i) risk assessment of passengers and identification of "unknown" persons [...], (ii) earlier availability than API data, and provision of an advantage to law enforcement authorities in allowing more time for its processing, analysis and any follow-up action, (iii) identification to which persons specific addresses, credit cards etc that are connected to criminal offences belong, and (iv) matching of PNR against other PNR for the identification of associates of suspects, for example by finding who travels together."[971]

While point (i) and (iv) seem to be describing specific PNR uses, the same cannot be argued for (ii) and (iii), which appear to present the advantages of the PNR data.

1.3 'Born in the USA': A Brief History of Airline Passenger Screening

The screening of airline passengers is not an invention of the post 9/11 era. Passenger profiling was taking place since the 1960s in the USA in order to deal with the increased airline hijackings in that period.[972] More particularly, the US Federal Aviation Administration ("FAA") had established "approximately twenty-five characteristics empirically linked with hijackers historically".[973] The scheme, however, was abandoned in 1972 as it was found ineffective.[974] In 1996, after an airline tragedy,[975] President Clinton announced the creation of the "White House Commission on Aviation Safety and Security" which was mandated "to look at the changing security threat"[976] in the field of aviation, and "develop and recommend to

---

[971] Commission Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries, s*upra* note 18, 5.
[972] Ravich, *supra* note 965, at 9.
[973] *Id.*
[974] *Id.* at 10.
[975] TWA flight 800 from New York to Rome, with a stopover in Paris exploded and crashed into the Atlantic Ocean on July 17, 1996, 12 minutes after takeoff, killing all 230 persons on board. Initially, it was believed that a terrorist attack was the cause of the accident; afterwards, however, it was found that the cause might have been an explosion of flammable fuel/air vapours in a fuel tank. *See* NATIONAL TRANSPORTATION SAFETY BOARD, AIRCRAFT ACCIDENT REPORT IN-FLIGHT BREAKUP OVER THE ATLANTIC OCEAN TRANS WORLD AIRLINES FLIGHT 800 BOEING 747-131, N93119 NEAR EAST MORICHES, NEW YORK JULY 17, 1996 (200AD), *available at* http://www.ntsb.gov/doclib/reports/2000/AAR0003.pdf. Joan Lowy, *Jet Fuel-tank Protection Ordered U.S. Cites 1996 Explosion of 747*, SEATTLE POST-INTELLIGENCER (2008).
[976] WHITE HOUSE COMMISSION ON WHITE HOUSE COMMISSION ON AVIATION SAFETY AND SECURITY AVIATION SAFETY AND SECURITY, FINAL REPORT TO PRESIDENT CLINTON 3 (1997), *available at* http://www.fas.org/irp/threat/212fin~1.html.

the President a strategy designed to improve aviation safety and security, both domestically and internationally."[977] The "White House Commission on Aviation Safety and Security", also known as "Gore Commission", in its final report made a number of recommendations in order to make flights safer.[978] It noted that:

> "Profiling can leverage an investment in technology and trained people. Based on information that is already in computer databases, passengers could be separated into a very large majority who present little or no risk, and a small minority who merit additional attention."[979]

The Commission, therefore, recommended three steps:

> "First, FBI, CIA, and ATF should evaluate and expand the research into known terrorists, hijackers, and bombers needed to develop the best possible profiling system. They should keep in mind that such a profile would be most useful to the airlines if it could be matched against automated passenger information which the airlines maintain.
>
> Second, the FBI and CIA should develop a system that would allow important intelligence information on known or suspected terrorists to be used in passenger profiling without compromising the integrity of the intelligence or its sources…
>
> Third, the Commission will establish an advisory board on civil liberties questions that arise from the development and use of profiling systems."[980]

The Report seemed to be mandating two things: first, the creation of profiles for potential hijackers and terrorists through the use of intelligence information; second, the matching of those profiles with PNR data in order to get to the 'real' people.

The plan did not take long to be implemented. The first "Computer Assisted Passenger Screening" ("CAPS") programme was developed by Northwest Airlines in 1997 with a grant from FAA.[981] CAPS was turned by FAA into the "Computer Assisted Passenger Pre-screening System" ("CAPPS"), and offered to all major

---

[977] Executive Order No 13015, 61 Fed. Reg. 43, 937 (August 22, 1996). *See* also Ravich, *supra* note 965, at 10–11.

[978] White House Commission on White House Commission on Aviation Safety and Security Aviation Safety and Security, *supra* note 976. *See* also Robert Hahn, *The Economics of Airline Safety and Security: An Analysis of the White House Commission's Recommendations*, 20 HARV. J. L. & PUB. POL'Y 791 (1997).

[979] White House Commission on White House Commission on Aviation Safety and Security Aviation Safety and Security, *supra* note 976, paragraph 3.19.

[980] *Id.*

[981] Ravich, *supra* note 965, at 11; Dummer, *supra* note 961, at 587.

airlines with hopes that it would be eventually adopted on a voluntary basis.[982] FAA rules required that "selectees", i.e. those who were regarded as a risk to the aircraft, were subjected to a secondary screening only of their checked baggage;[983] additional screening of the person or the carry-on baggage was not required.[984] CAPPS utilised approximately forty pieces of passenger data to identify passengers that fit predetermined profiles.[985] The criteria used by CAPPS in order to profile individuals remain unknown.[986] According to the "Gore Commission" report, "no profile should contain or be based on material of a constitutionally suspect nature – e.g., race, religion, national origin of U.S. citizens," and, therefore, the elements of the profiling system should be developed in such a way that ensures that "selection is not impermissibly based on national origin, racial, ethnic, religious or gender characteristics."[987] Despite this, CAPPS was criticised for targeting passengers of a certain racial group as "increased threats",[988] and that it lacked transparency,[989] and was ultimately abandoned.[990]

---

[982] Michael AuBuchon, *Comment: Choosing How Safe Is Enough: Increased Antiterrorist Federal Activity and Its Effect on the General Public and the Airport/airline Industry*, 64 J. AIR L. & COM. 891, 904 (1999).

[983] United States National Commission for Terrorist Attacks, *The Aviation Security System and the 9/11 Attacks*, STAFF STATEMENT NO. 3, 6.

[984] *Id.* For this reason, the 9/11 suicide bombers that were identified by CAPPS were allowed toboard their flight. The 9/11 Commission notes in its Report: "The consequences of selection reflected FAA's view that non- suicide bombing was the most substantial risk to domestic aircraft. Since the system in place on 9/11 confined the consequences of selection to the screening of checked bags for explosives, the application of CAPPS did not provide any defense against the weapons and tactics employed by the 9/11 hijackers. On American Airlines Flight 11, CAPPS chose three of the five hijackers as selectees. Since Waleed al Shehri checked no bags, his selection had no consequences. Wail al Shehri and Satam al Suqami had their checked bags scanned for explosives before they were loaded onto the plane... All five of the American Airlines Flight 77 hijackers were selected for security scrutiny.
Hani Hanjour, Khalid al Mihdhar, and Majed Moqed were chosen via the CAPPS criteria... for hijacker selectees Hani Hanjour, Nawaf al Hazmi, and Khalid al Mihdhar, who checked no bags on September 11, there were no consequences for their selection by the CAPPS system."

[985] Dummer, *supra* note 961, at 588.

[986] According to limited public information, profiles most likely took into account information such as: passenger's address; method of ticket purchase; when the ticket was purchased; travel companions; rental car status; departure date; flight destination and origin; passenger destination; and the round trip or one-way nature of the ticket. *See* Charu Chandrasekhar, *Flying While Brown: Federal Civil Rights Remedies to Post-9/1 1 Airline Racial Profiling of South Asians*, 10 ASIAN L.J. 215, 221 (2003). AuBuchon notes that "The Gore Commission has called such screening "positive profiling" as it seeks out those who meet beneficial criteria in order to single out the terrorist." AuBuchon, *supra* note 982, at 904.

[987] White House Commission on White House Commission on Aviation Safety and Security Aviation Safety and Security, *supra* note 976, paragraph 3.19.

[988] Chandrasekhar, *supra* note 986, at 217.

[989] Jamie Rhee, *Comment, Rational And Constitutional Approaches To Airline Safety In The Face Of Terrorist Threats*, 49 DEPAUL L. REV. 847, 865 (2000); Chandrasekhar, *supra* note 986, at 222.

[990] Chandrasekhar, *supra* note 986, at 222.

Following the terrorist attacks of 9/11, the Congress passed in November 2001 the Aviation and Transportation Security Act (ATSA),[991] which was intended to change "both the way in which passengers are screened and the entities responsible for conducting the screening."[992] ATSA also created the Transport Security Administration (TSA) within the Department of Transportation.[993] The TSA was mandated to carry out "security screening operations for passenger air transportation and intrastate air transportation."[994] It assumed responsibility for civil aviation security from the Federal Aviation Administration, and for passenger and baggage screening from the air carriers.[995] TSA was charged to develop the second generation of the "Computer- Assisted Passenger Prescreening System" ("CAPPS II")[996], in order to "confirm the identities of passengers and identify foreign terrorists or persons with terrorist connections before they board US aircraft."[997] The system operated as follows: during the reservation process, the passenger was required to provide four pieces of information: full name, home address, home phone number, and date of birth. This information is sent electronically to CAPPS II. Before the flight, CAPPS II would request an identity authentication from commercial data provider(s), meaning that the PNR data obtained during the reservation process would be verified by information held in the databases of one or more of the commercial data providers.[998] After obtaining the passengers' authentication scores, CAPPS II would conduct risk assessments using government databases, including classified and intelligence data, to generate a risk score categorizing the passenger as an acceptable risk, unknown risk, or unacceptable risk.[999] When the passenger would check in for a flight at the airport, her risk category would be transmitted from CAPPS II to the check-in counter.

---

[991] Aviation and Transportation Security Act of 2001, Pub. L. No. 107-71 § 36, 115 Stat. 597, 637 (2001).
[992] UNITED STATES GENERAL ACCOUNTING OFFICE, REPORT TO CONGRESSIONAL COMMITTEES, AVIATION SECURITY COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM FACES SIGNIFICANT IMPLEMENTATION CHALLENGES 6 (GAO Report, February 2004), *available at* www.gao.gov/new.items/d04385.pdf.GAO report, 6.
[993] The Homeland Security Act of 2002, Pub. L. No. 107-296, § 403, 116 Stat. 2135, 2178, transferred TSA from the Department of Transportation to the Department of Homeland Security (DHS).
[994] Aviation and Transportation Security Act, *supra* note 51, at § 101. *See* also Rasmussen, *supra* note 946, at 570.
[995] United States General Accounting Office, *supra* note 992, at 6.
[996] Notice to amend a system of records, 68 Fed. Reg. 2101 (January 15, 2003).
[997] *See* Leigh A. Kite, *Red Flagging Civil Liberties and Due Process Rights of Airline Passengers: Will a Redesigned CAPPS II System Meet the Constitutional Challenge?*, 61 WASH. & LEE L. REV. 1385, 1396 (2004).
[998] United States General Accounting Office, *supra* note 992, at 6.
[999] *Id.* at 7.

Passengers of an acceptable or unknown risk would receive a boarding pass encoded with their risk level so that checkpoint screeners would know the level of scrutiny required. Passengers whose risk assessment is determined to be unacceptable would not be issued boarding passes, and appropriate law enforcement agencies would be notified.[1000] Following CAPPS' fate, CAPPS II was revoked by TSA in August 2004 due to increased civil liberties concerns.[1001]

"Secure Flight" is the successor of CAPPS II, specifically developed to address the problems of its "controversial predecessor".[1002] It was created under the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, through which the Congress mandated TSA to "commence testing of an advanced passenger prescreening system that will allow the Department of Homeland Security to assume the performance of comparing passenger information...to the automatic selectee and no fly lists."[1003] The differences of Secure Flight from CAPPS are not so obvious. According to the Government Accountability Office Report on Secure Flight, the system "among other changes, will only prescreen passengers flying domestically within the United States, rather than passengers flying into and out of the United States.[1004] Also, the CAPPS rules will not be implemented as part of Secure Flight, but rather the rules will continue to be applied by commercial air carriers.[1005] Secure Flight will operate on the Transportation Vetting Platform (TVP) -the underlying infrastructure (hardware and software) to support the Secure Flight application, including security, communications, and data management; and, the Secure Flight application is to perform the functions associated with receiving, vetting, and returning requests related to the determination of whether passengers are on government watch lists."[1006] Under Secure Flight, when a passenger makes a

---

[1000] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, TESTIMONY BEFORE THE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, U.S. SENATE, AVIATION SECURITY, SIGNIFICANT MANAGEMENT CHALLENGES MAY ADVERSELY AFFECT IMPLEMENTATION OF THE TRANSPORTATION SECURITY ADMINISTRATION'S SECURE FLIGHT PROGRAM 7 (GAO Report, February 09, 2006), *available at* http://www.gao.gov/new.items/d06374t.pdf.

[1001] United States General Accounting Office, *supra* note 992, at 42. The GAO Report noted: "Until TSA finalizes its privacy plans for CAPPS II and addresses such concerns, we lack assurance that the system will fully comply with the Privacy Act." *See* also, Ravich, *supra* note 965, at 17–19; Kite, *supra* note 997, at 1401; Ellen Baker, *Flying While Arab- Racial Profiling and Air Travel Security*, 67 J. AIR L. & COM. 1375 (2002).

[1002] Ravich, *supra* note 965, at 20.

[1003] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 102, 118 Stat. 3638, 3715.

[1004] United States Government Accountability Office, *supra* note 1000, at 9.

[1005] *Id.*

[1006] *Id.*

reservation, the system accepting it, such as the air carrier's reservation office or a travel agent, will enter the passenger's PNR data, which will then be stored in the air carrier's reservation system.[1007] The PNR data required by Secure Flight may include information, such as, names, phone numbers, number of bags, seat number, and form of payment.[1008] Approximately 72 hours prior to the flight, portions of the passenger data contained in the PNR will be sent to Secure Flight through a network connection provided by DHS's CBP.[1009] TSA processes the PNR data through the Secure Flight application running on the TVP.[1010] "During this process, Secure Flight is to determine if the passenger data match the data extracted daily from TSC's Terrorist Screening Database (TSDB)—the information consolidated by TSC from terrorist watch lists to provide government screeners with a unified set of terrorist-related information."[1011] TSA will also screen against its own watch list composed of individuals who do not have a nexus to terrorism but who may pose a threat to aviation security.[1012] When the passenger checks in for the flight at the airport, she receives a level of screening based on her designated category. A cleared passenger is to be provided a boarding pass and allowed to proceed to the screening checkpoint in the normal manner. A selectee passenger is to receive additional security scrutiny at the screening checkpoint. A no-fly passenger will not be issued a boarding pass, and law enforcement authorities will be notified.[1013]

Although Secure Flight appears to have removed certain elements criticised in CAPPS II, such as some "computer-based risk assessment algorithms mined from vast commercial databases, in its verification process",[1014] the system has been characterised as "a stripped-down version of the old CAPPS II... with a more consumer-friendly name."[1015] In its 2006 Report on Secure Flight, the United States Government Accountability Office (GAO) concluded that "TSA has not followed a disciplined life cycle approach in developing Secure Flight, in accordance with best practices for large-scale information technology programs."[1016] The programme was

[1007] *Id.*
[1008] *Id.*
[1009] *Id.* at 10.
[1010] *Id.*
[1011] *Id.*
[1012] *Id.*
[1013] *Id.* at 13.
[1014] Dummer, *supra* note 961, at 590.
[1015] Bill Scannell, *TSA Cannot Be Trusted*, USA TODAY (2004).
[1016] United States Government Accountability Office, *supra* note 1000, at 13.

eventually abandoned in 2006,[1017] and the development of subsequent programmes going under the names "Registered Traveller",[1018] and "Trusted Traveller"[1019] were announced.[1020] In August 12, 2009, the TSA announced that it would begin implementing the second phase of the Secure Flight programme in late 2009[1021] and that it expected "all international carriers with direct flights to the U.S. to begin using Secure Flight by the end of 2010."[1022]

2. The EU-US Passenger Name Record (PNR) Agreement: A Chronology

2.1 EU Airlines between a Rock and a Hard Place

The European Union- United States of America Passenger Name Record (PNR) saga began two months after the tragic events of September 11, 2001.[1023] It is a story fraught with a myriad of complex issues: counter-terrorism, air security, human rights, "different cultures of privacy",[1024] European law internal cross-pillar controversies, international aviation law.[1025] It is also fraught with conflicts: security

[1017] Electronic Privacy Information Center, *Spotlight on Surveillance: Secure Flight Should Remain Grounded Until Security and Privacy Problems Are Resolved* (2007).
[1018] Registered Traveller, http://www.tsa.gov/approach/rt/index.shtm (last visited September 20, 2011). According to TSA, Registered Traveler was a pilot programme contracted at 19 airports in July 2008. It was a market-driven venture offered by the private sector in partnership with airports and airlines. *See* also ACLU, *Why the "Registered Traveler" Program Will Not Make Airline Passengers Any Safer* (2006).
[1019] Bruce Schneier, *An Easy Path for Terrorists*, BOSTON GLOBE (2004).
[1020] Rasmussen, *supra* note 946, at 571.
[1021] Press Release, TSA, TSA's Secure Flight Program Enters Next Public Phase, http://www.tsa.gov/press/releases/2009/0812.shtm. *See* also Yevgenia Kleiner, *Racial Profiling in the Name of National Security: Protecting Minority Travelers' Civil Liberties in the Age of Terrorism*, 30 B.C. THIRD WORLD L.J. 103, 134 (2010).
[1022] Press Release, Secretary Napolitano Announces Major Aviation Security Milestone, DHS performs 100 percent watchlist matching for domestic flights, June 7, 2010, *available at* http://www.tsa.gov/press/releases/2010/0607.shtm.
[1023] For a general analysis of the EU-US counter-terrorism cooperation *see* WYN REES, TRANSATLANTIC COUNTER-TERRORISM COOPERATION : THE NEW IMPERATIVE (2006).
[1024] *See* James Q Whitman, *Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE LAW JOURNAL 1151 (2003).
[1025] Pablo Mendes De Leon, *The Fight Against Terrorism Through Aviation : Data Protection Versus Data Production*, XXXI AIR & SPACE LAW 320, 328 (2006).

versus privacy,[1026] US versus EU anti-terrorist legislation, EU versus US legal privacy regime, European Parliament versus Council and Commission, 'commercial processing' of data versus 'law enforcement processing', data protection versus data mining.

The first conflict was faced by European airline companies: violate EU data protection legislation or pay heavy fines and lose landing rights in the US?[1027] More specifically, the Aviation and Transportation Security Act, adopted on November 19, 2001,[1028] required airlines flying into the US territory to transfer to the Commissioner of Customs data relating to passengers and cabin crew (Passenger Manifest Information).[1029] The airlines were also obliged to provide Customs with PNR information upon request.[1030] The purpose was to identify individuals "who may pose a threat to aviation safety or national security".[1031] The Department of Homeland Security (DHS) also passed legislation requiring airlines to make available to US Customs PNR information relating to a passenger's identity and travel plans when that passenger is flying to or from the US.[1032] The information should be transmitted no later than 15 minutes after the departure of the aircraft.[1033] The data transmitted would be stored in the centralized Interagency Border Inspection System ("IBIS") database, which is accessible by more than twenty different agencies including: the Federal Bureau of Investigation, Interpol, Drug Enforcement Agency, Alcohol Tobacco and Firearms, the Internal Revenue Service, the Coast Guard, the Federal Aviation Administration, the Secret Service, and the Animal and Plant Health Inspection Service.[1034] Failure to forward the information required or forwarding incorrect or incomplete information was punishable with loss of landing rights and the

---

[1026] Megan Roos, *Definition of the Problem: The Impossibility of Compliance with Both European Union and United States Law*, 14 TRANSNAT'L L. & CONTEMP. PROBS. 1137, 1138 (2005).
[1027] *Id.* at 1137.
[1028] See above Section 1.3 and in particular note 51.
[1029] 49 U.S.C. § 44909 (Passenger Manifests Law). *See* Article 29 Working Party, *Opinion 6/2002 on Transmission of Passenger Manifest Information and Other Data from Airlines to the United States*, *supra* note 947, at 2.
[1030] *Id.* § 44909(3). According to § 44909(5), information "may be shared with other Federal agencies for the purpose of protecting national security." *See* Roos, *supra* note 1026, at 1139.
[1031] ATSA, 49 U.S.C. § 114 (h) (4).
[1032] Passenger Name Record (PNR) Regulation, 19 C.F.R. § 122.49(a) and 122.49b(2). *See* also Roos, *supra* note 1026, at 1139.
[1033] *Id.* 19 C.F.R. § 122.49a(b) (2)(i).
[1034] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, TERRORIST WATCH LIST SCREENING EFFORTS TO HELP REDUCE ADVERSE EFFECTS ON THE PUBLIC 66 (September 2006), *available at* http://www.gao.gov/new.items/d061031.pdf; Rasmussen, *supra* note 946, at 575.

payment of a fine of up to $ 6000 per passenger whose data had not been appropriately transmitted.[1035]

On the other side of the Atlantic, European airlines had to face EU data protection legislation, and in particular Article 25 (1) of the Data Protection Directive which, in principle, prohibits the transfer of personal data to third countries that do not ensure an "adequate level of protection".[1036] The Directive applies to the data processed by the air carriers, as PNR information is data related to an identified person, and therefore 'personal data';[1037] and, its collection, storage, and transfer to the US authorities constitutes 'processing',[1038] which is 'commercial' and does not fall within the exceptions of Article 3 (2). According to the Data Protection Directive, European airlines can be considered as 'controllers',[1039] and be, therefore, subject to fines from EU National Data Protection Authorities for not respecting their obligations under the Directive.[1040]

European airline companies were, thus, caught between "a rock" (if they followed Community law, they were liable to US sanctions) and "a hard place" (if they gave in to the US authorities' demands, they fell foul of EU data protection requirements),[1041] and the European Commission had to enter the scene.[1042] In June 2002, the Commission informed the US authorities that the PNR data transfers to US law enforcement authorities for counter-terrorism purposes could conflict with Community and Member States' legislation on data protection and with some

---

[1035] ELSPETH GUILD & EVELIEN BROUWER, THE POLITICAL LIFE OF DATA: THE ECJ DECISION ON THE PNR AGREEMENT BETWEEN THE EU AND THE US (CEPS, Policy Brief No. 109, July 2006); Article 29 Working Party, *Opinion 6/2002 on Transmission of Passenger Manifest Information and Other Data from Airlines to the United States*, *supra* note 947, at 4.

[1036] Art. 25 (1) provides: "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place *only if*, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection." Emphasis added. For a more detailed analysis on Article 25 *see* below.

[1037] Art. 2(a) Data Protection Directive.

[1038] Art. 2 (b) Data Protection Directive.

[1039] Art. 2 (d) Data Protection Directive. On the question whether the US authorities could be also considered as 'controllers' under the Directive *see* below.

[1040] On an initial assessment of the data protection problems of the transfer of PNR *see* Article 29 Working Party, *Opinion 6/2002 on Transmission of Passenger Manifest Information and Other Data from Airlines to the United States*, *supra* note 947, at 8–9.

[1041] European Parliament Resolution on transfer of personal data by airlines in the case of transatlantic flights, 13 March 2003, P5_TA(2003)0097. *See* also Guild & Brouwer, *supra* note 1035, at 2.

[1042] ELS DE BUSSER, DATA PROTECTION IN EU AND US CRIMINAL COOPERATION: A SUBSTANTIVE LAW APPROACH TO THE EU INTERNAL AND TRANSATLANTIC COOPERATION IN CRIMINAL MATTERS BETWEEN JUDICIAL AND LAW ENFORCEMENT AUTHORITIES (2009).

provisions of the Regulation on Computerised Reservation Systems (CRSs).[1043] The US authorities accepted to postpone the entry into force of the new requirements only until 5 March, 2003.[1044] The Commission and the US administration entered into negotiations to reach a compromise, and on 18 February 2003, they issued a joint statement, recalling their shared interest in combating terrorism and setting out initial data protection undertakings agreed by US Customs in order to pursue talks with a view to allowing the Commission to make a decision of adequacy of the US privacy regime in accordance with Article 25 (6) of the Data Protection Directive.[1045] As a commentator have cynically noted, "the discussions essentially sought to enhance US data protection standards and reduce those of the EC."[1046]

Meanwhile, the European Parliament and the Article 29 Data Protection Party joined actively the debate on the side of fundamental rights. In two Resolutions, the European Parliament highlighted that that there was "an imperative and urgent need to give passengers, airlines and reservation systems clear indications as soon as possible on which measures are to be taken in response to the demands made by the US authorities",[1047] and criticized the Commission for its 18 February 2003 joint declaration with the US which lacked "any legal basis and could be interpreted as an

---

[1043] Council Regulation (EEC) No 2299/89 of 24 July 1989 on a code of conduct for computerised reservation systems (OJ 1989 L 220, p. 1), as amended by Council Regulation (EC) No 323/1999 of 8 February 1999 (OJ 1999 L 40, p. 1).

[1044] It should not go unnoticed that since then (and before the entry into force of the first PNR Agreement on 28 May 2004) European airlines were providing to the US authorities access to PNR data.

[1045] EUROPEAN COMMISSION/US CUSTOMS TALKS ON PNR TRANSMISSION BRUSSELS, 17/18 FEBRUARY JOINT STATEMENT, *available at* http://ec.europa.eu/transport/air_portal/security/doc/prn_joint_declaration_en.pdf. The Joint Statement demonstrates that "The two sides agreed to take all necessary steps as quickly as possible to reconcile and respect fully legal obligations on both sides leading towards mutually satisfactory solution, providing legal certainty." In particular, they "agreed to work together towards a bilateral arrangement under which the Commission, in response to information and undertakings provided by the US side about the way transferred data would be handled and protected in the US, will adopt a decision under Article 25 paragraph 6 of the Data Protection Directive. The information and undertakings would reflect existing law and practice, coupled if necessary with additional undertakings especially as regards the necessity and proportionality of data processing. Such a decision will provide legal certainty in particular as regards the international transfer aspects of the transmission of PNR data. It was agreed that the information and undertakings to be provided would need to cover in particular: definition of the purposes for which the data will be used and limitation of use to these purposes; conditions and limits of data sharing and onward transfer; protection of data from unauthorised access; duration and conditions of data storage; additional measures for the protection of sensitive data; remedies for passengers, including possibilities to review and correct data held by US Customs; reciprocity."

[1046] I. Ntouvas, *Air Passenger Data Transfer to the USA: The Decision of the ECJ and Latest Developments*, 16 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 73, 79 (2007).

[1047] European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA, 9 October 2003, P5_TA(2003)0429, ¶ E.

indirect invitation to the national authorities to disregard Community law".[1048] Nevertheless, accepting the need for negotiations in order to ensure genuine cooperation with the US authorities,[1049] it called for an Agreement where: 1) there is no discrimination against non-US passengers and no retention of data beyond the length of a passenger's stay on US territory; 2) passengers are provided with full and accurate information before purchasing their ticket and give their informed consent regarding the transfer of such data to the USA; and, 3) passengers have access to a swift and efficient appeals procedure, should any problem arise.[1050] Similar concerns were also raised by the Art.29 Working Party in a series of Opinions it issued since the EU-US PNR conflict broke out.[1051]

2.2 Appeasing the conflict: The 2004 PNR Agreement

Amidst the complaints of the Parliament and the Working Party, the Commission announced,[1052] on 16 December 2004, "the successful conclusion of negotiations."[1053] The Commission contended that the result reflected a "balanced, integrated, multi-strand approach."[1054] The draft decision on adequacy, alongside

[1048] European Parliament Resolution on transfer of personal data by airlines in the case of transatlantic flights, 13 March 2003, *supra* note 99, para 3.
[1049] European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA, 9 October 2003, *supra* note 102, para 3.
[1050] *Id.*, para 3 (a).
[1051] *See* Article 29 Working Party, *Opinion 6/2002 on Transmission of Passenger Manifest Information and Other Data from Airlines to the United States*, *supra* note 8; EUROPEAN DATA PROTECTION AUTHORITIES, OPINION ON THE TRANSFER OF PASSENGERS' DATA TO THE UNITED STATES, 17.6.2003; ARTICLE 29 WORKING PARTY, OPINION 2/2004 ON THE ADEQUATE PROTECTION OF PERSONAL DATA CONTAINED IN THE PNR OF AIR PASSENGERS TO BE TRANSFERRED TO THE UNITED STATES' BUREAU OF CUSTOMS AND BORDER PROTECTION (US CBP).
[1052] *See* Address of Frits Bolkestein (Member of the European Commission in charge of the Internal Market, Taxation and Customs) to European Parliament Committees on Citizens ' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market, EU/US talks on transfers of airline passengers' personal data SPEECH/03/613 of 16 December 2003.
[1053] *Id.* Bolkestein noted:"Those talks have now been completed – as I promised Parliament they would be "before Christmas". And today the Commission exercised its "political judgement" in deciding how to take matters forward." Ntouvas, *supra* note 1046, at 80.
[1054] *Id.* According to Commissioner Bolkestein, the main improved undertakings that the Commission secured since the beginning of the talks were: "Firstly, clear limits on the amount of data to be transferred with a closed list of 34 elements. Secondly, a significant movement on the length of data storage. The US has agreed to cut its initially proposed fifty year period to 3 ½ years. The third important success we achieved is that the arrangement will not cover the US Computer Assisted Passenger Pre-Screening System (CAPPS II). Fourthly, we obtained stronger guarantees with respect to overall US compliance. The US finally accepted – after refusing it earlier in our talks – an important safeguard in the form of a joint review, to be carried out together with EU authorities at least every year. The fifth useful development regards redress for individual EU

with the draft CBP Undertakings attached to it, was placed before the Parliament on 1 March 2004. In its Resolution of 31 March 2004, the European Parliament criticised heavily the draft decision on adequacy.[1055] Having noted its regret on "the fact that, throughout 2003, the Commission did not heed the repeated requests from Parliament and the data-supervision authorities",[1056] it stated that the draft decision "goes beyond the executive powers conferred on the Commission."[1057] In fact, according to the Parliament the draft decision "is not (and could not be) a legal basis capable of enabling, within the European Union, the purpose for which the data were collected in the PNR to be changed and enabling them to be transferred by the airlines, in whole or in part, to third parties; its effect, however, may well be a lowering of the data-protection standards established by means of Directive 95/46/EC within the EU or the creation of new standards in agreement with third countries."[1058] The EP expressed its doubts also concerning the binding nature of the "US Undertakings" and the use of the "pull" system for the transmission of the data,[1059] and concluded by calling upon the Commission to withdraw its draft decision on adequacy.[1060]

Notwithstanding this, the Commission adopted on 14 May 2004 a decision, on the basis of Article 25 (6) of the Data Protection Directive, confirming 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.[1061] Upon the Commission's decision on the adequacy of the protection of personal data in the US, the Council adopted on 17 May 2004 a decision authorising the conclusion of an agreement between the EC and the US on the transfer of PNR data by air carriers to the US DHS, Bureau of Customs and Border Protection.[1062] The legal basis for the

---

passengers. Finally, all categories of sensitive data will be deleted, and there will be no bulk sharing of data with other agencies."

[1055] European Parliament resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (2004/2011(INI)), P5_TA(2004)0245.

[1056] *Id.,*at K.

[1057] *Id.,*at 1.

[1058] *Id.,*at 1.1 (a).

[1059] *Id.,*at 1.2 and 1.3.

[1060] *Id.,*at 10.

[1061] Commission Decision 2004/535/EC 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, p. 11.

[1062] Council Decision 2004/496/EC 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 2004 L 183, p. 83, and corrigendum at OJ 2005 L 255, p. 168.

Council's decision was Article 95 EC in conjunction with the first sentence of the first subparagraph of Article 300 (2).[1063] On 28 May 2004, an Agreement permitting the transfer of PNR data to the United States was signed in Washington DC.[1064] The Agreement entered into force the same day.[1065]

2.2.1 Examining the adequacy of the Commission's adequacy decision

It should be stated from the outset that the Commission's adequacy decision is based on the assumption (proved wrong later by the ECJ)[1066] that the transfer of PNR data by European air carriers to the US authorities constitutes commercial processing, therefore it is a matter falling within Community law (former First Pillar), and the Data Protection Directive applies.[1067] That being said let us take a closer look to the 'adequacy requirement' and the decision itself. Simply put, the 'adequacy' requirement means that personal data cannot travel to third countries that do not offer an 'adequate' level of protection.[1068] What are the criteria that determine an adequate level of protection? According to the Data Protection Directive:

[1063] It reads as follows "[...] the conclusion of the agreements shall be decided on by the Council, acting by a qualified majority on a proposal from the Commission." The Council noted in Recital 2 of the decision that "the European Parliament has not given an Opinion within the time-limit which, pursuant to the first subparagraph of Article 300(3) of the Treaty, the Council laid down in view of the urgent need to remedy the situation of uncertainty in which airlines and passengers found themselves, as well as to protect the financial interests of those concerned." Article 300 (3) provides: "The Council shall conclude agreements after consulting the European Parliament […]. The European Parliament shall deliver its opinion within a time-limit which the Council may lay down according to the urgency of the matter. In the absence of an opinion within that time limit, the Council may act." On the PNR case, on 28 April 2004 the Council, on the basis of the first subparagraph of Article 300(3) EC, sent a letter to the Parliament asking it to deliver its opinion on the proposal for a decision relating to the conclusion of the Agreement by 5 May 2004. On 4 May 2004 the Parliament rejected the Council's request to it of 28 April for urgent consideration of that proposal, after taking note of the continuing lack of all the language versions of the proposal for a Council decision. The Council final adopted its decision on 17 May 2004. On 4 June 2004, the Presidency-in-Office of the Council informed the Parliament by letter that Decision 2004/496 took into account the fight against terrorism – a priority of the Union – but also the need to address the uncertain legal situation of air carriers as well as their financial interests.

[1064] 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.

[1065] *Id.,* para 7.

[1066] *See* below.

[1067] Vagelis Papakonstantinou & Paul de Hert, *The PNR Agreement and Transatlantic Anti-Terrorism Co-operation: No Firm Human Rights Framework on Either Side of the Atlantic*, 46 COMMON MARKET LAW REVIEW 885, 901 (2009).

[1068] *See* Article 25 (1) of the Data Protection Directive, *supra* note 2. A similar rule exists for the former third pillar as Article 13 (1) (d) provides: "Member States shall provide that personal data transmitted

> "The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied within that country."[1069]

The 'adequacy requirement' has been characterised as "notorious" "regulatory "gunboat diplomacy"."[1070] An examination of the Commission's adequacy decision in the PNR case, however, hardly justifies such a characterisation. Essentially, the Commission seems to be finding what it wants to find in the CPB Undertakings.[1071] Its assessment of the data protection principles affected by the transfer of PNR data is somewhat superficial: As regards the purpose limitation principle, air passengers' personal data will be processed for a specific purpose because they will be used strictly for purposes of preventing and combating terrorism and related crimes, other serious transnational crimes, and flight from warrants or custody for those crimes.[1072] As regards the proportionality principle, a maximum of 34 PNR data categories will be transferred; and PNR will be deleted after a maximum of three years and six months, with exceptions for data that have been accessed for specific investigations, or otherwise manually accessed.[1073] As regards the transparency principle, CBP will provide information to travellers as to the purpose of the transfer and processing, and the identity of the data controller in the third country, as well as other information.[1074]

---

or made available by the competent authority of another Member State may be transferred to third States or international bodies, only if: (d) the third State or international body concerned ensures an adequate level of protection for the intended data processing."

[1069] Article 25 (2) Data Protection Directive.

[1070] Papakonstantinou & de Hert, *supra* note 1067, at 899; Paul De Hert & Bart de Schutter, *International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift*, JUSTICE, LIBERTY, SECURITY : NEW CHALLENGES FOR EU EXTERNAL RELATIONS 303, 315–316 (Bernd Martenczuk & Servaas Van Thiel, 2008).

[1071] *See* Recital 14 of the Commission decision on adequacy. "The standards by which CBP will process passengers' PNR data on the basis of United States legislation and the Undertakings cover the basic principles necessary for an adequate level of protection for natural persons."

[1072] Recital 15 of the Commission adequacy decision.

[1073] Recital 16 of the Commission adequacy decision.

[1074] Recital 17 of the Commission adequacy decision.

Notwithstanding this, it is clear from the decision that the Commission regards its adequacy finding as not permanent and rebuttable.[1075] This means that the competent authorities in Member States may suspend data flows to CBP where a competent United States authority has determined that CBP is in breach of the applicable standards of protection; or where there is a substantial likelihood that the standards of protection agreed with CBP are being infringed, there are reasonable grounds for believing that CBP is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects, and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide CBP with notice and an opportunity to respond.[1076] Furthermore, if the basic principles necessary for an adequate level of protection are no longer being complied with, or any body responsible for ensuring compliance with the standards of protection by CBP, the Commission has the right to repeal or suspend its adequacy decision.[1077] Finally, the Commission's adequacy finding applies for a period of three and six months, after which the PNR Agreement should be renegotiated.[1078]

Following the Commission's finding of adequacy, the Council's decision is laconic. In only two Articles the Council solemnly announces that the Community approves the conclusion of the Agreement for the transfer of PNR data to the US authorities.[1079] The same applies to the Agreement between EU and US for the transfer of PNR data. It contains merely seven Articles and makes reference to the Commission's adequacy decision and the Undertakings.[1080]

2.2.2 Making sense of the CBP Undertakings

Annexed to the Commission's decision are the forty-eight CBP Undertakings that illustrate how PNR data would be used.[1081] The Undertakings include provisions

[1075] *See* Article 5 of the Commission adequacy decision.
[1076] Article 3 (1) of the Commission adequacy decision.
[1077] Article 4 (3) of the Commission adequacy decision.
[1078] Article 7 of the Commission adequacy decision.
[1079] Article 1 of the Council's decision on the conclusion of the Agreement.
[1080] Article 3 of the Agreement.
[1081] *See* Irfan Tukdi, *Transatlantic Turbulence: The Passenger Name Record Conflict*, 45 HOUS. L. REV. 587, 601 (2008).

of substantial nature that regulate in essence the details of the DHS processing; for this reason, their implementation was central for the adoption of the adequacy decision.[1082] Their legal nature, however, is far from clear. In the Commission's own words the Undertakings "have varying degrees of legal effect."[1083] This is because they are incorporated in a variety of different legal documents: statutes, regulations, directives or other policy instruments in the United States.[1084] Nevertheless, because the Undertakings are to be published in full in the Federal Register under the authority of the DHS, the Commission considers that "they represent a serious and well considered political commitment on the part of the DHS."[1085] This is certainly not very reassuring for a number of reasons. First of all, political commitments do not have the binding nature and the enforceability of legal obligations. The Working Party at its 2/2004 Opinion was categorical about this point: "It is clear that the US undertakings will not be legally binding on the US side."[1086] A closer look at Undertaking 47 confirms this: "these Undertakings do not create or confer any right or benefit on any person or party, private or public". Moreover, individuals lack legal certainty on how to challenge the measures since they are enshrined in legal texts of different nature. The Commission's assertion, therefore, that non-compliance "could be challenged through legal, administrative and political channels"[1087] seems rather difficult to take place in practice.

As discussed above, the European Parliament had echoed similar concerns about the Undertakings in its Opinion regarding the draft decision. The Parliament was both concerned on the source and the substance of the Undertakings: on the one hand, the source is "purely administrative and therefore subject to possible re-organisations within the DHS; on the other hand, on the substance, "guarantees are mentioned for which there is no legal basis in the USA, and the option is kept open of amending rules at any time, with particular reference to the arrangements for using and re-using the data."[1088] In the same tone, the Working Party had warned:

[1082] Papakonstantinou & de Hert, *supra* note 1067, at 905.
[1083] Recital 13 of the Commission adequacy decision.
[1084] *Id.*
[1085] *Id.*
[1086] Article 29 Working Party, *Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)*, *supra* note 1051, at 5.
[1087] Recital 13 of the Commission adequacy decision.
[1088] European Parliament Resolution, *supra* note 113, at 1.2.

"...any Commission decision should not rest on mere "undertakings" of administrative agencies, but on commitments that are officially published at least at the level of the Federal register and fully binding on the US side. In particular, there should be no ambiguity about the capability to create rights in favour of third parties."[1089]

On the substance, the Undertakings purport to convince on the commitments assumed by the CBP for the use of the PNR data. CBP requires access to thirty-four categories of data,[1090] even if it "believes that it will be rare that an individual PNR will include a full set of the identified data."[1091] The PNR data will be used for three purposes: preventing and combating 1) terrorism and related crimes, 2) other serious crimes, including organised crime, that are transnational in nature, and 3) flight from warrants or custody for the crimes described above.[1092] CBP will not use "sensitive" data,[1093] and it will implement "an automated system which filters and deletes certain "sensitive" PNR codes and terms."[1094] With regard to the method of accessing the PNR data, CBP will "pull" passenger information from air carrier reservation systems until such time as air carriers are able to implement a system to "push" the data.[1095] CBP will pull the data 72 hours prior to the departure of the flight, and can re-check them for another three times since the initial pull.[1096] PNR data can be accessed by authorized CBP users for a period of three years and six months, unless they are manually consulted. In this case, they will be kept for another eight years in a deleted

[1089] Article 29 Working Party, *Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)*, *supra* note 1051, at 5.
[1090] The data elements are listed in Attachment A of the CBP Undertakings. They comprise: 1) PNR record locator code; 2) Date of reservation; 3) Date(s) of intended travel; 4) Name; 5) Other names on PNR; 6) Address; 7) All forms of payment information; 8) Billing address; 9) Contact telephone numbers; 10) All travel itinerary for specific PNR; 11) Frequent flyer information (limited to miles flown and address(es)); 12) Travel agency; 13) Travel agent; 14) Code share PNR information;
15) Travel status of passenger; 16) Split/divided PNR information; 17) E-mail address; 18) Ticketing field information; 19) General remarks; 20) Ticket number; 21) Seat number ; 22) Date of ticket issuance; 23) No show history; 24) Bag tag numbers; 25) Go show information; 26) OSI information; 27) SSI/SSR information; 28) Received from information; 29) All historical changes to the PNR; 30) Number of travellers on PNR; 31) Seat information; 32) One-way tickets; 33) Any collected APIS (Advanced Passenger Information System) information; and, 34) ATFQ (Automatic Ticketing Fare Quote) fields.
[1091] Undertaking 4.
[1092] Undertaking 3.
[1093] Undertaking 9.
[1094] Undertaking 10.
[1095] Undertaking 13.
[1096] Undertaking 14.

record file.[1097] CBP will provide, in its discretion, PNR data to other government authorities, including foreign government authorities, with counter-terrorism or law-enforcement functions, on a case-by-case basis, for purposes of preventing and combating criminal offences.[1098] The data may also be disclosed in any criminal judicial proceedings or as otherwise required by law.[1099] CBP will provide information to the travelling public regarding the transfer of its PNR data to the US authorities and its use,[1100] and it will rectify the data at the request of the data subject.[1101] Finally, CBP and European Commission will jointly review implementation of the Undertakings.[1102]

2.3 The end of the reconciliation period: The ECJ *PNR* decision and "the decline and fall"[1103] of the 2004 Agreement

While the dilemma faced by the European airlines caused by the conflict between US counter-terrorism policies and EU data protection legislation seemed to calm down after the 2004 PNR Agreement, another controversy emerged. This time the conflict was an internal, European one: the European Parliament sought the annulment before the ECJ of both the Commission's adequacy decision and the Council's decision approving the signing of the Agreement.[1104] As it is noted astutely in the House of Lords Report, "the Parliament's quarrel was in fact not so much with the legality of [...] the Decision[s] as with the substance of the data protection undertakings, which the Parliament regarded as inadequate. The proposal to link a

[1097] Undertaking 15.
[1098] Undertaking 29.
[1099] Undertaking 35.
[1100] Undertaking 36. According to Undertaking 37, Requests by the data subject to access her PNR data will fall under the Freedom of Information Act (FOIA).
[1101] Undertakings 39, 40.
[1102] Undertaking 43. Such joint review was carried out in 2005 and its report was issued on 12 December 2005. *See* COMMISSION STAFF WORKING PAPER, 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, WASHINGTON, 20-21 SEPTEMBER 2005 (COM (2005) final, December 12, 2005).
[1103] *See* House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, *supra* note 945, at 21.
[1104] Joined Cases C-317/04 and C-318/04, *European Parliament* v. *Council and Commission (PNR)*, Judgment of the Grand Chamber of 30 May 2006, [2006] ECR I-4721.

challenge to the legality of the Decision[s] with its main complaint on the substance proved fatal to its case."[1105]

Let us take the story from the beginning. On 27 July 2004, the Parliament filed an action of annulment of the Commission's adequacy decision (Case C-318/04), based on four pleas: 1) the adoption of the Commission's decision was *ultra vires* because the provisions laid down in the Data Protection Directive were not complied with; 2) The adequacy decision breached the fundamental principles of the Data Protection Directive; 3) it infringed fundamental rights, and in particular the right to privacy; and 4) it breached the principle of proportionality.[1106] In its action against the Council's decision on the conclusion of the Agreement (Case C-317/04), the Parliament advanced six pleas for annulment: 1) incorrect choice of Article 95 EC as legal basis; 2) infringement of the second subparagraph of Article 300(3) EC; 3) infringement of the right to protection of personal data; 4) breach of the principle of proportionality; 5) lack of a sufficient statement of reasons for the decision at issue; and 6) breach of the principle of cooperation in good faith laid down in Article 10 EC.[1107]

2.3.1 The Opinion of the Advocate General

In his Opinion, Advocate General Léger argued that the Commission's adequacy decision was excluded *ratione materiae* from the scope of the Data Protection Directive, because the use by CBP and the making available to the latter of air passenger data from air carriers' reservation systems constitute data processing operations which concern public security and relate to State activities in areas of criminal law.[1108] This is supported by the wording of the adequacy decision, which provides that PNR data will be used strictly for purposes of preventing and combating: terrorism and related crimes; other serious crimes, including organised crime, that are transnational in nature; and flight from warrants or custody for those

[1105] House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, *supra* note 945, paragraph 52.
[1106] Joined Cases C-317/04 and C-318/04 *(PNR), supra* note 162, para 50.
[1107] Joined Cases C-317/04 and C-318/04 *(PNR), supra* note 162, para 62.
[1108] Opinion of Advocate General Léger, Joined Cases C-317/04 and C-318/04 , delivered on 22 November 2005, para 97.

crimes.[1109] The Advocate General admitted that "the processing constituted by the collection and recording of air passenger data by airlines has, in general, a commercial purpose in so far as it is connected with the operation of the flight by the air carrier", and consequently the PNR data initially collected by airlines fall within the scope of Community law; he noted, however, that the data processing which is taken into account in the adequacy decision "is quite different in nature, since it covers a stage subsequent to the initial collection of the data."[1110] In fact, the adequacy decision does not concern a data processing operation necessary for a supply of services, but one regarded as necessary to safeguard public security and for law enforcement purposes. That is the purpose of the transfer and the processing of PNR data. Consequently, according to the Advocate General, the fact that personal data have been collected in the course of a business activity cannot, justify the application of the Data Protection Directive.[1111]

Along similar lines, the Advocate General rejected Article 95 as the appropriate legal basis for the adoption of the Council's decision on the conclusion of the PNR Agreement.[1112] Article 95(1) EC concerns the adoption by the Council of measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market. Even if the PNR Agreement with the US could be accepted to remove "any distortion of competition between the Member States' airlines and between the latter and the airlines of third countries";[1113] this purpose was "*incidental in character* to the two main objectives of combating terrorism and other serious crimes and protecting passengers' personal data"[1114] According to the "centre of gravity" theory applied by the Court, if a Community measure pursues more than one purpose, and if one is identifiable as the main or predominant purpose, whereas the other is merely incidental, the measure must be founded on a single legal basis, namely that required by the main or predominant purpose or component.[1115] The Advocate General, considered therefore, that since the principle aim and content of

[1109] *Id.,* at para 99.
[1110] *Id.,* at para 102.
[1111] *Id.,* at para 103.
[1112] *Id.,* at para 140.
[1113] *Id.,* at para 144.
[1114] *Id.,* at para 147.
[1115] *Id.,* at para 154.

the agreement were not about the functioning of the internal market, Article 95 EC was not the correct legal basis for its adoption.[1116]

Advocate General Léger also dealt with the Parliament's plea alleging an infringement of fundamental rights, in particular privacy and data protection. The way he viewed the two rights will be discussed in detail below, because it is very relevant to the argument advanced by the present thesis. For the time being, however, we can take a closer look at his analysis regarding the infringement of the right to privacy. The Advocate General followed the usual formula employed by the ECtHR, and having established an interference with the right to privacy, he went on to examine whether this was disproportionate by looking whether the requirements "in accordance with the law", "legitimate aim", and "necessary in a democratic society" were complied with. Concerning the "in accordance with the law" requirement, and in particular the "accessibility" and "foreseeability" requirement, the Advocate General was satisfied that it was complied with because "the airlines covered by the PNR regime are informed of the obligations imposed on them under the agreement, and airline passengers are informed of their rights, in particular as regards access to and rectification of data."[1117] Furthermore, the interference pursued the aim of combating terrorism, which is a legitimate aim.[1118] As regards his analysis on the necessity requirement, the Advocate General held:

> "In the light of the nature and importance of the objective of combating terrorism, [...], and having regard to the politically sensitive context in which the negotiations between the Community and the United States were conducted, I am of the opinion that, in this case, the Court should hold that the Council and the Commission had a wide margin of appreciation in negotiating, with the US authorities, the content of the PNR regime. It follows that, in order to respect that wide margin of appreciation, the Court's review of the necessity of the interference should, in my view, be limited to determining whether there was any manifest error of assessment on the part of those two institutions. By carrying out a restricted review of that kind, the Court would thus avoid the pitfall of substituting its own assessment for that of the Community political

[1116] *Id.,* at para 155.
[1117] *Id.,* at para 219.
[1118] *Id.,* at para 222.

authorities as to the nature of the most appropriate and expedient means of combating terrorism and other serious crimes."[1119]

The Advocate General asked the Court to respect the principle of the separation of powers,[1120] and argued that the list of 34 PNR data was not excessive as "the need to profile potential terrorists may require access to a large number of pieces of data;"[1121] and the period of storage of the PNR data for three years and six months did not constitute a patent infringement of the right to privacy "bearing in mind in particular the fact that [...] investigations which may be conducted following terrorist attacks or other serious crimes sometimes last several years."[1122] Therefore, he concluded that "the Council and the Commission did not exceed the limits placed on their margin of appreciation when adopting the PNR regime."[1123]

2.3.2 The judgment of the Court

On 30 May 2006 the ECJ delivered its judgment in the PNR case. In a rather uninspired reasoning, the Court agreed with the Advocate General that the Commission's adequacy decision was not adopted on the correct legal basis,[1124] because the transfer of PNR data to CBP did not constitute processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes,[1125] and therefore did not fall within the scope of the Data Protection Directive, pursuant to the provision of Article 3 (2).[1126] The ECJ reached the same conclusion concerning the Council's decision. "In an exercise of remarkable verbal economy",[1127] it decided that Article 95 EC could not justify Community competence to conclude the Agreement,[1128] because this related to

[1119] *Id.,* at para 231.
[1120] *Id.,* at para 233.
[1121] *Id.,* at para 238.
[1122] *Id.,* at para 242.
[1123] *Id.,* at para 254.
[1124] Joined Cases C-317/04 and C-318/04 *(PNR), supra* note 162, para 60.
[1125] *Id.,* at para 57.
[1126] *Id.,* at para 59.
[1127] Jorrit J. Rijpma & Gráinne Gilmore, *Joined Cases C-317/04 and C-318/04, European Parliament V. Council and Commission, Judgment of the Grand Chamber of 30 May 2006, [2006] ECR I-4721*, 44 COMMON MARKET LAW REVIEW 1081, 1087 (2007).
[1128] Joined Cases C-317/04 and C-318/04 *(PNR), supra* note 162, para 67.

"the same transfer of data as the decision on adequacy and therefore to data processing operations which [...] are excluded from the scope of the Directive."[1129]

The ECJ therefore annulled both the Commission's adequacy decision[1130] and the Council's decision on the conclusion of the Agreement.[1131] It was very careful, however, concerning the implications of its judgment.[1132] Having noted that under paragraph 7 of the Agreement, either party may terminate the Agreement at any time and the termination takes effect 90 days from the date of notification of termination to the other party,[1133] it decided to preserve the effect of the adequacy decision for 90 days, until 30 September 2006, in order to allow the political institutions to negotiate a new arrangement.

The judgment of the Court of Justice brought about new problems and controversies.[1134] The European Parliament welcomed the annulment of the Council and the Commission decision,[1135] but regretted that the Court did not respond to its concerns about the legal structure of the agreement and the congruency of its content with the data protection principles.[1136] In fact, the decision of the Court has been characterised as a "Pyrrhic victory"[1137] for the European Parliament. The annulment of the Community instruments as a basis for the PNR transfer, meant that the Agreement had to be renegotiated within the framework of the (former) third pillar, with all the consequences therein, among which, the limited role of the European Parliament itself.[1138] For the European Data Protection Supervisor, therefore, the

---

[1129] *Id.,* at para 69.
[1130] *Id.,* at para 61.
[1131] *Id.,* at para 70.
[1132] Rijpma & Gilmore, *supra* note 1127, at 1097.
[1133] Joined Cases C-317/04 and C-318/04 *(PNR), supra* note 162, para 71.
[1134] *See* in general Mario Mendez, *Passenger Name Record Agreement – European Court of Justice*, 3 EUROPEAN CONSTITUTIONAL LAW REVIEW (EUCONST) 127 (2007); Guild & Brouwer, *supra* note 1035, at 3; Marco Botta & Mario Viola de Azevedo Cunha, *La Protezione Dei Dati Personali Nelle Relazioni Tra Ue E Usa, Le Negoziazioni Sul Trasferimento Dei Pnr*, XXVI IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA 315, 326 (2010).
[1135] EUROPEAN PARLIAMENT, COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, REPORT 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 (2006/2193(INI)) 4 (July 19, 2006).
[1136] *Id.*
[1137] Rijpma & Gilmore, *supra* note 1127, at 1081.
[1138] According to Christopher Patton, Johannes Voggenhuber, a Member of the European Parliament, made the following observation regarding the 2006 PNR Agreement: "Today we are looking at an agreement under the third pillar, no public debate, no role of [European Parliament], no ratification of national parliaments... it continues to be a transfer of data outside the protection of the law." *See* Christopher Patton, *No Man's Land: The EU-U.S. Passenger Name Record Agreement*

judgment created "a loophole in the protection of European citizens whereby their data are used for law enforcement purposes."[1139] Along the same lines, for the Article 29 Working Party, the Court's ruling showed "once more the difficulties arising from the artificial division between the pillars and the need for a consistent cross pillar data protection framework."[1140]

The Court seemed to have gotten it wrong everywhere. On the pillars issue, "the PNR case is a good example of the difficulty of allocating an international agreement to the correct legal base (and pillar), and of the consequences of getting it wrong."[1141] On the distinction between 'commercial' and 'law enforcement' processing, despite the efforts of the Court to distinguish the two, it failed ultimately to place the two Community measures under their corresponding processing regime.[1142] The EC had nothing to do with the law enforcement processing of the PNR data. That was a demand by the US; the data would be used for counter-terrorism and law enforcement purposes only there. The EU data protection regime governed the initial processing of the data by the air carriers for commercial purposes.[1143] As regards the EU's external relations, the judgment illustrated to what extent EU internal inter-institutional and cross pillar conflicts can affect its "capacity

---

and What It Means for the European Union's Pillar Structure, 40 GEO. WASH. INT'L L. REV. 527, 539–540 (2008).

[1139] European Data Protection Supervisor, *PNR: EDPS First Reaction to the Court of Justice Judgment*, PRESS RELEASE (2006).

[1140] ARTICLE 29 WORKING PARTY, OPINION 5/2006 ON THE RULING BY THE EUROPEAN COURT OF JUSTICE OF 30 MAY 2006 IN JOINED CASES C-317/04 AND C-318/04 ON THE TRANSMISSION OF PASSENGER NAME RECORDS TO THE UNITED STATES 3.

[1141] MARISE CREMONA, EU EXTERNAL ACTION IN THE JHA DOMAIN: A LEGAL PERSPECTIVE 17 (EUI Working Papers LAW 2008/24).

[1142] De Hert and de Schutter note "From a legal point of view, the European Court of Justice has been clear in its judgment: the only factor to take into account in order to determine the scope of the data processing is the nature of *the processing* itself, as opposed to the origin of the data." *See* De Hert & de Schutter, *supra* note 1070, at 330.

[1143] *See* Edward Harris, *Tradeoffs in Personal Data Privacy: A Swedish Church Lady, Austrian Public Radio Employees and Transatlantic Air Carriers Show That Europe Does Not Have the Answers*, 22 AMERICAN UNIVERSITY INTERNATIONAL LAW REVIEW 745, 791–792 (2007). Harris notes: "Although the Court took pains to distinguish the processing activities of the commercial airlines from the processing that took place pursuant to the security/ criminal law framework put into place by public authorities, the security/ criminal law framework was not that of the EU but, rather of the United States... It was therefore not a European security/ criminal law framework under which the decisions of the Commission and the Council were made and thus they should not have been excluded from the Directive's scope. The Commission's motivation in negotiating any agreement with the United States for the sharing of PNR data seems to have been primarily to preserve the privacy protections of the EU citizens and avoid negative economic consequences to the commercial interests of EU air carriers and the travelling public. The aims of the Commission and the Council in proceeding as they did on the PNR issue appear to be more related to commerce than to security and criminal law. "

to conduct meaningful relations with third countries."[1144] Finally, on the balance between fundamental rights and counter-terrorism/ law enforcement requirements, the Court got the worst of both worlds - even if, in practice it did not pronounce on the issue. On the one hand, not only the question on the potential fundamental rights infringements by the PNR Agreement remained unanswered by the Court, despite being the Parliament's main plea; but also the fundamental rights ramifications of the judgment were severe: a new Agreement had to be negotiated under a framework with significantly reduced fundamental rights' protection compared to the one of the Community. On the other hand, as Americans complained "by nullifying the decisions of the Commission and the Council, the ECJ has essentially sacrificed the security of both the United States and the European Union."[1145] According to this argument, if the PNR data is made unavailable to the United States, "the United States will lack an important tool in combating crime and terrorism which may lead to a less secure environment" for both the US and the EU.[1146]

It appears that the ECJ *PNR* judgment negatively affected all the above mentioned issues. As Bruno de Witte astutely noted "there are ... cases in which a court action seemed to raise important questions of constitutional substance, but where the ECJ judgment disappointingly remains focused on the more arcane institutional issues. This happened in the Passenger Name Records judgment of June 2006."[1147]

2.4 A "small legal war":[1148] the Interim PNR Agreement

Following the Court of Justice decision, there was one path to be taken by Council and Commission: the denunciation of the 2004 Agreement. Indeed, on 3 July 2006, the Council and the Commission notified the US government that the PNR

[1144] Rijpma & Gilmore, *supra* note 1127, at 1096; Vanessa Serrano, *Comment: The European Court of Justice's Decision to Annul the Agreement Between the United States and European Community Regarding the Transfer of Personal Name Record Data, Its Effects, and Recommendations for a New Solution*, 13 ILSA J. INT'L & COMP. L. 453, 468 (2007).
[1145] Harris, *supra* note 1143, at 793.
[1146] *Id.* at 794.
[1147] See Bruno de Witte, *Too Much Constitutional Law in the European Union's Foreign Relations?*, EU FOREIGN RELATIONS LAW : CONSTITUTIONAL FUNDAMENTALS 3, 11 (Marise Cremona & Bruno de Witte, 2008).
[1148] Arthur Rizer, *Dog Fight: Did the International Battle over Airline Passenger Name Records Enable the Christmas-Day Bomber*, 60 CATH. U. L. REV. 77, 78 (2010).

Agreement had to be terminated with effect from 30 September 2006.[1149] On 27 June 2006, the EU entered a second round of negotiations with the US administration to conclude a new PNR Agreement, under the (former) third pillar. The actors conducting the negotiations on the EU's side were different this time. Instead of the Commission authorised by the Council in the 2004 PNR Agreement, now it was the Presidency, assisted by the Commission, according to Article 24 (1) TEU.[1150] On 6 October 2006 negotiations were completed and on 16 October 2006, the Council authorised the Presidency to sign the Agreement reached with the US.[1151] The Agreement was signed on behalf of the US at Washington DC on 19 October 2006 and applied provisionally from the same date.[1152] The Agreement, unless otherwise terminated, would remain into force until 31 July 2007.[1153]

The 2006 Interim Agreement comprises of seven points and does not seem to add anything to its 2004 predecessor, had it not been for Point 1 which states:

> "In reliance upon DHS's continued implementation of the aforementioned Undertakings *as interpreted in the light of subsequent events*, the European Union shall ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America process PNR data contained in their reservation systems as required by DHS."[1154]

The phrase "as interpreted in the light of subsequent events" refers to the letter sent by Stewart Baker, Assistant Secretary for Policy at the DHS, to the Presidency and the Commission "concerning the interpretation of certain provisions of the undertakings issued by DHS on 11 May 2004 in connection with the transfer

---

[1149] Council Notice concerning the denunciation of the 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 C219/1 of 12 September 2006.

[1150] Article 24 (1) TEU provides: "When it is necessary to conclude an agreement with one or more States… in implementation of this title, the Council may authorise the Presidency, assisted by the Commission as appropriate, to open negotiations to that effect. Such agreements shall be concluded by the Council on a recommendation from the Presidency."

[1151] 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, OJ L 298/27 of 27 October 2006.

[1152] *See* Point 7 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, OJ L 298/29 of 27 October 2006 and Article 3 of Council Decision 2006/729/CFSP/JHA.

[1153] *Id.*

[1154] Emphasis added.

by air carriers of PNR data (the "Baker letter").[1155] The letter is intended to set forth the US' administration "understandings with regard to the interpretation of a number of provisions"[1156] of the 2004 PNR Undertakings, since "things have changed in Washington in the last couple of years."[1157] The Baker letter in essence introduced a number of unilateral changes to the 2004 Undertakings,[1158] which means that "the commitments of the United States under the Interim Agreement are markedly different from those under the 2004 Agreement."[1159]

Under the new US understanding of the Undertakings, PNR data will be shared with further government authorities, besides the DHS, in order to fight terrorism.[1160] If PNR data are 'pulled' from the airlines, the US authorities reserve the right to obtain them more than 72 hours prior to the departure of a flight.[1161] Moreover, the PNR data might be used for other purposes, besides the fight against terrorism and international crime in order to present the "vital interests" of the data subject or of other persons. According to the Baker letter, vital interests "encompasses circumstances in which the lives of the data subject or of others could be at stake and includes access to information necessary to ensure that those who may carry or may have been exposed to a dangerous communicable disease can be readily identified, located, and informed without delay."[1162] The reference to the period of retention of the PNR data in the Baker letter seems rather confusing. It starts by pointing out that "several important uses for PNR data help to identify potential terrorists; even data that is more than 3.5 years old can be crucial in identifying links among terrorism suspects."[1163] It then goes on to explain that Undertaking 15 of the 2004 Agreement required the destruction of any data, but

---

[1155] 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, OJ C 259/1 of 27 October 2006.
[1156] *Id.*
[1157] *See* Jonathan Faul testimony in House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, *supra* note 945, paragraph 60.
[1158] *See* ELSPETH GUILD, INQUIRY INTO THE EU-US PASSENGER NAME RECORD AGREEMENT (CEPS, Policy Brief No. 125, March 2007).
[1159] House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, *supra* note 945, paragraph 60.
[1160] Letter to the Council Presidency and the Commission, *supra* note 211. *See* also the Preamble of the Interim Agreement, which states: "For the purposes of this Agreement, DHS means the Bureau of Customs and Border Protection, US Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it..."
[1161] *Id.*
[1162] *Id.*
[1163] *Id.*

"questions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the United States and the European Union as part of future discussions."[1164] This seems to be suggesting that CBP has no intention of deleting the PNR data after the 3.5 year period, even if those were collected under the (previous) 2004 Agreement.[1165]

2.5 Third round: The 2007 PNR Agreement

With the Interim PNR Agreement deemed to expire on 31st July 2007, the EU had to start a new round of negotiations with the United States for a new and this time more permanent agreement. On 22 February 2007, the Council authorised once again the Presidency, assisted by the Commission, to open negotiations for a long-term PNR agreement. The Parliament, having noted that "a future agreement must have more democratic legitimacy, with the full involvement of the European Parliament and/or ratification by national parliaments",[1166] called for an assessment of the effectiveness of the previous agreements before the adoption of a new one;[1167] and asked that the principles of purpose limitation[1168] and proportionality;[1169] as well as the rights to information, access and rectification of the data subjects are respected.[1170]On the other side of the Atlantic, in an attempt to exercise some political pressure, US Secretary of Homeland Security Michael Chertoff addressed, on 14 May 2007, the LIBE

[1164] *Id.*
[1165] The House of Lords severely criticises this development as a "blatant disregard of the final sentence of Undertaking 15" which also has "an ethical dimension." According to the House of Lords report, "For the purposes of the new Agreement being negotiated we have concluded that fixing a precise time limit is not the most important aspect of data retention. We would not therefore be opposed to an Agreement which provided that data transferred under the 2004 and 2006 Agreements should be retained for longer than 3.5 years. What we strongly oppose is the assumption that this can take place simply by a unilateral abrogation of the Undertaking, without the consent of the EU expressed in a provision of the new Agreement. The negotiators should as a matter of principle insist that data transferred under the 2004 and 2006 Agreements must be destroyed no later than 3.5 years after the transfer, unless a formal Agreement is negotiated allowing these data to be retained longer." *See* House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, *supra* note 945, paragraph 67, 69, 71–72.
[1166] European Parliament resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues P6_TA(2007)0039.
[1167] *Id.*
[1168] *Id.*
[1169] *Id.*
[1170] *Id.*

Committee of the European Parliament, stating that PNR data transfer is "a tool which at minimal cost of civil liberty has the tremendous potential to save lives".[1171]

On 28 June 2007 the draft agreement between the EU and the US was sent to the European Parliament LIBE Committee. In its July 2007 Resolution, the Parliament having expressed its disappointment on "the lack of democratic oversight of any kind"[1172] concerning the new Agreement, which was "negotiated and agreed without any involvement of the European Parliament and leaving insufficient opportunity for national parliaments to exercise any influence over the negotiating mandate",[1173] concluded that the draft agreement was "substantively flawed in terms of legal certainty, data protection and legal redress for EU citizens, in particular as a result of open and vague definitions and multiple possibilities for exceptions."[1174]

Despite the Parliament's objections, the Agreement was signed on 23 July 2007.[1175] Following the general pattern of the previous PNR Agreements, it does not resemble in form a typical international agreement. This is because, the 2007 Agreement is not found in one unique document. In the words of Commissioner Franco Frattini, "the agreement is divided into three parts. First, an agreement signed by both parties. Second, a letter which the United States sent to the EU in which it set out assurances on the way in which it will handle European PNR data in the future. And third, a letter from the EU to the United States acknowledging the receipt of assurances and confirming that on that basis it considers the level of protection afforded by the US Department of Homeland Security to be adequate for European PNR data."[1176] This form, while not new in the PNR context (letter of Undertakings in the first PNR, Baker letter in the Interim PNR Agreement), raises concerns, especially

---

[1171] US Homeland Security Secretary Michael Chertoff's Address before the Civil Liberties Committee of the European Parliament, Brussels 14 May 2007, *supra* note 3.
[1172] European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America P6_TA-PROV(2007)0347.
[1173] *Id.*
[1174] *Id.*
[1175] 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), OJ L 204/16 of 4 August 2007.
[1176] European Parliament Debates, Monday, 9 July 2007, Strasbourg, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20070709+ITEM-018+DOC+XML+V0//EN&language=EN.

as regards the legal nature of the DHS letter, and its relationship with the Agreement.[1177]

As regards its substance, the 2007 Agreement[1178] seems imbalanced; obligations are imposed on the EU side only; the US authorities provide mere 'assurances'[1179] on the use of the data. The first Article of the Agreement is illustrative:

> "On the basis of the *assurances* in DHS's letter explaining its safeguarding of PNR (the DHS letter), the European Union will ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America will make available PNR data contained in their reservation systems *as required* by DHS."[1180]

In fact, the DHS letter constitutes the most important part of the 2007 Agreement. More particularly, the letter is "intended to explain how the United States Department of Homeland Security handles the collection, use and storage of PNR."[1181] Concerning the purposes for which PNR data are used, it had already been mentioned in the Baker letter that besides preventing and combating terrorism and other serious crimes, PNR may be used also "for the protection of the vital interests of the data subject or other persons." The DHS letter confirms this[1182] and adds that PNR data may be further used where necessary "in any criminal judicial proceedings, or as otherwise required by law."[1183] PNR data will be exchanged with other government authorities in third countries "in support of counterterrorism, transnational crime and

---

[1177] European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, *supra* note 230.

[1178] 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 L 204/18 of 4 August 2007.

[1179] The European Parliament "is concerned that the DHS's handling, collection, use and storage of PNR data is not founded on a proper agreement, but only on non-binding assurances that can be unilaterally changed by the DHS at any given moment and that do not confer any rights or benefits on any person or party." *See* European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, *supra* note 230. Papakonstantinou and de Hert astutely note: "Obviously, the DHS "assures" but does not "warrant" or "undertake" to safeguard PNR data. The qualitative difference is clear for everyone to see." *See* Papakonstantinou & de Hert, *supra* note 1067, at 909–910.

[1180] Emphasis added.

[1181] DHS letter.

[1182] *Id.* Article I.

[1183] *Id.* This change of the scope of the Agreement has been criticized by Art. 29 Working Party. *See* ARTICLE 29 WORKING PARTY, OPINION 5/2007 ON THE FOLLOW-UP 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 CONCLUDED IN JULY 2007.

public security related cases (including threats, flights, individuals and routes of concern) they are examining or investigating".[1184] "Concomitantly, the EU will not interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds."[1185] The categories of PNR data collected are reduced from 34 in the 2004 Agreement to 19. This reduction, however, has been characterised by the European Parliament as "cosmetic" since it is essentially merging the 34 into 19 data fields.[1186] The Article 29 Working Party goes further in its examination and speaks of an extension of the data transmitted to the DHS.[1187] Sensitive data collected will be filtered and promptly deleted, unless there is an exceptional case "where the life of a data subject or of others could be imperilled or seriously impaired."[1188] In this case, it might be accessed and used by DHS officials, and will be deleted "within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law. DHS will provide notice normally within 48 hours to the European Commission that such data, including sensitive data, has been accessed."[1189] The data will be retained for an overall of fifteen years: seven years in an active analytical database,[1190] and eight years in a dormant, non-operational status.[1191] According to the DHS letter, this

[1184] *Id.* Article II. In its Resolution, the European Parliament "strongly opposes the provision that third countries in general may be given access to PNR data if adhering to DHS-specified conditions, and that third countries may exceptionally, in unspecified emergency cases, be given access to PNR data without assurances that the data will be handled according to the DHS level of data protection." *See* European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, *supra* note 230.

[1185] Article 6 of the Agreement.

[1186] The European Parliament "points out that the reduction is largely cosmetic due to the merging and renaming of data fields instead of actual deletions." *See* European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, *supra* note 230.

[1187] "The new list indicates data elements previously not included in the list and so extends the scope of information DHS requires." *See* Article 29 Working Party, *Opinion 5/2007 on the Follow-up 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 Concluded in July 2007*, *supra* note 1183.

[1188] DHS letter Article III.

[1189] *Id.*

[1190] The European Parliament found this period excessive: "[The Parliament] is concerned that data will be kept for seven years in 'active analytical databases', leading to a significant risk of massive profiling and data mining, which is incompatible with basic European principles and is a practice still under discussion in the US Congress." *See* European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, *supra* note 230.

[1191] *Id.* Article VII. The DHS letter is not very clear, however, on the deletion of the PNR data after the 15 year period. More particularly, it notes: "We expect that EU PNR data shall be deleted at the end of this period; questions of whether and when to destroy PNR data collected in accordance with this letter will be addressed by DHS and the EU as part of future discussions." The length of the retention period was strongly criticised by the European Parliament. *See* European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, *supra* note 230.

retention period also applies to the PNR data collected on the basis of the 2004 and 2006 Agreements, raising questions as to whether the data collected under the two previous agreements were ever deleted in the respective periods required by those Agreements. Concerning the never resolved issue of the use of a 'push' system for the transfer of the data,[1192] the DHS letter notes that thirteen airlines have implemented it, and the responsibility rests with the remaining air carriers to migrate their systems and comply with DHS's technical requirements. For the airlines that do not implement such a system, the 'pull' system will remain in effect.[1193] Insofar as the data subjects' rights are concerned, the DHS letter seems to be making an important concession: administrative Privacy Act protections are to be extended to "PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens."[1194] Individuals also have the right to access the data held on them in accordance with the US Privacy Act and the US Freedom of Information Act (FOIA).[1195]

The EU's reply to the DHS letter forms part of the 2007 Agreement, but does not add any substantial point itself.[1196] It merely notes that "the assurances explained in [the DHS] letter allow the European Union to deem [...] that DHS ensures an adequate level of data protection."[1197] The same verbal economy applies to the agreement, which contains only nine Articles. The most ambiguous one is Article 5:

[1192] The European Parliament in its Resolution refers to the highly debated method of transfer of the PNR data: "[The Parliament] regrets the fact that the shift – already foreseen in the 2004 PNR agreement – has been delayed for years, even though the condition of technical feasibility has long since been met; believes that the PUSH system for all carriers should be a *sine qua non* for PNR transfers…" *See* European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, *supra* note 230. Similar concerns are raised by the Art. 29 Working party. *See* Article 29 Working Party, *Opinion 5/2007 on the Follow-up 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 Concluded in July 2007*, *supra* note 1183.

[1193] *Id.* Article VIII.

[1194] *Id.* Article IV. This provision was welcomed as a positive development by the Parliament in its Resolution. *See* European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, *supra* note 230.

[1195] *Id.*

[1196] The value of the EU's reply letter to DHS has been questioned: "Why did the EU feel compelled to send a letter accepting "the DHS letter"? Given the wording of the Second PNR Agreement, the EU is already aware of the content of the "DHS letter" and it is on its exact premises that the Agreement itself is concluded. Why then introduce a "letter exchange" process, whereby the DHS addresses a letter to the EU, and the EU accepts it by replying back in writing […] No matter how innocent and well-intended such a "letter exchange" might appear, one cannot help but think that it introduces in practice an amendment process, whereby the DHS will be addressing "DHS letters" to the EU, and the EU will be assessing and responding to them accordingly." *See* Papakonstantinou & de Hert, *supra* note 1067, at 910.

[1197] EU letter to US.

> "By this Agreement, DHS expects that it is not being asked to undertake data protection measures in its PNR system that are more stringent than those applied by European authorities for their domestic PNR systems. DHS does not ask European authorities to adopt data protection measures in their PNR systems that are more stringent than those applied by the U.S. for its PNR system. If its expectation is not met, DHS reserves the right to suspend relevant provisions of the DHS letter while conducting consultations with the EU with a view to reaching a prompt and satisfactory resolution."

The language of this provision cannot go unnoticed: it constitutes a unilateral statement by the US authorities warning the EU on its future positions regarding PNR negotiations.[1198]

From a fundamental rights' point of view, the 2007 PNR Agreement "does not stand a chance".[1199] It has "markedly weakened" the safeguards provided for under its predecessors, which were already considered "weak" themselves, and "contains too many emergency exceptions" and shortcomings."[1200]

2.6 Implementing the PNR Agreement: An Insight into the DHS Privacy Office Report

On 18 December 2008, the DHS Privacy Office published its Report concerning Passenger Name Record Information derived from flights between the US and the EU.[1201] The purpose of the report was to "determine whether the Department of Homeland Security (DHS) and, in particular, the U.S. Customs and Border Protection (CBP) are operating in compliance with the Automated Targeting System (ATS) System of Records Notice (SORN) published on August 6, 2007 in the Federal

[1198] The Article 29 Working Party finds this provision as a "very worrying development", which "may affect the EU efforts to guarantee a high level of data protection in any future EU PNR regime." *See* Article 29 Working Party, *Opinion 5/2007 on the Follow-up 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 Concluded in July 2007*, *supra* note 1183.

[1199] Papakonstantinou & de Hert, *supra* note 1067, at 913.

[1200] Article 29 Working Party, *Opinion 5/2007 on the Follow-up 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 Concluded in July 2007*, *supra* note 1183.

[1201] U.S. Department of Homeland Security, Privacy Office, *supra* note 967.

Register and the 2007 Letter of Agreement between the United States and the Council of the European Union dated July 26, 2007 (2007 Letter)."[1202] ATS SORN was adopted by the DHS in order to implement the provisions and, thus, comply with the 2007 PNR Agreement.[1203]

A closer examination of the ATS SORN reveals several inconsistencies with the 'assurances' laid down in the DHS letter. For instance, on the issue of the sharing of PNR, the letter provides laconically that "DHS shares EU PNR data only for the purposes named in Article I."[1204] ATS SORN states:

> "In addition to those disclosures generally permitted under 5 U.S.C. 552a (b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a *routine use*[1205] pursuant to 5 U.S.C. 552a (b) (3)."[1206]

The disclosure of PNR data to other US authorities for routine (and not case-by-case, use, as was envisaged in the previous Agreements), is not found anywhere in the DHS letter. According to Report, the DHS Privacy Office found that in addition to the types of terrorism related, flights from warrants related, and transnational crimes related disclosures, PNR was "regularly shared by the National Targeting Centre (NTC-P)

[1202] *Id.* at 4.
[1203] *Id. See* also Marjorie J. Yano, *Come Fly the (Unfriendly) Skies: Negotiating Passenger Name Record Agreements Between the United States and European Union*, 5 ISJLP 479, 501 (2008).
[1204] DHS letter Article II.
[1205] Routine Uses A, B, C and D U.S.C. § 552a (b)(1), (b)(3), b(8) and (e)(10) read as follows:
"A. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws;
B. To Federal and foreign government intelligence or counterterrorism agencies or components where CBP becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;
C. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or where the information is relevant to the protection of life, property, or other vital interests of a data subject and such disclosure is proper and consistent with the official duties of the person making the disclosure;
D. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk)." *See* U.S. Department of Homeland Security, Privacy Office, *supra* note 967, at 15.
[1206] Emphasis added.

with the Centre for Disease Control (CDC) to properly coordinate appropriate responses to health concerns associated with international air transportation."[1207]

Concerning the extension by the DHS letter of the rights of access and redress of individuals, that was much "triumphed over by the European side",[1208] the Privacy Office, reviewed seven requests for PNR and three other requests related to searches for "all information held by CBP". According to the Report, "the requests for PNR took more than one year to process and were inconsistent in what information was redacted."[1209] A similar conclusion was also reached in the February 2010 joint review of the 2007 Agreement.[1210]

Finally, it seems also that ATS SORN confirms the concerns raised in the EU on the time of deletion of the collected PNR data.[1211] It provides that:

> "ATS both collects information directly, and derives other information from various systems. To the extent information is collected from other systems, data is retained in accordance with the record retention requirements of those systems. The retention period for data maintained in ATS will not exceed fifteen years, after which time it will be deleted, except as noted below...Information maintained only in ATS that is linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (i.e., specific and credible threats; flights, individuals, and routes of concern; or other defined sets of circumstances) will remain accessible for the life of the law

---

[1207] In fact, the SORN for ATS allows for sharing of information "to appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk." (Routine use D, ATS SORN DHS/CBP-006, August 6, 2007, 72 FR at 43654). *See* U.S. Department of Homeland Security, Privacy Office, *supra* note 967, at 14.

[1208] Papakonstantinou & de Hert, *supra* note 1067, at 912.

[1209] U.S. Department of Homeland Security, Privacy Office, *supra* note 967, at 26. An attempt also to exercise the right to access to PNR data held by DHS reveals the complexity of the procedure which makes access almost impossible. The Privacy Officer recommended that "The FOIA/PA request process needs to be strengthened to improve response time, improve the quality of the responses and the redaction, and sufficiency of searches."

[1210] "It is noted that the newly introduced tracking system for such requests is not ideal. It is only able to track requests under the general heading 'travellers' and it is unable to distinguish between requests for access to PNR data and requests for other data, and it also unable to track requests specifically relating to EU-originating PNR data. Further steps should be taken in order to fine-tune the tracking systems." *See* 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 RECORD (PNR) DATA BY AIR CARRIERS TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY (DHS) 8-9 FEBRUARY 2010 11 (April 07, 2010).

[1211] *See* above.

enforcement matter to support that activity and other enforcement activities that may become related."[1212]

This means, effectively, that PNR data will not be deleted even after the fifteen year retention period if it is related to a specific case or investigation.

2.7 Negotiating a new PNR Agreement?

According to Article 9, the 2007 Agreement is bound to expire in 2014, seven years after its signature. In May 2011, a draft Agreement between the USA and the EU on the use and transfer of PNR data to the US Department of Homeland Security was circulated from the Presidency.[1213] Before taking a brief look at this draft Agreement, one important clarification should be made. Any new PNR Agreement will operate under the legal framework introduced by the Lisbon Treaty, and in particular, under Article 218 of the Treaty on the Functioning of the European Union, which requires the consent of the European Parliament for the conclusion of international agreements.

The first major difference one notices talking a look at the draft PNR Agreement is that it looks more like an international agreement than all the other PNR Agreements. As it stands at the moment, all its core provisions are included in the text of the Agreement itself, without any Undertakings or side letters. There is a further development to be mentioned: the drafting of the Agreement seems 'more European' or 'more data subject-friendly'. The different data protection principles are put under the title "Safeguards Applicable to the Use of PNR", and analysed in separate Articles: data security (Article 5), sensitive data (Article 6), automated individual decisions (Article 7), retention of data (Article 8), non-discrimination (Article 9), transparency (Article 10), access for individuals (Article 11), correction or rectification (Article 12), redress for individuals (Article 13), and oversight (Article 14). In this way, it is at least clearer to the data subject what her rights are and how they can be exercised.

[1212] U.S. Department of Homeland Security, Privacy Office, *supra* note 967, at 30.

[1213] Council of the European Union, Draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record data to the United States Department of Homeland Security, 10453/11, Brussels, 20 May 2011.

That being said, on questions of substance the draft Agreement does not seem to change much from the others. Regarding the use of PNR, while open definitions such as preventing, detecting, investigating and prosecuting 'terrorist offences and related crime', 'other serious transnational crimes', have been defined more precisely, with reference to European standards, they are still problematic because they remain unduly open.[1214] The retention period continues to be for fifteen year, this time under a different arrangement: DHS will retain PNR in an active database for five years, then the data, after being depersonalised and masked, will be transferred to a dormant database and held for another ten years. Finally, concerning individual rights, there has been no significant improvement to the position of the data subject under the draft Agreement.

For these reasons, the Commission's legal service in its Opinion on the draft PNR, concluded that:

> "despite certain presentational improvements, the draft agreement does not constitute a sufficiently substantial improvement of the agreement currently applied [...] For these reasons, the Legal Service does not consider the agreement in its present form as compatible with fundamental rights."[1215]

3. EU-US: Two Different Cultures of Privacy?

3.1 The misconceptions about the EU privacy culture

It has been argued in both sides of the Atlantic, that "the drama that played out between the United States and the European Union over PNR-data transfers is a prominent example of the clash between conflicting philosophies on privacy

[1214] *See* European Commission Legal Service, Note for the Attention of MR Stefano Manservisl Director General, DG Home, Draft Agreement on the Use of Passenger Name Records (PNR) between the EU and the United States, Brussels, 18 May 2011, *available at* http://www.statewatch.org/news/2011/jun/eu-usa-pnr-com-ls-opinion-11.pdf.
[1215] *Id.*

protection."[1216] In fact, an American scholar criticised the 'strict' pro-privacy stance adopted by the EU in the PNR negotiations:

> "increased information sharing is the best way of preventing terrorism, but information sharing between the public and private sector may be difficult if Americans are focused on the dangers of state surveillance and Europeans are concerned about protecting the dignity of the consumer."[1217]

While such a comment would raise eyebrows in Europe, it reflects a perception that is far from rare in the American literature. Legal historian James Whitman, argued in an Article in Yale Law Journal:

> "American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity."[1218]

According to Whitman, European privacy law, being based on personal dignity, focuses on the protection of rights such one's image, name, reputation, and informational self-determination.[1219] Whitman, therefore, identifies the media as the prime enemy of the right to privacy in the European continental conception.[1220] By contrast, America, according to the same author, "is much more oriented toward values of liberty, and especially liberty against the state."[1221] In essence, at the conceptual core of the American right to privacy lies "the right to freedom from intrusions by the state, especially in one's own home."[1222]

Whitman's argument is based on the historical analysis of the evolution of the right to privacy in Germany and France, and although it is valid from many respects, it suffers from a number of fallacies. First, it fails to acknowledge that Europe or the EU is not only Germany and France. It is true that the EU fundamental right to data protection derived from the German conception of informational self-

---

[1216] Rizer, *supra* note 1148, at 79. According to Rasmussen, "The dispute between the United States and European Union over the transfer of PNR data is a *prima facie* conflict of laws dispute." Rasmussen, *supra* note 946, at 588. *See* also Fernando Mendez & Mario Mendez, *Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States*, 40 PUBLIUS: THE JOURNAL OF FEDERALISM 617 (2009); Allen Shoenberger, *Privacy Wars: EU Versus US: Scattered Skirmishes, Storm Clouds Ahead*, 17 IND. INT'L & COMP. L. REV. 375 (2007).

[1217] Jeffrey Rosen, *Continental Divide: Americans See Privacy as a Protection of Liberty, Europeans as a Protection of Dignity. Will One Conception Trump the Other—or Are Both Destined to Perish?*, LEGAL AFFAIRS (2004); Ravich, *supra* note 965, at 49.

[1218] Whitman, *supra* note 1024, at 1163.ROSEN, THE UNWANTED GAZE, *supra* note 96.

[1219] Whitman, *supra* note 1024, at 1167.

[1220] *Id.* at 1171. "Continental privacy law is, […], "society" privacy for everybody."

[1221] *Id.* at 1161.

[1222] *Id.* at 1162.

determination,[1223] but it had an evolution of its own within the EU legal order. Second, while we can talk about a 'European privacy culture', there are two fundamental rights to be found in the EUCFR: privacy (Article 7), and data protection (Article 8). Both have vertical and horizontal application, in that they apply against the state and against other individuals. Traditionally the right to privacy in the EU has been conceived as a non-interference protective rule.[1224] But also, data protection in the EU does not merely cover 'commercial' processing, it covers also processing by public authorities. In fact, the two most important EU data protection instruments, the EU Data Protection Directive and the Data Protection Framework Decision, apply to processing both in the private and the public sector. To argue, therefore, that Europeans are concerned about protecting "the dignity of the consumer" is, at best, an inaccurate generalisation.[1225] Moreover, the American notion of privacy is not entirely based on liberty, as it is not merely limited to 'decisional' privacy, namely, the independence to make certain kind of importance decisions;[1226] it comprises also 'informational' privacy, which is the interest in avoiding disclosure of personal matters.[1227]

Setting aside such misconceptions, it is true that EU and US have different privacy regimes. The EU privacy regime, has been discussed in Chapter 2. The US privacy regime will be examined briefly in the following section.

3.2 The US privacy regime

Describing the US privacy regime, legal scholar Gregory Shaffer notes:

> "data privacy regulation in the United States is fragmented, ad hoc, and narrowly targeted to cover specific sectors and concerns. It is decentralised and uncoordinated, involving standard setting and enforcement by a wide variety of

[1223] *See* Chapter 1.
[1224] *See* Chapter 1 for the relevant discussion. *See* also De Hert & Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *supra* note 197, at 62.
[1225] Papakostantinou and de Hert characterise the statement "US privacy protects individual liberty, while in Europe the value protected is dignity" as "metaphysical assertion." *See* Papakonstantinou & de Hert, *supra* note 1067, at 898.
[1226] For instance in *Roe v. Wade* (410 US 179 (1973)), the Supreme Court upheld a woman's right to an abortion under certain circumstances.
[1227] *See* Chapter 1.

actors, including federal and state legislatures, agencies and courts, industry associations, individual companies, and market forces."[1228]

US privacy law can be found in a number of different sources: US Constitution, Supreme Court case law, federal legislation, state legislation and the theory of torts.[1229]

The Constitutional protection of privacy is mainly based on the First Amendment (protection of free speech and freedom of assembly), the Fourth Amendment (protection from unreasonable searches and seizures), and the Fifth Amendment (privilege against self-incrimination).[1230] As the Supreme Court have stated, "the overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[1231] The Fourth Amendment is, therefore, the most relevant provision in the present context. It provides:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[1232]

The Fourth Amendment contains two clauses: the first, the substantive one, protects against certain government activities; the second, the procedural one, regulates government power through the process of obtaining a warrant.[1233] A warrant can be obtained when there is a "probable cause" for conducting a search or seizure.[1234] In *Katz v. United States*,[1235] the Supreme Court established that the protection of the Fourth Amendment against government intrusion applies, when an individual has a

---

[1228] Gregory C. Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards*, 25 YALE JOURNAL OF INTERNATIONAL LAW 1, 22 (2000).
[1229] Papakonstantinou & de Hert, *supra* note 1067, at 892.
[1230] Susan Brenner, *Constitutional Rights and New Technologies in the United States*, CONSTITUTIONAL RIGHTS AND NEW TECHNOLOGIES : A COMPARATIVE STUDY 225, 230 (Ronald Leenes et al., 2008).
[1231] *Schmerber v. California*, 384 U.S 757 (1966).
[1232] US Constitution, IV Amendment.
[1233] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 SOUTHERN CALIFORNIA LAW REVIEW 1083, 1118 (2002).
[1234] SOLOVE & SCHWARTZ, *supra* note 70, at 237.
[1235] The decision has been characterized as "the most important judicial decision on the scope of the Fourth Amendment." *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK : THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 13 (2007).

"reasonable expectation of privacy."[1236] Justice Harlan in his concurring opinion in *Katz* articulated the twofold requirement, known as the "reasonable expectation privacy test"[1237] that triggers the application of the Fourth Amendment:

> "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognise as "reasonable."[1238]

This means, according to Justice Harlan, that "conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."[1239] A similar statement was made by the majority opinion, which held that "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[1240]

In *Smith v. Maryland*,[1241] the Court applied this reasoning on phone records. The police, without a warrant, asked the telephone company to install a pen register[1242] to record the numbers dialled from the defendant's home.[1243] The Court agreed that there was no reasonable expectation of privacy regarding the numbers someone dials on her phone. The Court reasoned:

> "First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All users realise that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realise, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud and preventing violations of law." [...] Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the company has facilities for recording this

---

[1236] *Katz v. United States*, 389 U.S 347 (1967).
[1237] Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society*, 42 DUKE L.J. 727, 731 (1993).
[1238] *Id.* Justice John Harlan concurring.
[1239] *Id.*
[1240] *Id.*
[1241] *Smith v. Maryland* U.S 735 (1979).
[1242] A pen register is a device that records outgoing telephone calls.
[1243] Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, *supra* note 1233, at 1134.

information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbour any general expectation that the numbers they dial will remain secret."[1244]

Smith v. Maryland establishes, therefore, a general rule, according to which, "if information is in the hands of third parties, then an individual can have no reasonable expectation of privacy in that information, which means that the Fourth Amendment does not apply."[1245] As Christopher Slobogin notes, this decision suggests that "transaction surveillance[1246] is [...] immune from the restrictions of the Fourth Amendment."[1247]

In the context of the present discussion, leaving aside the obvious similarities of *Smith v. Maryland* with the EU Data Retention Directive discussed in Chapter 3, the decision is also illuminating for the PNR analysis. Applying the *Smith v. Maryland* reasoning, PNR data cannot be covered by the Fourth Amendment protection, since travellers cannot enjoy any reasonable expectation of privacy of data they gave themselves to the airline companies in order to effectuate the ticket reservation.[1248]

At federal level, statutes are "narrowly tailored to specific privacy problems."[1249] In fact, as Shaffer observes,

"Rather than engage in a concerted effort to protect individual privacy, in most cases, Congress has simply reacted to public scandals. In passing the Fair Credit Reporting Act, Congress responded to "consumer horror stories of dealings with credit report agencies." The Driver's Privacy Protection Act "was inspired by the murder of an actress... who was tailed by a stalker who obtained her address... from state driver's license records." Congress enacted the Video Privacy Protection Act after the video records of Judge Robert Bork were obtained and published by a news reporter in the course of a campaign against

[1244] *Smith v. Maryland*, *supra* note 300.
[1245] Also known as third party doctrine. *See* Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, *supra* note 1233, at 1135.
[1246] Slobogin explains that "transaction surveillance involves accessing *recorded* information about communications, activities, and other transactions." *See* SLOBOGIN, *supra* note 1235, at 3.
[1247] *Id.* at 16.
[1248] To what extent PNR is covered under the European notion of privacy will be discussed below.
[1249] Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, *supra* note 94, at 1440.

his Supreme Court nomination. As a result, in the United States, "video rentals are afforded more federal protection than medical records.""[1250]

The most significant and "the only federal omnibus" piece of privacy legislation is the Privacy Act of 1974.[1251] The Privacy Act embodies fair information principles in a statutory framework governing the means by which federal agencies collect, maintain, use, and disseminate personally identifiable information. The Privacy Act applies to information that is maintained in a "system of records." A system of records is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. While the Privacy Act applies to government records it is ambiguous as to whether it applies to "commercial data brokers who supply information to the government".[1252] As one American author notes, "it is not clear whether a database which originates in the private sector, and is then used by the government, is subject to the Act."[1253] This could be problematic in the case of the PNR data that originate in air carrier databases. The Privacy Act applies to US citizens and lawful permanent residents. According to 2007 DHS letter, Privacy Act safeguards were extended administratively to EU citizens concerning their PNR data.[1254] As already mentioned above, an important limitation of the Privacy Act is the so-called "routine use" exception, according to which, information may be disclosed for any "routine use" if disclosure is "compatible" with the purpose for which the agency collected the information.[1255] PNR data, as seen above, are disclosed by the DHS for "routine use." The Privacy Act is further limited, as its primary enforcement mechanism is a civil action in federal court, generally for damages.[1256]

[1250] Shaffer, *supra* note 287, at 25 and references therein.
[1251] Pub. L. No. 93-579, 88 Stat. 1896 (2000) (codified at 5 U.S.C. § 552a).
[1252] Chris Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595, 622 (2004).
[1253] Anita Ramasastry, *Lost in Translation - Data Mining, National Security and the Adverse Inference Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 793 (2006).
[1254] *See* above.
[1255] Daniel Solove, *A Brief History of Information Privacy Law*, PROSKAUER ON PRIVACY, GWU LAW SCHOOL PUBLIC LAW RESEARCH PAPER NO. 215 1, 26 (2006); Paul Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 585 (1995); Daniel Solove, *The Origins and Growth of Information Privacy Law*, 748 PLI/PAT 29 (2003).
[1256] Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 BOSTON COLLEGE LAW REVIEW 609, 633 (2007).

Another important piece of federal legislation is the Freedom of Information Act (FOIA) adopted in 1966.[1257] FOIA permits any person (regardless of nationality or country of residence) access to a US federal agency's records, except to the extent such records (or a portion thereof) are protected from disclosure by an applicable exemption under the FOIA. In the 2007 PNR Agreement, FOIA was also extended to apply to individuals travelling with European airlines.[1258] According to DHS, PNR data are not disclosed to the public, but to the data subjects or their agents in accordance with US law.

3.3 The need for a comprehensive framework?

The seriously limited US privacy regime, discussed above, creates problems to unimpeded transatlantic data flows. As the PNR experience proved, negotiations are difficult, with data protection differences being at the heart of the conflict.[1259] A solution would, therefore, be what the Community did sixteen years ago, in order to ensure free movement of data across its Member States: harmonise data protection rules. Obviously, to talk of 'harmonisation' of EU and US privacy regimes, is absurd and therefore out of the question. What can be done in this context is an international agreement setting down certain data protection guarantees that will govern data exchanges between the two parties, in order to raise restrictions on data flows; and that's what was opted for.

In particular, the EU-US Justice and Home Affairs Ministerial Troika on 6 November 2006 decided to establish an informal high level advisory group[1260] to start discussions on privacy and personal data protection in the context of the exchange of information for law enforcement purposes. On 28 May 2008, the Presidency of the Council of the European Union announced to the COREPER, that the EU-US High Level Contact Group (hereafter HLCG) on information sharing and privacy and

[1257] 5 U.S.C. § 552(a)(3)(A).
[1258] *See* above.
[1259] Besides PNR, a number of other EU-US Agreements refer to the exchange of personal data. For instance, the Extradition and Mutual Legal Assistance Agreement (2003); the Agreements governing personal data exchange between the United States and Europol (2002) and Eurojust (2006); the SWIFT Agreement (discussed below).
[1260] The group was composed of senior officials from the Commission, the Council Presidency (supported by the Council Secretariat) and the U.S. Departments of Justice, Homeland Security and State.

personal data protection had finalised its report. The report was made public on 26 June 2008.[1261]

The report aims to identify "a set of core principles on privacy and personal data protection, acceptable as minimum standards when processing personal data for law enforcement purposes."[1262] These should be included preferably in an international agreement binding both the EU and the US,[1263] instead of non-binding instruments or politically declarations.[1264] It was agreed by both sides that a binding instrument would provide "the greatest level of legal security and certainty", and "the advantage of establishing the fundamentals of effective privacy and personal data protection for use in any future agreements relating to the exchange of specific law enforcement information that might arise between the EU and the US."[1265]

The HLCG, indeed, agreed on a number of principles. These are: 1) purpose specification/purpose limitation; 2) integrity/data quality; 3) relevant and necessary/proportionality; 4) information security; 5) sensitive data; 6) accountability; 7) independent and effective oversight; 8) individual access and rectification; 9) transparency and notice; 10) redress; 11) automated individual decisions; and 12) restrictions on onward transfers to third countries.[1266]

Nevertheless, there were outstanding issues were differences remain: the question of redress;[1267] the consistency in private entities' obligations during data transfers;[1268] the equivalent and reciprocal application of privacy and personal data protection law;[1269] the impact of the agreement on relations with third countries;[1270]

[1261] Council of the European Union, Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection, 9831/08 JAI 275 DATAPROTECT 31 USA 26.
[1262] *Id.* at 3.
[1263] *Id.* at 8.
[1264] *Id.* at 9.
[1265] *Id.* at 8.
[1266] *Id.* at 4.
[1267] On 2 October 2009, the HLCG agreed on a text with regard to the redress principle: "Recognizing that both the US and EU provide multiple mechanisms for administrative and judicial redress, wherever an individual's privacy has been infringed or data protection rules have been violated with respect to that individual, that individual [should/shall] have, before an impartial competent authority, independent court or tribunal, an effective remedy and/or appropriate and effective sanctions." *See* Addendum to the Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, Report and Agreed Text from the High Level Contact Group as of 28 October 2009.
[1268] It was established that "any adverse impact on private entities resulting from data transfers, including those impacts deriving from diverging legal and regulatory requirements, should be avoided to the greatest extent possible." *See id.*
[1269] "The European Union and the United States should use best efforts to ensure respect for the requirements, taken as a whole as opposed to singular examples, that each asks the other to observe."

specific agreements regulating information exchanges and privacy and personal data protection;[1271] and issues related to the institutional framework of the EU and US.[1272] The two sides also seem to understand differently "law enforcement purposes",[1273] which is central for the agreement. For the EU "law enforcement purposes" mean "use for the prevention, detection, investigation or prosecution of any criminal offense." For the US, "law enforcement purposes" is somewhat a broader notion, as it comprises "the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for non-criminal judicial or administrative proceedings related directly to such offenses or violations."[1274] The HLCG does not seem to find these differences important:

> "These two different ways of describing "law enforcement purposes" reflect respective domestic legislation and history but may in practice coincide to a large extent."[1275]

The initiative was welcomed by the EDPS, who expressed, nevertheless, a number of concerns.[1276] In May 2010, the European Commission, taking up the work done by the HLCG, asked the Council to authorise the opening of negotiations with the United States of America for an agreement, based on Article 16 TFEU, "when personal data are transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters within the scope of Chapter 4 or 5 of Title V of Part Three of the TFEU."[1277] The

---

[1270] The HLCG held: "when the European Union or the United States has international agreements or arrangements for information sharing with third countries, each should use their best endeavours to avoid putting those third countries in a difficult position because of differences relating to data privacy including legal and regulatory requirements." *See id.*

[1271] In these cases it was agreed that "the processing of personal information in specific areas should be made subject to specific conditions and should include the necessary safeguards for the protection of privacy and personal data and individual liberties through the negotiation of an information sharing agreement. Such rules may offer individuals a wider measure of protection." *See id.*

[1272] The HLCG statement is rather economical on the issue: "the European Union and the United States intend to consult each other as necessary to discuss and if possible resolve matters arising from divergent legal and regulatory requirements." *See id.*

[1273] Council of the European Union, Reports by the High Level Contact Group *supra* note 317, at 3.

[1274] *Id.* at 4.

[1275] *Id.*

[1276] EUROPEAN DATA PROTECTION SUPERVISOR, OPINION ON THE FINAL REPORT BY THE EU-US HIGH LEVEL CONTACT GROUP ON INFORMATION SHARING AND PRIVACY AND PERSONAL DATA PROTECTION (November 11, 2008).

[1277] EUROPEAN COMMISSION, PROPOSITION DE RECOMMANDATION DU CONSEIL AUTORISANT L'OUVERTURE DE NEGOCIATIONS EN VUE D'UN ACCORD ENTRE L'UNION

Commission noted that the aims of the future EU-US agreement should be fourfold: First, the agreement should ensure a high level of protection of the fundamental rights and freedoms of individuals, in particular the right to protection of personal data, in line with the requirements of the EUCFR.[1278] Second, it should provide a clear and coherent legally binding framework of personal data protection standards. Such a framework should remove the uncertainties and bridge the gaps in protection created in the past because of significant differences between EU and US data protection laws and practices. The agreement itself should therefore, according to the Commission, provide enforceable data protection standards and establish mechanisms for implementing them effectively.[1279] Third, the agreement should provide a high level of protection for personal data transferred to and subsequently processed in the US for law enforcement purposes.[1280] Finally, the agreement would not do away with the requirement for a specific legal basis for transfers of personal data between the EU and the US, with specific data protection provisions tailored to the particular category of personal data in question.[1281] On 29 March 2011, it was announced that the EU and the US opened negotiations on an agreement to protect personal information exchanged in the context of fighting crime and terrorism.[1282]

3.4 'Spillovers of privacy' or 'spillovers of security'?

In an Article in 2000, legal scholar Gregory Shaffer argued that US privacy standards were "ratcheting up" to the level of European data protection standards.[1283] Shaffer explained that this was due to cross-border economic exchange that can help

---

EUROPEENNE ET LES ETATS- UNIS D'AMERIQUE SUR LA PROTECTION DES DONNEES PERSONNELLES LORS DE LEUR TRANSFERT ET DE LEUR TRAITEMENT A DES FINS DE PREVENTION, D'INVESTIGATION, DE DETECTION OU DE POURSUITE D'ACTES CRIMINELS Y COMPRIS LE TERRORISME, DANS LE CADRE DE LA COOPERATION POLICIAIRE ET JUDICIAIRE EN MATIERE PENALE COM(2010) 252/2.

[1278] *Id.*

[1279] *Id.*

[1280] *Id.*

[1281] *Id.*

[1282] Press Release, EU-US Negotiations on an agreement to protect personal information exchanged in the context of fighting crime and terrorism, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/203.

[1283] Shaffer, *supra* note 1228, at 1. *See* also Chuan Sun, *The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective*, 2 NW. J. TECH. & INTELL. PROP. 99 (2003).

"leverage standards upward, even in a powerful state such as the United States."[1284] He found that US businesses implement new internal data protection practices, in order to be able to engage in trade with EU-based businesses, avoiding EU data transfer restrictions.[1285] Taking advantage of the publicity given to the EU Data Protection Directive, US privacy advocates press further the legislators to enact additional data privacy legislation in the US.[1286] According to Shaffer

> "[t]he war over privacy standards is fought not just between Europe and the US. It is a civil war as well, fought within the United States itself, with European law changing the balance of power on the fields where US interest groups clash."[1287]

Shaffer was referring to the US-EU Safe Harbor programme, under which US-based companies may avoid EU data protection restrictions on data transfers if they self-certify that they abide with certain data protection principles.[1288] Shaffer contended that

---

[1284] Shaffer, *supra* note 1228, at 5.
[1285] *Id.* at 4.
[1286] *Id.*
[1287] *Id.*
[1288] For an overview of the EU-US Safe Harbor Agreement *see* http://export.gov/safeharbor/eu/eg_main_018365.asp. For an analysis *see inter alia* James Assey & Demetrios Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters*, 9 COMMLAW CONSPECTUS 145 (2001); Sylvia Kierkegaard Mercado, *Safe Harbor Agreement - Boon or Bane*, 1 SHIDLER J. L. COM. & TECH. 1 (2004); Rosa Barcelo, *Seeking Suitable Options for Importing Data from the European Union*, 36 INT'L L. 985 (2002); Daniel Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement*, 41 CASE W. RES. J. INT'L L. 193 (2009); David Castor, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, 12 IND. INT'L & COMP. L. REV. 265 (2002); David Raj Nijhawan, *The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939 (2003); David Tallman, *Financial Institutions and the Safe Harbor Agreement: Securing Cross-Border Financial Data Flows*, 34 LAW & POL'Y INT'L BUS. 747 (2003); Christopher Kuner, *Beyond Safe Harbor: European Data Protection Law and Electronic Commerce*, 35 INT'L L. 79 (2001); James Sunosky, *Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles*, 9 CURRENTS: INT'L TRADE L.J. 80 (2000); Angela Vitale, *The EU Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet*, 35 VAND. J. TRANSNAT'L L. 321 (2002); John Soma et al., *An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor*, 39 TEX. INT'L L.J. 171 (2004); Mike Ewing, *The Perfect Storm: The Safe Harbor and the Directive on Data Protection*, 24 HOUS. J. INT'L L. 315 (2002); Marsha Cope Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA. J. COMP. & INT'L L. 391 (2002); Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 FORDHAM INT'L L.J. 2024 (1999); Joel Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717 (2002); Tracey DiLascio, *How Safe Is the Safe Harbor - U.S. and E.U. Data Privacy Law and the Enforcement of the FTC's Safe Harbor Program*, 22 B.U. INT'L L.J. 399 (2004); Andrew Charlesworth, *Clash of the Data Titans - US and EU Data Privacy Regulation*, 6 EUR. PUB. L. 253 (2000); Jordan Blanke, *Safe Harbor and the European Union's Directive on Data Protection*, 11 ALB. L.J. SCI. & TECH. 57 (2001); Peter Blume, *Transborder Data Flow: Is There a Solution in Sight*, 8 INT'L J.L. & INFO. TECH. 65 (2000); Robert Schriver, *You Cheated, You Lied: The Safe Harbor*

> "In this way, Europe's regulatory approach may have spillover effects within the United States, leading to some convergence in data privacy practices, despite differing US and EC regulatory systems."[1289]

Legal scholar Francesca Bignami argued in an Article of 2007 that the regulatory convergence, suggested by Shaffer, finds its limits when interests such as policing and national defense come into play.[1290] According to Bignami,

> "[e]ven when the economic interests of big players in the global marketplace such as airlines and banks are at stake, a strong countervailing regulatory policy will trump the trade interest in convergence. In this instance, that opposing policy interest is government access to information to assist with law enforcement and national security. Furthermore, when an activity is entrusted to state—not private—actors, the pressure to develop a single modus operandi applicable in all jurisdictions is significantly lower. Policing and national defense are the prime examples of activities handled by government actors, not private firms. And the resistance to convergence of such actors is evident in the continuing difference in how police and spy agencies handle personal data in the United States and Europe."[1291]

Bignami certainly makes a valid point. Regulatory convergences in 'commercial processing' are not normally followed by similar spillovers in 'law enforcement processing'. However, the opening of negotiations between the EU and the US on the conclusion of a binding international agreement on data protection principles in the field of law enforcement,[1292] constitutes an interesting twist regarding this argument. If the agreement will be concluded, it will potentially provide leverage to domestic

---

Agreement and Its Enforcement by the Federal Trade Commission, 70 FORDHAM L. REV. 2777 (2002); Kamaal Zaidi, *Harmonizing U.S.-EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, 12 MICH. ST. J. INT'L L. 169 (2003); Seth Hobby, *The EU Data Protection Directive: Implementing a Worldwide Data Protection Regime and How the U.S. Position Has Progressed*, 1 INT'L L. & MGMT. REV. 155 (2005); Elizabeth Barnes Morey, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, 27 NW. J. INT'L L. & BUS. 171 (2007); Julia Gladstone, *The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy*, 7 WILLAMETTE J. INT'L L. & DIS. RES. 10 (2000); Henry Farrell, *Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement*, 57 INTERNATIONAL ORGANIZATION 277 (2003).

[1289] Gregory C. Shaffer, *Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements*, 9 COLUM. J. EUR. L. 29, 57 (2002).

[1290] Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, *supra* note 1256, at 676.

[1291] *Id.* at 676–677.

[1292] *See* above.

actors in the US to press for the levelling up of internal privacy standards in the area. Probably, in the future, we can therefore, be talking of privacy spillovers also in the law enforcement context.

While this for now is no more than mere speculation, the other side of the coin is that in the counter-terrorism context the EU is looking more towards the US, than the other way round. As an American author predicted in 2002

> "Since EU and US political interests are largely aligned […] against terrorism, it is possible that the European Union will move closer to the United States as a result of the [September 11] attacks, rather than the United States moving away from the European Union. To the extent that Europeans feel vulnerable as a result of terrorism, they may shift their emphasis away from data privacy and toward protective anti-terrorist surveillance programs."[1293]

PNR is a prominent example of this. Despite the apparent clash, the EU is already moving towards the establishment of its own PNR system.[1294] While potential 'spillovers of privacy' are not visible yet, 'spillovers of security', looking towards the opposite direction, are certainly here.

[1293] Steven Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 694 (2002).
[1294] *See* below.

4. "Outside Bad, Inside Good". The EU PNR Arrangement

4.1 The Quest for Reciprocity: The Proposal for an EU PNR Framework decision

All the three EU-US PNR Agreements contain a reciprocity clause, according to which the EU might develop its PNR system in the future.[1295] The wording is almost identical:

> "In the event that a PNR system is implemented in the European Union or in one or more of its Member States that requires air carriers to make available to authorities PNR data for persons whose travel itinerary includes a flight to or from the European Union, DHS shall, strictly on the basis of reciprocity, actively promote the cooperation of the airlines within its jurisdiction."[1296]

The clause does not establish a legal obligation on the US side; DHS merely undertakes to "actively promote the cooperation" of US-based airlines. Notwithstanding this, the EU's intentions are clear. Already since 2003, the Commission aspired on the development of an EU PNR scheme.[1297] According to the Commission, such a system would form the basis for the establishment of an "information policy" for law enforcement authorities, "which would become the backbone for a prevention policy in the field of organised crime and terrorism addressing in particular the safeguards of data processing systems and the reciprocity of data exchange."[1298]

On 6 November 2007 the Commission introduced its Proposal for a Council Framework decision on the use of PNR for law enforcement purposes on the basis of Articles 29, 30 (1) (b), and 34 (2) (b).[1299] The draft Framework decision had as its

---

[1295] Undertaking 45 and Article 6 of the 2004 PNR Agreement; Article 5 of the 2006 (Interim) PNR Agreement; and, Article 5 of the 2007 PNR Agreement.
[1296] Article 5 of the 2007 PNR Agreement. The wording differs only slightly in the 2004 Agreement.
[1297] On 9 October 2003 an experts' meeting was organised by the Commission, with the participation of law enforcement and data protection authorities of the Member States, in order to discuss the establishment of an EU PNR system.
[1298] Communication from the Commission to the Council and the Parliament, Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, Brussels, 16 December 2003 COM(2003) 826 final.
[1299] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes COM(2007) 654 final.

purpose "the making available by air carriers of PNR data of passengers of international flights to the competent authorities of the Member States, for the purpose of preventing and combating terrorist offences and organised crime, as well as the collection and retention of those data by these authorities and the exchange of those data between them."[1300] For this reason, the Framework decision required each Member State to designate a competent authority ("Passenger Information Unit" ("PIU")), which would be responsible for collecting the PNR data of international flights arriving or departing from its territory.[1301] The PIU would further be responsible for analysing the PNR data and for carrying out a risk assessment of the passengers, in order to: identify persons who are or may be involved in a terrorist or organised crime offence, as well as their associates; create and update risk indicators for the assessment of such persons; provide intelligence on travel patterns and other trends relating to terrorist offences and organised crime; use the risk assessment in criminal investigations and prosecutions of terrorist offences and organised crime.[1302]

The PNR data to be transmitted according to the draft Framework decision were "almost identical to the categories listed in the EU/US Agreement."[1303] The draft Framework decision asked for (exactly) nineteen data fields as the 2007 PNR Agreement.[1304] Air carriers would be required to make available the data to the relevant PIU twice: 24 hours before the scheduled flight departure, and immediately after flight closure.[1305] PNR data of persons identified for requiring further investigation would be transmitted to PIUs of other Member States when such transmission is necessary in the prevention and fight against terrorist offences and organised crime.[1306] The PNR data would be retained for a period of thirteen years in total: for five years in a PIU database and subsequently for another eight years, during which access would be limited in exceptional circumstances.[1307] Concerning the data protection principles applicable to the EU PNR system, the draft Framework decision could not be briefer: two Articles referred to data protection among which one was

---

[1300] Article 1 .
[1301] Article 3.
[1302] Article 3 (5).
[1303] HOUSE OF LORDS EUROPEAN UNION COMMITTEE, THE PASSENGER NAME RECORD (PNR) FRAMEWORK DECISION ¶ 22 (15th Report of Session 2007–08).
[1304] *See* Annex of the draft Framework decision.
[1305] Article 5.
[1306] Article 7.
[1307] Article 9.

dedicated to data security.[1308] On the protection of personal data, the draft Framework decision merely stated that the Framework decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters (not adopted yet back then) would apply.[1309] The Framework decision also prohibited any enforcement action to be taken by the PIUs or the Member States "only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation."[1310]

4.2 Behind the proposal: Why an EU PNR system?

It is at least puzzling why the EU, which has constructed for itself the successful image of a "moral leader of good"[1311] in the fight against terrorism due to its alleged higher respect to human rights standards compared to the US, introduced a proposal for an internal PNR scheme.[1312] This is all the more if one recalls the EU objections to the relevant US initiative and the controversies that surrounded the EU-US PNR negotiations described above. Furthermore, when the proposal for an EU PNR was tabled, the EU had already at place a system collecting API data.[1313] In particular, Directive 2004/82/EC requires air carriers to transmit the information included in the machine-readable part of a passport (API data), in order to combat illegal immigration and improve border control.[1314] The use of API data for law enforcement purposes is also permitted by the Directive under certain conditions.[1315] Data, therefore, such as name, gender, data of birth, nationality, type of travel document, departure and arrival time of transportation, the border crossing point of entry into the territory of the EU Member States, and the initial point of embarkation of passengers entering the EU were already available through the API system. This is, of course, if the EU Member States transposed the Directive, and it

[1308] Article 11 (Protection of personal data) and Article 12 (Data security).
[1309] Article 11 (1).
[1310] Article 11 (3).
[1311] Natalia Chaban et al., *The European Union as Others See It*, 11 EUROPEAN FOREIGN AFFAIRS REVIEW 245, 259 (2006).
[1312] PATRYK PAWLAK, MADE IN THE USA? THE INFLUENCE OF THE US ON THE EU'S DATA PROTECTION REGIME 5 (CEPS, November 2009).
[1313] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, *supra* note 16.
[1314] Article 1 of Council Directive 2004/82/EC.
[1315] Article 6 (1) of Council Directive 2004/82/EC.

seems that there is no "overwhelming enthusiasm"[1316] for that. The Directive should have been transposed by 5 September 2006, but in its 27 September 2006 Opinion, the Article 29 Working Party noted that a number of Member States have not met the deadline for the implementation of the Directive and it was not clear when this would actually be fully implemented.[1317] Implementation of this Directive is still, at the time of the writing, not ensured in all Member States.

It is not only the proposal for an EU PNR system that surprises; it is also that "this is in a number of areas almost the exact mirror of the transatlantic PNR system."[1318] The data categories to be retained, the retention arrangements that recall the US 'active' and 'dormant' database distinction, the periods of the retention,[1319] and the purposes of the PNR collection uncannily remind the EU-US PNR Agreement.[1320] The question is therefore: why an EU PNR system which all the more looks like a replica of the US Agreement so vigorously opposed?

The reasons that the Commission gives in its Explanatory Memorandum seem "a little ambiguous."[1321] It starts by explaining that only a limited number of Member State have adopted a PNR system, and thus "the potential benefits of an EU wide scheme in preventing terrorism and organised crime are not fully

---

[1316] EVELIEN BROUWER, THE EU PASSENGER NAME RECORD SYSTEM AND HUMAN RIGHTS: TRANSFERRING PASSENGER DATA OR PASSENGER FREEDOM? 25 (CEPS Working Document No. 320, September 2009).

[1317] ARTICLE 29 WORKING PARTY, OPINION 9/2006 ON THE IMPLEMENTATION OF DIRECTIVE 2004/82/EC OF THE COUNCIL ON THE OBLIGATION OF CARRIERS TO COMMUNICATE ADVANCE PASSENGER DATA.

[1318] Javier Argomaniz, *When the EU Is the "Norm-taker": The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms*, 31 JOURNAL OF EUROPEAN INTEGRATION 119, 130 (2009).

[1319] Concerning the data retention period the EDPS noted in his Opinion on the Framework decision: "the period of 13 years is comparable to the retention period of 15 years in the most recent agreement with the United States. The EDPS has always understood that this long retention period was only agreed upon because of strong pressure by the US Government to have a much longer period than 3.5 years, not because it was in any stage defended by the Council or the Commission. There is no reason to transpose such a compromise —that only has been justified as a necessary result of negotiations — to a legal instrument within the EU itself." *See* Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes OJ C 110/1 of 1 May 2008, ¶ 103.

[1320] As Article 29 Working Party elegantly put it "The proposal is closely modelled on the EU-US PNR agreement signed in July 2007 and many features of the present draft are similar to that agreement." *See* ARTICLE 29 WORKING PARTY, WORKING PARTY ON POLICE AND JUSTICE, JOINT OPINION ON THE PROPOSAL FOR A COUNCIL FRAMEWORK DECISION ON THE USE OF PASSENGER NAME RECORD (PNR) FOR LAW ENFORCEMENT PURPOSES, PRESENTED BY THE COMMISSION ON 6 NOVEMBER 2007.

[1321] Brouwer, *The EU Passenger Name Record System and Human Rights: Transferring Passenger Data or Passenger Freedom?*, *supra* note 1316, at 4.

realised."[1322] At the time of the proposal, the UK was the only country in the EU collecting PNR data.[1323] According to the Commission's Explanatory Memorandum, "the UK was able to report numerous arrests, identification of human trafficking networks and gaining of valuable intelligence in relation to terrorism in the two years of the operation of its pilot [PNR] project."[1324] A more specific account of these alleged successes of PNR in the UK is, however, missing in the Explanatory Memorandum. Denmark and France had also laid down relevant legislation, but they were not collecting any data yet. Surprisingly enough, the Commission speaks then of the need for a harmonised approach concerning PNR:

> "Action by the EU will better achieve the objectives of the proposal because a harmonised approach makes it possible to ensure EU wide exchange of the relevant information. Also, it makes it possible to provide for a harmonised approach towards the outside world."[1325]

Furthermore, the Commission seems convinced of the necessity of a PNR system as a counter-terrorism tool because of its 'worldwide acceptance': "the use of PNR data is growing and is increasingly seen as a mainstream and necessary aspect of law enforcement work."[1326] This trend is, according to the Commission, the result of three parameters:

> "First, international terrorism and crime are a serious threat to society and steps need to be taken to deal with these problems. The access to and analysis of PNR data is one such step that is considered necessary from a law enforcement perspective. Second, recent technological developments have rendered such access and analysis possible, which was inconceivable some years ago… And lastly, with the rapid increase of international travel and the volume of passengers, the electronic processing of data in advance of the arrival of passengers largely facilitates and expedites security and border control checks since the risk assessment process is done before arrival. It provides the opportunity to law enforcement to focus only on those passengers

---

[1322] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, *supra* note 356, at 2.
[1323] House of Lords European Union Committee, *The Passenger Name Record (PNR) Framework Decision*, *supra* note 1303, at 5.
[1324] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, *supra* note 356, at 2.
[1325] *Id.* at 7.
[1326] Commission Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries, *supra* note 18, at 3.

for whom they have a fact-based reason to believe that they might pose an actual risk to security, rather than making assessments based on instinct, pre-conceived stereotypes or profiles."[1327]

The true reasons for the development of an EU PNR system, however, may lie elsewhere. First, one should not underestimate the EU's quest for reciprocity. This is possibly explained by the fact that all the three PNR Agreements with the US displayed an asymmetry of power[1328] or some form of 'unilateralism'. As one author points out correctly, the Agreements

"did not authorise the *exchange* of PNR data, but only the *one-way* access of US government agencies to European data."[1329]

It cannot surprise, therefore, that all three PNR Agreements contained a reciprocity clause. As Argomaniz observes, one Commission official noted that "it would have been difficult to explain to European passengers that US authorities would receive more information than their own national services."[1330] In his Oral Evidence to the House of Lords Jonathan Faull, then Director-General for Justice, Freedom and Security stated:

"The Commission's view is that it would make sense to have a PNR system for ourselves in the European Union on the basis of which we would then have very good grounds for saying to our American partners, 'This must be completely reciprocal. We have our PNR system, you have yours'."[1331]

It should not go unnoticed that the Commission had reciprocity requests in mind also when it tabled its own PNR proposal. In particular, in its Explanatory Memorandum it recognised that it cannot be excluded that some countries may request reciprocal access to PNR data relating to flights from the EU to their territories, "even though in practice" it found "such an eventuality very remote."[1332]

Second, political scientists argue that the negotiation processes with the US authorities had an impact on EU institutions taking part in them, such as the Commission. Thus, according to a commentator,

---

[1327] *Id.* at 5.
[1328] Argomaniz, *supra* note 1318, at 126–127.
[1329] Bert-Jaap Koops, *Law, Technology, and Shifting Power Relations*, 25 BERKELEY TECH. L.J. 973, 987 (2010).
[1330] *See* Argomaniz, *supra* note 1318, at 130.
[1331] House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, *supra* note 945, paragraph 150.
[1332] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, *supra* note 356, at 6.

> "[a]s expected by sociological institutionalist authors, the Commission approach to the transmission of passenger's data for security purposes has been fundamentally shaped by its interaction with other international actors; leading to learning practices, compliance and full normative socialization."[1333]

As the Commission admits in the Explanatory Memorandum, on the basis of an exchange of information with the US, "the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes."[1334] This is further illustrated by the fact that an EU PNR system was supported by the EU negotiating agents (i.e. the Commission and the Presidency), but not by other EU actors, such as the European Parliament, the Article 29 Working Party, and the EDPS, who had been kept excluded from the negotiations with the US.[1335] Another political scientist agrees that the negotiations on the US PNR influenced the EU institutions, but in a slight different way. He argues that since dialogue at the transatlantic level is taking place through informal networks, personal relationships are formed among policy-makers, which is demonstrated, according to the same author, from "the gradual substitution of formal instruments with less formal contracts and informal understandings shaping the content of formal agreements" and the internal policy-making.[1336] Since he fails, however, to provide adequate evidence to prove that, his argument remains rather unsubstantiated.

4.3 The reaction of the "outsiders": Article 29 Working Party, EDPS, Fundamental Rights Agency, European Parliament

The proposal on the Framework decision establishing an EU PNR regime was received with fierce criticisms by the Article 29 Working Party, the EDPS, the Fundamental Rights Agency (FRA), and the European Parliament. In particular, the Article 29 Working Party in its joint opinion with the Working Party on Police and Justice could not have been more critical:

[1333] Argomaniz, *supra* note 1318, at 130.
[1334] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, *supra* note 356, at 2.
[1335] Argomaniz, *supra* note 1318, at 132.
[1336] Pawlak, *supra* note 1312, at 14.

> "The current proposal must be considered a further milestone towards a European surveillance society in the name of fighting terrorism and organised crime."[1337]

Along the same lines, the EDPS noted:

> "The proposal ... is a further step in a movement towards a routine collection of data of individuals who are in principle not suspected of any crime. As mentioned above, this evolution is taking place at international and European level."[1338]

And continued:

> "The measures apply to all passengers, be they under investigation or not by law enforcement authorities. It constitutes proactive research, on an unprecedented scale."[1339]

The reaction of the Article 29 Working Party, the EDPS, and the European Parliament to the EU PNR proposal is even more severe than the criticisms they voiced for the EU-US PNR Agreements. Both the Working Party and the EDPS demand that an EU PNR system must be "demonstrably necessary."[1340] The necessity of the EU-US PNR Agreements was also questioned, but given the position of the European airlines and the pressure exercised by the US authorities for the prompt conclusion of an agreement, the Working Party, the EDPS, and the Parliament were focusing more on the substantial assessment of the relevant provisions interfering with the right to data protection. Having to deal with an EU measure this time, their position became necessarily stricter: the Commission has to prove beyond doubt the added value and necessity of an EU PNR system.[1341]

Another criticism raised against the proposal by all four institutions concerned the profiling aspirations of the EU PNR regime. As the EDPS noted eloquently, contrary to the API data that are supposed to help identifying individuals, PNR data "would contribute to carrying out risk assessments of persons, obtaining intelligence

---

[1337] Article 29 Working Party, Working Party on Police and Justice, *Joint Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes, Presented by the Commission on 6 November 2007*, *supra* note 1320.

[1338] Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, *supra* note 376, at ¶ 8.

[1339] *Id.* at ¶ 30.

[1340] *Id.* at ¶ 26; Article 29 Working Party, Working Party on Police and Justice, *Joint Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes, Presented by the Commission on 6 November 2007*, *supra* note 1320, at 5.

[1341] *Id.* at 6.

and making associations between known and unknown people."[1342] The purpose of a PNR system does not only cover the catching of *known* persons but also the locating of persons that may be of interest for law enforcement reasons.[1343] A substantial part of FRA's Opinion concerning the draft PNR Framework decision is dedicated to a human rights' assessment of the 'profiling purposes' of the proposal, mainly on the basis of the prohibition of discrimination found in Article 21 EUCFR.[1344] The European Parliament also raises similar concerns in its Resolution.[1345]

Finally, there were numerous problems identified in the proposal: the excessive categories of data to be retained,[1346] the disproportionate retention periods,[1347] the uncertainty on the individuals' rights,[1348] the questions on the applicable legal framework,[1349] and the role of PIUs and intermediaries.[1350]

4.4 The proposal for an EU PNR Directive: Back to European Standards?

Upon the entry into force of the Lisbon Treaty on 1 December 2009, the Commission's proposal of 6 November 2007 for a Framework decision on PNR, which had not been adopted by the Council by that date, became obsolete. On 2 February 2011, the Commission introduced a new proposal, this time for a Directive, on the establishment of an EU PNR system.[1351] The proposal is based once again on

---

[1342] Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, *supra* note 375, at ¶ 6.
[1343] *Id.* at ¶ 15.
[1344] FUNDAMENTAL RIGHTS AGENCY, OPINION ON THE PROPOSAL FOR A COUNCIL FRAMEWORK DECISION ON THE USE OF PASSENGER NAME RECORD (PNR) DATA FOR LAW ENFORCEMENT PURPOSES 7 (October 28, 2008), *available at* http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf.
[1345] European Parliament resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes P6_TA(2008)0561.
[1346] *Id.;* Article 29 Working Party, Working Party on Police and Justice, *Joint Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes, Presented by the Commission on 6 November 2007*, *supra* note 1320.
[1347] *Id.*
[1348] *Id.*
[1349] Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, *supra* note 375, at ¶ 39.
[1350] *Id.* at ¶ 68.
[1351] 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.

the need for harmonisation of the Member States relevant provisions. This time, however, the Commission seems slightly more convincing. According to the Explanatory Memorandum, the UK already has its PNR system, while France, Denmark, Belgium, Sweden and the Netherlands have either enacted relevant legislation or are currently testing using PNR data. According to the Commission, several other Member States are also considering setting up PNR systems that might diverge in several respects. The Commission, therefore, foresees as a result, the creation of up to 27 considerably diverging PNR systems that "would result in uneven levels of protection of personal data across the EU, security gaps, increased costs and legal uncertainty for air carriers and passengers alike."[1352]

The Commission explained that it carried out an Impact Assessment for the development of an EU PNR system where four options were examined: a) refraining from addressing the issue at EU level and maintaining the status quo; b) regarding the structure of the PNR system, either decentralised collection and processing of data by Member States or centralised collection and processing of data at EU level; c) concerning the purposes of the proposed measure, either access for the prevention, detection, investigation and prosecution of terrorist offences and serious crime only or access for the prevention, detection, investigation and prosecution of terrorist offences and serious crime and other policy objectives; and d) addressing the modes of transport to be covered by the proposed measure, either air carriers or air, sea and rail carriers.[1353] The Impact Assessment concluded that "a legislative proposal applicable to travel by air with decentralised collection of PNR data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and other serious crime was the best policy option."[1354]

The draft Directive is based on Articles 82 (1) (d)[1355] and 87 (2) (a) TFEU,[1356] and regulates "the transfer by air carriers of PNR data of passengers of international flights to and from the Member States, as well as the processing of that data, including

[1352] *Id.* at 4.
[1353] *Id.* at 4.
[1354] *Id.*
[1355] Article 82 (1) (d) provides: "The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures to: (d) facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions."
[1356] Article 87 (2) (a) reads: "…the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures concerning: (a) the collection, storage, processing, analysis and exchange of relevant information."

its collection, use and retention by the Member States and its exchange between them."[1357] Law enforcement authorities are allowed to process PNR data for the purpose of preventing, detecting, investigating, and prosecuting terrorist offences and serious crimes,[1358] which are subject to a prison sentence of at least three years. Member States are, once again, required to establish a single designated unit (PIU) responsible for handling and protecting the data.[1359] The categories of PNR data to be transmitted are the same 19 elements found in the EU-US PNR Agreements and the draft Framework decision. Air carriers are obliged to transmit the PNR data 24 to 48 hours before the scheduled time for flight departure, and immediately after flight closure.[1360] The data are to be retained for a period of five years: initially for 30 days after their transfer to the relevant PIU, and subsequently, after being masked out and anonymised they will be held for another five years.[1361] The draft Directive prohibits the collection and use of sensitive data.[1362] It obliges carriers to transmit PNR data exclusively by the "push" method, meaning that the Member States will not have direct access to the carriers' IT systems.[1363] The result of the processing of PNR data by a PIU should be exchanged, where necessary, with the PIUs of other Member States.[1364] PNR data may also be transferred by Member States to third countries in limited circumstances and on a case-by-case basis.[1365] The national data protection authorities will be responsible for advising and monitoring how PNR data are processed.[1366]

Concerning the data protection safeguards, the draft Directive is very brief, even more economical than the draft Framework decision: it lays down merely that "every passenger shall have the same right to access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress as those adopted under national law in implementation of Articles 17, 18, 19 and 20 of the Framework Decision on the Protection of Personal Data Processed in the Framework

[1357] Article 1 (1) of the draft PNR Directive.
[1358] Article 1 (2) of the draft PNR Directive.
[1359] Article 3 of the draft PNR Directive.
[1360] Article 6 of the draft PNR Directive.
[1361] Article 9 of the draft PNR Directive.
[1362] Article 11 (3) of the draft PNR Directive.
[1363] Article 6 (1) of the draft PNR Directive.
[1364] Article 7 of the draft PNR Directive.
[1365] Article 8 of the draft PNR Directive.
[1366] Article 12 of the draft PNR Directive.

of Police and Judicial Co-operation in Criminal Matters.[1367] Member States are, further, required to ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.[1368] Finally, the draft Directive prohibits the transfer of PNR data by PIUs and competent authorities to private parties in Member States or in third countries.[1369]

It has to be acknowledged that the Commission has been very careful concerning the drafting of the Directive on PNR in an attempt to address the severe criticisms raised against the draft Framework decision. In this respect, it has taken great pains to prove that a PNR system at the EU level has indeed an added value. The Commission's justification is long and in many aspects irrelevant as it cites an extensive amount of information and statistical data on criminal offences in general in the Member States (approximately 14 000 per 100 000 population); on the economic cost of crimes ($2 508 368 218 in industrialised economies); on the annual cocaine-related deaths in the EU (1000); on the number of opioid users in Europe (1,35 million); and, on the total Member States' expenditure relating to illicit drugs (EUR 4.2 billion).[1370] Concerning the value of a PNR system, it notes, first, that the absence of harmonised provisions on the collection and processing of PNR data at EU level, explains why detailed statistics on the extent to which such data are useful to combat terrorism and crime are not available.[1371] It then goes on, to provide information from the experience of the use of PNR by other countries. A great part of the analysis is no more than anecdotal.[1372] Furthermore, statistical data prove, according to the Commission, that with respect to drugs, "the majority of seizures are made due to the

[1367] Article 11 (1) of the draft PNR Directive.
[1368] Article 11 (5) of the draft PNR Directive.
[1369] Article 11 (6) of the draft PNR Directive.
[1370] 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, *supra* note 407, at 2.
[1371] *Id.* at 6.
[1372] *Id.* at 5. For instance, *see* the example given on the usefulness of credit card information "which is part of the PNR data" and "may enable law enforcement authorities to identify and prove links between a person and a known criminal or criminal organisation." According to the Explanatory Memorandum, "cartels were importing drugs to several destinations in Europe. They were using drugs swallowers who were themselves trafficked persons. They were identified on the basis of having bought the ticket with stolen credit cards on the basis of PNR." Another reported success of PNR analysis is that it "uncovered a group of human traffickers always travelling on the same route. Using fake documents to check in for an internal flight, they would use authentic papers to simultaneously check in for another flight bound for a third country. Once in the airport lounge, they would board the internal flight. Without PNR it would have been impossible to unravel this human trafficking network."

use of PNR data in real-time and pro-actively."[1373] The Commission's analysis, on the necessity of an EU PNR system, despite being clearly more elaborated than the one provided in the draft Framework decision, fails once again to convince.[1374]

Regarding the substance, despite some "visible improvements" compared to the draft Framework decision, such as, for instance, the reduced retention period, the implementation of a 'push' system, and the exclusion of any collection and processing of sensitive data, the draft Directive does not add much. In particular, it is lamentable that the data protection legal framework applicable to the PNR Directive is the Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters, even in the post-Lisbon context.[1375] The draft Directive may not remind the transatlantic PNR Agreements anymore, but its data protection standards are not truly European either.

5. Going Deep: Is Air Passenger Surveillance a Privacy or a Data Protection Issue?

5.1 Why getting it wrong between privacy and data protection can affect the standards of judicial review: The case of PNR

Fundamental rights concerns have been at the very heart of the PNR conflict. Air passenger screening has been alleged to interfere with the right to privacy, the right to data protection, the prohibition of discrimination,[1376] the right to move (travel)

[1373] According to the Commission, Belgium reported that 95% of all drugs seizures in 2009 were exclusively or predominantly due to the processing of PNR data. Sweden reported that 65-75% of all drugs seizures in 2009 were exclusively or predominantly due to the processing of PNR data. The United Kingdom reported that during a period of 6 months in 2010, 212 kilos of cocaine and 20 kilos of heroine were seized exclusively or predominantly due to the processing of PNR data.

[1374] 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, Brussels, 25 May 2011 at ¶ 10; ARTICLE 29 WORKING PARTY, OPINION 10/2011 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.

[1375] *Id.*

[1376] *See* below.

freely,[1377] and the right to property.[1378] The debate on the privacy and data protection implications of the Agreement highlights once again, the conceptual misconceptions that follow the two rights, presented in Chapter 2, and further discussed with connection to the EU centralised databases and the Data Retention Directive. This time, however, the consequences of not recognising that data protection can have a hard core and operate also negatively, as a tool of non-interference –without the need to fall back to the right to privacy- are seen more clearly, and demonstrate why the time has come for data protection to be accepted as a fully-fledged fundamental right in the EU legal order.

The Opinion of Advocate General Léger in the *PNR* cases analysed above is illuminating and the present analysis will use it as an example. The Advocate General started his assessment on the Parliament's plea that the 2004 PNR Agreement infringed the fundamental rights to privacy and data protection, by noting:

> "In the course of laying down that case-law, the Court has found it necessary to incorporate the right to respect for private life into Community law. The right to protection of personal data constitutes one of the *aspects* of the right to respect for private life and is therefore protected by Article 8 of the ECHR, including in the Community legal order, through the prism of the general principles of law."[1379]

It can be assumed from this pronouncement that the Advocate General follows the general trend of the Court of Justice, presented in Chapter 3, which regards data protection as an aspect of the right to respect for private life. This is not the problem, however. It has been argued elsewhere that the present thesis does not purport to focus on the nature of the relationship between the rights to privacy and data protection, and on questions whether data protection is a 'separate', 'autonomous' right, or an aspect of privacy. The present thesis focuses instead on data protection as a fundamental right. The Advocate General is not, therefore, to be criticised for this approach. What will be criticised, however, is the pattern that he follows to determine whether there is a disproportionate infringement with fundamental rights:

> "I shall examine whether the PNR regime constitutes an infringement of the right to respect for private life by following the analytical pattern which stems

[1377] Kite, *supra* note 997, at 1410; Dummer, *supra* note 961, at 599.
[1378] Kite, *supra* note 997, at 1416; Dummer, *supra* note 961, at 602.
[1379] Opinion of Advocate General Léger, Joined Cases C-317/04 and C-318/04 , *supra* note 168, para 209 (emphasis added).

from the wording of Article 8 of the ECHR. Thus, after establishing whether that regime constitutes interference in the private life of airline passengers, I shall determine whether that interference is duly justified."[1380]

Having noted that data protection is an aspect of the right to privacy; the Advocate General went on to examine whether there was an interference to this on the basis of Article 8 ECHR and using the formula employed by the ECtHR. This means, however, that the issues the EU-US PNR poses, have to be addressed on the basis of the right to private life. Here, come the difficulties, though. How do PNR data, which include data on names, contact details, baggage, etc, interfere with the private life of the passengers? Do they reveal anything private that might affect the personal or family life of the person? To the extent that they are sensitive data concerning someone's health problems for instance, this is true. But, what about the great bulk of the data? On the other side of the Atlantic, such questions are similarly perplexing. As US Homeland Security Secretary Chertoff noted in his address to the European Parliament concerning PNR:

"It's basic information. It's nothing that's particularly confidential by its very nature."[1381]

Such an assertion is confirmed by the US Constitutional law and the case-law of the Supreme Court, discussed above. To put it differently, PNR data cannot be expected to enjoy a 'reasonable expectation of privacy'.[1382] Privacy protection in Europe certainly differs significantly from the US notion of 'reasonable expectation' but the problem with PNR data still remains. If we exclude the category of sensitive data for the moment, we are faced with the difficulty on how to explain conceptually the harm caused by PNR on the right to private life. If this cannot be seen, then the collection of PNR data presents no interference, or even if it does, its proportionality cannot be assessed on the right basis. This is the fallacy committed by the Advocate General. Having to assess PNR on the basis of Article 8 ECHR, he had to engage in a discussion on why PNR affects the right to privacy. It is true that he found it easy to confirm the existence of interference in the private life of the passengers:

"The existence of interference in private life [...] is hardly in doubt, in my opinion. It seems clear to me that the consultation, the use by CBP and the

[1380] *Id.*, at para 210.
[1381] US Homeland Security Secretary Michael Chertoff's Address before the Civil Liberties Committee of the European Parliament, *supra* note 3.
[1382] *See* analysis above.

making available to the latter of airline passengers' data from air carriers' reservation systems located within the territory of the Member States constitute interference by public authorities in the private life of those passengers."[1383]

Even so, the Advocate General noted some difficulties:

"[...] the interference in the private life of airline passengers appears to me to be established *even though certain PNR data elements, considered in isolation, could be regarded as not individually infringing the privacy of the passengers concerned*."[1384]

However, it was more difficult for him to explain why such interference would be disproportionate. This can be seen in his reasoning, but also in his conclusions. Concerning his reasoning, the Advocate General had to make a distinction based on the nature of the data, because "the review of proportionality by the European Court of Human Rights varies according to parameters such as the nature of the right and activities at issue, the aim of the interference and the possible presence of a common denominator in the States' legal systems."[1385] Therefore, according to the Advocate General:

"As regards the nature of the right and activities at issue, where the right is one which *intimately affects the individual's private sphere*, such as the right to confidentiality of health-related personal data, the European Court of Human Rights seems to take the view that the State's margin of appreciation is more limited and that its own judicial review must be stricter."[1386]

Following the Advocate General's reasoning, PNR data, in principle, do not seem to "intimately affect the individual's private sphere", and consequently the margin of appreciation left to the executive would be wider and the judicial review more lenient. Taking into account the importance of the purpose of using PNR data, for the fight against terrorism,[1387] the conclusion reached by the Advocate General that the interference with the right to private life is not disproportionate, cannot be surprising. It is lamentable, however, that by using the right to privacy to make his assessment,

---

[1383] Opinion of Advocate General Léger, Joined Cases C-317/04 and C-318/04 , *supra* note 168, para 211.
[1384] *Id.*, at para 212(emphasis added).
[1385] *Id.*, at para 228.
[1386] *Id.*, at para 229 (emphasis added).
[1387] The Advocate General noted: "where the aim of the interference is to maintain national security or to combat terrorism, the European Court of Human Rights tends to allow States a wide margin of appreciation." *See Id.*, at para 230.

the Advocate General decided that the level of judicial review should be decreased in the name of the fight against terrorism.

5.2 Why PNR is more about data protection? The limited value of privacy in PNR

Which issues fall under privacy and which under data protection in the case of PNR? Let us start the analysis from the right to privacy. First of all, the right to privacy covers this portion of PNR data that contain information relating to the personal or family life of the person concerned, namely mainly sensitive data. To the extent therefore that PNR data reveal confidential information about potential health problems of the individual, or her credit card details, or the contact details of her family or friends, or her religious beliefs based on the meal she ordered during the flight, they fall within the scope of the right to privacy under Article 7 EUCFR and Article ECHR. Such data are covered also by the right to data protection that provides for enhanced protection in these cases. The rest of the PNR data, however, it is difficult to justify why they would fall under privacy, as the Advocate General's analysis, discussed above, has demonstrated.

An argument that can be made, further, is that the right to privacy applies insofar as PNR data is confidential commercial information of the air carrier, or better the confidentiality of this information finds its legal basis on the contractual rights and obligations arising from the contract concluded between the air carrier and the customer/passenger. This, however, means that the application of a fundamental right (privacy) is made subject to private law obligations assumed in the process of a contract concluded between two private parties. Certainly, the air carrier is bound by the obligation not to reveal the information communicated to it for the execution of the contract, but this is a mere contractual private law obligation that cannot be put at equal standing with the public law purpose of combating terrorism and serious crime. The question has been brought up before US Federal Courts, and, not surprisingly, they held that, "without a specific showing of damages, passengers have no cause of action against airlines that disclose or transfer PNR data to third parties."[1388]

[1388] For a more detailed analysis *see* Rasmussen, *supra* note 946, at 567.

More particularly, in *re Northwest Airlines Privacy Litigation*, passengers claimed that the transfer by Northwest of PNR data to the National Aeronautical and Space Administration to assist in a study of airline security, violated the airline's privacy policy.[1389] The US Court, however, dismissed the claim stating that "general statements of policy are not contractual."[1390] This demonstrates that an argument based on the passengers' privacy arising from the contractual obligations assumed by the air carriers has limited value in the use of PNR data for law enforcement purposes.

Such problems do not arise with regard to the right to data protection. All the categories of data contained in PNR constitute information related to an identified person, and therefore personal data, regardless of whether they are connected to the intimate private sphere of the person or not. An assessment therefore of the Agreement on the basis of the specific data protection principles enshrined in the fundamental right to data protection would not encounter the difficulties found in the Advocate General's analysis on the basis of the right to privacy. But, the right to data protection is not only useful for a finding of interference in the PNR case. At the end of the day, such an interference was found by the Advocate General, albeit with some difficulties, with regard to the right to privacy as well. The most important contribution of data protection lies in the assessment of whether the interference posed by PNR was disproportionate or not. Data protection provides for specific principles, on the basis of which such an assessment can be undertaken: among others, purpose limitation, proportionality concerning the amount of data processed and the periods of their retention, consent of the data subject, individual due-process rights, enhanced protection of sensitive data, and independent supervision.

The present thesis argues that data protection is, therefore, the correct fundamental rights' basis to assess data transfers as the one in the PNR case for two reasons: First, because all PNR data, despite their level of intimacy, are personal data, and consequently their transfer constitutes an interference with the right to data protection, avoiding problems of the level of intimacy of the data and making fundamental rights' protection subject to private law obligations. Second, the specific data protection principles are the right forum to discuss whether such interference is

[1389] Re *Northwest Airlines Privacy Litigation*, No. Civ.04-126(PAM/JSM), 2004 WL 1278459, at 1 (D. Minn. June 6, 2004).
[1390] *Id.*

disproportionate, instead of the general privacy right that cannot catch all the problems posed by the PNR transfer.

Furthermore, there is another argument that points toward the applicability of the right to data protection in the case of PNR. While a particular harm can be identified with regard to the right to privacy in PNR transfers only in connection with the limited cases of sensitive data; the harms posed on the different data protection principles are more than visible: using commercial data for law enforcement purposes is not only a change of purpose, it is a "purpose deviation";[1391] the quantities of data processed and the extensive retention periods turn the 'function creep' into a "function rush".[1392] Moreover, the processing, collation, and comparison of these data against unknown patterns make the "powerlessness" and "vulnerability"[1393] of the data subjects even greater, especially taking into account that they lack any meaningful form of participation in this processing of their information.

That being said, it should be reiterated that the main problem is not found in the Advocate General's assumption that data protection is an aspect of privacy instead of an autonomous right itself. The main problem is in the analytical pattern he follows for his fundamental rights' assessment via Article 8 ECHR. Certainly, it has to be recognised that at the time of the ruling, the EU Charter of Fundamental Rights was not a binding legal instrument, and data protection did not enjoy the status of an EU fundamental right yet. Thus, it is understandable that the Advocate General had to follow the path of Article 8 ECHR via the "prism of the general principles of law in the Community legal order."[1394] Under the current developments though, with the entry of the force of the Lisbon Treaty, the assessment of PNR should be based on the fundamental right to data protection (Article 8 EUCFR) as this can be limited according to the conditions of Article 52 (1) EUCFR. On this basis, a substantive fundamental rights' assessment of PNR will be undertaken in the following section.

[1391] Els de Busser, *EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU Be Serving Its Citizens an American Meal ?*, 6 UTRECHT LAW REVIEW 86, 95 (2010).
[1392] Koops, *supra* note 1329, at 989.
[1393] Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, *supra* note 94, at 1423.
[1394] *See* Mendez, *supra* note 1134, at 131.

6. PNR: A Substantive Assessment

6.1 Assessing PNR under the scope of the right to data protection

Since the 2007 PNR is the one currently in force, this will be assessed regarding its compliance with the right to data protection. As explained above, the assessment will be carried out on the basis of Article 8 EUCRFR in conjunction with Article 52 EUCFR directly and not through the path followed under now by the ECJ via the prism of the general principles of law. Article 52 (1) reads as follows:

> "Any 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."

According to Article 52 (1), a) any limitation of a right of the Charter should b) be provided for by law; c) meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; d) be necessary e) be subject to the principle of proportionality; and, f) respect the essence of the right. The analysis below will employ this formula with regard to the right to data protection.

a. Limitation of the right to data protection

In order to assess, whether a limitation of the right to data protection exists, as a preliminary step, it must be examined if this right is applicable at all to the transmission of PNR data by air carriers to the United States Department of Homeland Security and the processing of these data by the latter. The fundamental right to data protection indeed applies in the present case because all the fields of data contained in the Passenger Name Record are 'personal data' to the extent that they are related to an identified person; and, second, the collection the transmission of the data to DHS by the air carriers, as well as the operations undertaken on the data by the latter constitute 'processing' of personal data.

A clarification is further needed at this point for the sake of accuracy of the analysis. In the case of PNR data transfer, we are dealing with two phases of processing of the same data: at the first phase, the airlines collect the data for the purpose of issuing the ticket and transmit them to DHS; at the second, DHS receives the data from the airlines, stores and processes them for its own purposes. Both the airline companies and DHS are 'controllers' in the sense of Article 2 (d) of the Data Protection Directive, since they determine the purposes and means of the processing of the data. Therefore, we have two different controllers processing the same data, therefore we have two distinct processing operations. The method of the transfer of data 'push' or 'pull' does not seem to make any significant difference, DHS is in both cases 'push' or 'pull' a controller.[1395] The assessment of these two different types of processing is not an easy task. The ECJ dealt with it in its 2006 judgment and attempted to separate them in order to decide in which pillar each one falls. The conclusion it reached based on the separation of the two types of processing was regrettable from many points of view, as seen above. Such a strict separation, as the one followed by the Court for its legal basis analysis, may be obsolete in the post Lisbon era. This thesis will not adopt it for a further more important reason: apart from the obligation laid on air carriers to transmit the PNR data to DHS, the rest of the 2007 PNR Agreement (and the previous Agreements) deals with the processing of the data by DHS. This will be, therefore, the centre of the present analysis.

The right to data protection is, therefore, applicable in the case under examination. It needs, furthermore, to be established whether this right has been limited by the 2007 PNR Agreement. The conditions for the transmission of PNR data to DHS and their processing thereof poses limitations to the following data protection principles: the purpose limitation principle, the adequacy principle, the fairness principle concerning the period of the retention of the data, and the non-discrimination principle. It also interferes with the due process and individual participation rights of the data subject, which form an inherent part of the right to data protection. Finally, it raises questions with regard to sensitive data to the extent they are also transmitted, and the consent of the data subject. Whether these limitations are proportionate to the aim they seek to achieve, will be examined further in the analysis.

[1395] *Contra* Ntouvas who argues that "... CBP accessing European PNR data through a 'push' system makes it a 'recipient', whereas a pull system makes it a 'controller', to which Dir. 95/46/EC is applicable. *See* Ntouvas, *supra* note 1046, at 88.

b. Provided by law

Following the established case-law of the European Court of Human Rights, any interference with a fundamental right should be provided by law that is foreseeable and accessible. It is difficult to see how these two conditions are satisfied with regard to the 2007 Agreement. As mentioned above, the Agreement forms part of three different documents: the Agreement signed by both parties, the DHS letter, and the EU letter replying to the DHS. Amongst them, the DHS letter is the most important because it lays down how it handles the collection, use and storage of PNR. As discussed above, DHS does not set down obligations of the US authorities concerning the PNR data; it merely provides assurances of their use according to the DHS letter. Moreover, DHS informs that subsequent US legislation might materially affect the statements made in its letter;[1396] in this case it assures that it will advice the Commission accordingly.[1397] This obviously goes against any legal certainty.

The legal basis in question, therefore, not only lacks accessibility and foreseeability for the individuals; also, its binding nature is disputable. Of course, the transfer of PNR data is provided by law, but how those are further handled is buried in legal uncertainties based on the assurances provided by the DHS letter. Furthermore, the rights of the data subjects and the conditions for their exercise are also uncertain, since they form part of the DHS assurances. For these reasons, the 2007 PNR Agreement does not satisfy the 'provided by law' requirement of Article 52 (1) EUCFR.[1398]

Since the requirement 'provided by law' is not satisfied, the analysis could have well stopped there, but for the sake of providing a complete fundamental rights assessment of the 2007 Agreement it will go on.

[1396] DHS letter Article I.
[1397] *Id.*
[1398] Along the same lines the conclusion of the Art. 29 Working Party. *See* Article 29 Working Party, *Opinion 5/2007 on the Follow-up 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 Concluded in July 2007*, *supra* note 1183.

c. 'Meet objectives of general interest recognised by the Union'

According to the DHS letter, EU PNR are used for the following purposes: 1) preventing and combating terrorism and related crimes; 2) other serious crimes, including organized crime, that are transnational; 3) flight from warrants or custody from the crimes described above; 4) for the protection of the vital interests of the data subject or other persons; 5) in criminal judicial proceedings, or 6) as otherwise required by law.

Preventing and combating terrorism and other serious transnational crimes is, without doubt, an objective of general interest recognised by the Union. The same can be argued for the protection of the vital interests of the data subject, although it is not clear how such an objective is pursued using PNR data. As regards, the two last, namely the use in criminal proceedings or as otherwise required by law, they are too vague and open, and do not seem, therefore, to satisfy the requirement 'meet objectives of general interest' as they currently stand.

d. Necessary

As seen in previous Chapters, the Strasbourg Court requires that the interference 'corresponds to a pressing social need' for the necessity requirement to be satisfied. The necessity of the PNR system is one of the most disputed issues. In fact, with connection to the EU's own PNR system, this was the major concern voiced from the EDPS, the Art. 29 Working Party, and the European Parliament.[1399] Their common conclusion was that the necessity of a PNR system is far from proven within the EU. The concerns they expressed apply regarding the 2007 EU-US PNR Agreement as well. Since the later, however, regulates solely the US PNR system, assessing its necessity is somewhat a quaint exercise. This is because such an assessment has to be based on the Americans' statements of the necessity of a Passenger Screening System for their internal security. Such a necessity has been overstressed by US policy makers, such as the Secretary of Homeland Security, Michael Chertoff, in some cases with exaggerated statements, such as

[1399] *See* above.

> "... despite the strong links we[Americans]'ve forged with our European partners to protect our nations, we still remain handcuffed in our ability to use all available resources to identify threats and stop terrorists."[1400]

Some American scholars seem to think along the same lines. For instance, Ravich notes:

> "Airline passenger profiling represents a necessary policy decision to ensure liberty through security. The central theory underlying modern profiling systems is that September 11 could have been prevented or at least contested. This article accepts that theory as fact and views as necessary efforts to lawfully screen airline passengers more thoroughly than had been done until September 11."[1401]

The necessity and effectiveness of datamining and profiling will be examined in a separate section below. For the time being, in order to examine the necessity of the PNR system, two further issues have to be addressed: first, its effectiveness, and second whether other less extensive alternatives are available. The assessment of both is not easy taking into account that it is the US system that is under examination. It should be noted, however, that the European Court of Human Rights allows for a wide margin of appreciation where the aim of the interference is to maintain national security,[1402] or to combat terrorism.[1403] Since the predominant aim of collecting and using PNR is combating terrorism and serious crime, it can be accepted in principle that the executive enjoys a wide margin in the present case to justify the necessity of a PNR system.

That being said, a more concrete examination raises numerous questions on such a necessity. First, information on the effectiveness of PNR is very limited. As the House of Lords Report points out:

> "The degree to which the collection, retention and transfer of PNR data is acceptable depends of course on its value in combating terrorism and other serious cross-border crime, but there is a major obstacle to the assessment of

[1400] Chertoff, *supra* note 959.
[1401] Ravich, *supra* note 965, at 56–57.
[1402] *Leander v. Sweden.*
[1403] *Murray v. the United Kingdom*, judgment of 28 October 1994, Series A, no. 300-A, § 47 and 90. In that case, the objective of combating terrorism provided justification for the recording by the armed forces of personal details concerning the first applicant. The Court of Human Rights pointed out that it is not for it 'to substitute for the assessment of the national authorities its own assessment of what might be the best policy in the field of investigation of terrorist crime'.

that value. The more serious the crime, the more reluctant the authorities are to disclose details of what information was used, and in what way, to prevent its commission or to arrest and bring to trial those suspected of committing it. Even when a case comes to court, the prosecuting authorities have to disclose only such evidence as is essential for them to prove their case or as the law requires them to disclose to the defence; and this will not necessarily include all the information about the data and methods that have led to the identification of the suspects."[1404]

In a letter of 14 May 2007 to the European Parliament, Secretary of Homeland Security Chertoff provided eight examples that "illustrate the necessity of analyzing and sharing PNR data."[1405] Among them only one refers to terrorism and in a rather indirect way.[1406] Some of the rest have mere anecdotal value and fail to convince regarding their seriousness.[1407] Second, the question of whether less intrusive measures are available in the US is also very difficult to answer. Nevertheless, it should be noted that the necessity of a passenger screening system has not been in general questioned by Congress, with most Government Accountability Office (GAO) Reports focusing solely on the management and implementation challenges faced by the CAPPS II and Secure Flight programmes.[1408] The House of Lords European Union Committee concluded in its Report that:

"...having received no evidence to the contrary, we are prepared to accept that PNR data constitute a valuable weapon in the fight against terrorism and

[1404] House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, *supra* note 945, paragraph 19.
[1405] Chertoff, *supra* note 959.
[1406] *Id.* "In June 2003, using PNR data and other analytics, one of our inspectors at Chicago's O'Hare airport pulled aside an individual for secondary inspection and questioning. When the secondary officers weren't satisfied with his answers they took his fingerprints and denied him entry to the United States. The next time we saw those fingerprints—or at least parts of them—they were on the steering wheel of a suicide vehicle that blew up and killed 132 people in Iraq."
[1407] *Id.* "At Boston Logan Airport in April 2006, CBP officers used PNR data to identify two passengers whose travel patterns exhibited high-risk indicators. During the secondary interview process, one subject stated that he was travelling to the United States on business for a group that is suspected of having financial ties to Al Qaeda. The examination of the subject's baggage revealed images of armed men, one of which was labelled "Mujahadin.""
[1408] *See* for instance United States Government Accountability Office, *Testimony Before the Committee on Commerce, Science, and Transportation, U.S. Senate, AVIATION SECURITY, Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, *supra* note 1000; United States General Accounting Office, *supra* note 992.

serious crime, and that their continued use is both necessary and justified."[1409]

The present thesis will not adopt such a resilient approach. Since no robust evidence is available concerning the effectiveness of PNR, the necessity of their use is far from proven.

e. Proportionate

The proportionality test, which examines whether the measure is (dis)proportionate to the purposes it seeks to achieve, is crucial for the determination of the fundamental rights' compliance of the measure at stake. The present analysis will discuss the proportionality of the 2007 EU-US PNR Agreement on the basis of the fair information principles it interferes with.

The examination will start from the purpose limitation principle, which has been described many times in the present thesis as the 'keystone' of data protection law. Purpose limitation requires that personal data are collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. As in the case of the Data Retention Directive discussed above, the use of commercial airline data for law enforcement purposes is a purpose incompatible with their initial collection necessary in order to purchase the airline ticket. The function creep question arises therefore again in the present context. In fact, this is a central problem identified in all the different cases of information processing discussed in the present thesis. It can be accepted, that in specific cases information already available for other/ commercials reason will be used for law enforcement purposes provided that such a use respects the 'essence' of the right to data protection. Such an examination will follow in the next section. For the time being, a second deviation of the purpose limitation principle can be identified in the case of PNR. The Agreement merely refers to the transfer of data in order to combat terrorism and serious transnational crime, but these data can be shared with further US authorities and used for unrelated purposes, such as to prevent transmittable diseases or in criminal

[1409] House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, *supra* note 945, paragraph 23.

proceedings in general or as otherwise required by law.[1410] These purposes are unduly vague and the data subject, even if informed about her collection of PNR data for counter-terrorism purposes, lacks any meaningful control and foreseeability on the further aims for which her data might be used. This clearly deviates from the purpose of the Agreement, which is the fight against terrorism and serious crime. Moreover, the proportionality of the use of PNR data for very broad and totally unrelated to the fight against terrorism and crime purposes laid down as the basis for the conclusion of the Agreement is questionable.

Another fair information principle that is interfered with in the PNR case is the adequacy principle. This requires that personal data must be adequate, relevant and not excessive in relation to the purposes for which they were collected and further processed. The 2007 PNR Agreement requires the transmission of 19 data categories. While the 19 data fields do not really introduce an improvement compared to the 34 of the 2004 Agreement, it can be argued that they are necessary for fighting terrorism, as the Advocate General contended in his Opinion, since "obtaining sufficient information may enable a State's security services to prevent a possible terrorist attack",[1411] and "the need to profile potential terrorists may require access to a large number of pieces of data."[1412] Setting aside the questions on legitimate profiling that will be addressed later, even if this argument of the Advocate General is accepted, it is not enough to determine that the proportionality of the limitation of the principle of adequacy. There are certain data fields in the Passenger Name Record that raise questions as to why they are required. For instance, the DHS letter requires the transmission of general remarks such as OSI (Other Service-related Information), SSI (Special Service Information), and SSR (Special Service Requests). These data most probably will reveal information concerning racial and ethnic origin (for instance on the meal ordered) or the health life of the person (for instance if a wheelchair was requested). DHS assures that it employs an automated system which filters those sensitive PNR codes and terms and does not use this information, unless required in exceptional cases,[1413] but this is far from enough. It should be reminded, first, that concerning this type of sensitive information the right to privacy applies as well,

[1410] DHS letter Article I.
[1411] Opinion of Advocate General Léger, Joined Cases C-317/04 and C-318/04 , *supra* note 168, para 238.
[1412] *Id.*
[1413] DHS letter Article III.

because it is related to the personal and family life of the person. Second, the relevant data protection rule prohibits the processing of such information, because it can lead to discrimination. For these reasons, it is difficult to see how the proportionality principle is complied with in connection to the adequacy information principle.

A further data protection principle stipulates that data should be kept no longer than is necessary for the purposes for which they were collected or further processed. The retention of PNR data for fifteen years raises questions regarding its proportionality. As seen above, the Commission has identified three uses of PNR: the reactive, the real-time, and the proactive. Reactive and real-time use cannot justify a retention period of fifteen years. The same applies to their proactive use, and the drawing of terrorist patterns and profiles. Even if it can be accepted that data can be retained longer for this purposes, a period of fifteen years is excessive. The distinction between 'active/analytic' and 'dormant' status does not make a difference to this conclusion. As the Article 29 Working Party has pointed out

> "from a data protection point of view there is no difference between active and so-called dormant periods of access. As long as personal data are accessible, albeit in only very limited and restricted cases during a dormant period, they remain available in a database and can be accessed and processed by DHS."[1414]

Normally data protection laws allow for the processing of data when the data subject has given unambiguously his consent. The proponents of the use of PNR data for law enforcement purposes might argue that such a processing is permissible because the data subject has given his consent. This argument, however, is based on false premises. The data subject has given his consent for the processing of his data from the airline company in order to purchase a ticket. No consent has been given for the transfer of the data to law enforcement authorities and it is not in any case the data subject the one that transfers them so as to be in a position to withdraw his consent. The issue is not, therefore, a matter of consent. It is a 'take it or leave it' deal. As one airline CEO put it:

> "You want to travel on the airline system? You give up your privacy. You don't want to give up your privacy? Don't fly. Your privacy isn't equal to the safety

[1414] Article 29 Working Party, *Opinion 5/2007 on the Follow-up 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 Concluded in July 2007*, *supra* note 1183.

of the rest of us...If there's anything about you that you don't want me to know, then don't fly."[1415]

Such a notion of consent is false and, therefore, consent can have in the PNR case very limited value.[1416]

f. Respect the 'essence' of the right to data protection

The blanket collection of PNR data of every passenger, irrespective of whether she is considered to be under suspicion or not and their processing in order to develop terrorist profiles, without granting adequate procedural rights to the individuals concerned to challenge it, touches the very 'essence' of the right to data protection. As analyzed in detail in Part 1, data protection as a fundamental right in the EU legal order should have a 'hard core' that determines which limitations are impermissible. In the case of the 2007 EU-US PNR Agreement under examination, this 'hard core' has been touched by the disproportionate limitations of numerous fair information principles discussed above.

7. Data-mining PNR data

7.1 Questions on Efficiency

The infringements of the right to data protection identified above tell only one part of the story of the PNR data. This focuses, in particular, on the collection and retention of the data by the US authorities in order to fight terrorism. However, there

[1415] Robert Crandall, *Security for the Future: Let's Get Our Airlines Flying, 2001 Airline Security and Economic Symposium*, 67 J. AIR L. & COM. 9, 19 (2002).

[1416] As Commissioner Bolkestein has noted "relying on consent alone would have been bad data protection, even if it resolved the legal problems. We would have been saying to people: it is up to you to decide whether to go to the US, but we are washing our hands entirely of what happens to your personal data once it gets to the US." *See* Address of Frits Bolkestein to LIBE Committee, EU/US talks on transfers of airline passengers' personal data, *supra* note 112.

is another part of the story regarding PNR that has not been dealt with yet: this concerns the use of such data.

As the Commission stated in its 2010 Communication on the global approach to transfers of PNR data to third countries,[1417] PNR data can be used re-actively, at the real-time and proactively. The two last uses are particularly interesting: PNR are necessary to create patterns (pro-active use) which will then be employed to identify "unknown" suspects (real-time use).[1418] This allegedly constitutes the main use and the added value of the processing of PNR data by law enforcement authorities. Such a practice is normally referred to as data-mining.

What exactly is data-mining? Numerous definitions of data-mining have been offered. [1419] The CATO Report on data-mining and counter-terrorism defines it as

> "the process of searching data for previously unknown patterns and using those patterns to predict future outcomes."[1420]

A 2007 Report for Congress[1421] explains:

> "[d]ata mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. These tools can include statistical models, mathematical algorithms, and machine learning methods (algorithms that improve their performance automatically through experience, such as neural networks or decision trees). Consequently, data mining consists of more than collecting and managing data, it also includes analysis and prediction."[1422]

Data-mining has been used extensively as a marketing strategy to increase sales.[1423] The rationale is simple. As the Congressional Report explains, its added

---

[1417] Commission Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries, s*upra* note 18.
[1418] *Id*.
[1419] Dempsey and Flint note eloquently: "terms such as "data-mining," "pattern analysis," "knowledge extraction," "dataveillance," and other ambiguous and sometimes loaded terms mean different things to different people. James Dempsey & Lara Flint, *Commercial Data and National Security*, 72 THE GEORGE WASHINGTON LAW REVIEW 1459, 1464 (2004). *See* also Taipale, *supra* note 962, at 21; Joseph Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1736 (2006).
[1420] JEFF JONAS & JIM HARPER, EFFECTIVE COUNTERTERRORISM AND THE LIMITED ROLE OF PREDICTIVE DATA MINING 1 (CATO Report, 2006).
[1421] JEFFREY SEIFERT, DATA MINING AND HOMELAND SECURITY: AN OVERVIEW (LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2007).
[1422] *Id.* at 1.
[1423] Jonas & Harper, *supra* note 1420, at 6. As a GAO Report reveals data-mining is also used by 52 US federal departments and agencies for a variety of reasons, such as to improve service or performance; detect fraud, waste, and abuse; analyze scientific and research information; manage human resources; detect criminal activities or patterns; and analyze intelligence and detect terrorist

value is clear compared to simpler analytical tools that use, for instance, a verification-based approach:

> "For example, a user might hypothesize that a customer who buys a hammer, will also buy a box of nails. The effectiveness of this approach can be limited by the creativity of the user to develop various hypotheses, as well as the structure of the software being used. In contrast, data mining utilises a discovery approach, in which algorithms can be used to examine several multidimensional data relationships simultaneously, identifying those that are unique or frequently represented. For example, a hardware store may compare their customers' tool purchases with home ownership, type of automobile driven, age, occupation, income, and/or distance between residence and the store. As a result of its complex capabilities, two precursors are important for a successful data-mining exercise; a clear formulation of the problem to be solved, and access to the relevant data."[1424]

Furthermore, data-mining in direct marketing works effectively because the sample used is very broad: millions of consumer-behaviour patterns are analyzed in order to draw up the profile of each customer.[1425] She can be subsequently targeted by individualised offers or advertisements. Even if the data-mining identifies a wrong pattern, the harm made is minimal: the marketer might lose a dollar for the imperfectly aimed-mail and the customer a moment of her time.[1426]

The story is not the same, however, when it comes to counter-terrorism data-mining. In this context, data-mining is not only ineffective; it is also disproportionate with regard to its effects. Starting from its potential benefits, experts explain that data-mining is not useful for counter-terrorism, because one necessary pre-requisite is missing: terrorist patterns.[1427]

> "With a relatively small number of attempts every year and only one or two major terrorist incidents every few years -each one distinct in terms of planning and execution- there are no meaningful patterns that show what behaviour

---

activities. *See* UNITED STATES GENERAL ACCOUNTING OFFICE, REPORT TO THE RANKING MINORITY MEMBER, SUBCOMMITTEE ON FINANCIAL MANAGEMENT, THE BUDGET, AND INTERNATIONAL SECURITY, COMMITTEE ON GOVERNMENTAL AFFAIRS, U.S. SENATE, DATA MINING- FEDERAL EFFORTS COVER A WIDE RANGE OF USES 2 (May 2004).

[1424] Seifert, *supra* note 1421, at 2.

[1425] Jonas & Harper, *supra* note 1420, at 7.

[1426] *Id.*

[1427] *Id.*

> indicates planning or preparation for terrorism. Unlike consumers' shopping habits and financial fraud, terrorism does not occur with enough frequency to enable the creation of valid predictive models."[1428]

This means that data-mining is not an effective means to predict terrorism because it lacks "well-constructed algorithms based on extensive historical patterns."[1429] Such lack cannot be remedied by collecting the data of virtually everyone, as in the case of PNR. Having every air traveller's data does not mean that it will prevent a terrorist attack. Contrary to direct marketing where consumers' profiles are based on "as many as millions of previous instances of the same particular behaviour",[1430] terrorist profiles cannot predict accurately, since the incidents of terrorist attacks are – fortunately- very few.[1431] But even it is assumed that an accurate terrorist profile can be drawn based on information about known terrorists, it does not necessarily mean that the system "will identify a suspect whose behaviour significantly deviates from the original model."[1432] As noted eloquently by a commentator,

> "[o]ne corollary to limited frequency and individuality of terrorist acts within the United States is that national security data mining efforts... tend to be backwards focused... Government data mining seems similarly likely to be fighting yesterday's battles—a problem that commercial data miners face to a far less extent, since the characteristics of desirable consumers are likely to change far less rapidly than those of terrorists."[1433]

Commentators often distinguish between subject-based and pattern-based analysis of data.[1434] Subject-based data analysis aims to "trace links from known individuals or things to others."[1435] Pattern-based analysis is more probabilistic: it

---

[1428] *Id.* at 8.
[1429] *Id.*
[1430] Seifert, *supra* note 1421, at 3.
[1431] Ramasastry, *supra* note 1253, at 773.
[1432] Seifert, *supra* note 1421, at 3.
[1433] Fred H Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARVARD CIVIL RIGHTS - CIVIL LIBERTIES LAW REVIEW 435, 474 (2008). Cate explains that since the 9/11 terrorists used box cutters to take over the airplanes, the US government banned box cutters and everything that resembled them, such as nail clippers, nail files, pocket knives, etc; when a terrorist attack was attempted by using detonating explosives hidden in the shoes, the TSA officials began screening shoes; when British officials uncovered the plot to blow up airplanes with liquid explosives, restrictions on the liquids carried on planes were introduced. "In each case, the government's action was wholly reactive to the most recently demonstrated threat, rather than proactive in responding to known threats whether or not they had been attempted."
[1434] Dempsey & Flint, *supra* note 1419, at 1466; Jonas & Harper, *supra* note 1420, at 6.
[1435] Jonas & Harper, *supra* note 1420, at 6.

aims to develop patterns that will be used to unveil previously unknown suspects.[1436] The main use of PNR and their alleged added value is found exactly in the pattern-based analysis that can be performed on this set of data.[1437] For a subject-based analysis, which is based on suspicion and not on uncertain patterns, the use of API data would have been enough.

However, data-mining is very limited: it can merely reveal patterns; it cannot explain the significance of these patterns or identify a casual relationship.[1438] It can only provide information about the '*what'* and not about the '*why'*.[1439] Checking, for instance, whether a passenger purchased a one-way ticket or a ticket within a short time before the departure of the flight, because such a behaviour was followed by the 9/11 terrorists, is not enough to reveal future terrorists. People might purchase one-way tickets within a short time before the departure for various reasons that have nothing to do with terrorism (for instance, because of the nature of their profession, their personal circumstances or because they merely found a good offer, etc.).[1440]

Moreover, whatever the technological capabilities of the data-mining system, its effectiveness depends also on other factors, especially, where 'commercial data' are used, as in the case of PNR. In this context, a first problem has to do with the accuracy and the completeness of the data (data quality).[1441] As the Congressional Report notes

> "[d]ata quality is a multifaceted issue that represents one of the biggest challenges for data mining."[1442]

In this context,

> "[t]he presence of duplicate records, the lack of data standards, the timeliness of updates, and human error can significantly impact the effectiveness of the more complex data mining techniques, which are sensitive to subtle differences that may exist in the data."[1443]

[1436] *Id.* Unlike subject-based analysis, pattern-based analysis is more characterised by prediction than by the traditional notion of suspicion.
[1437] *See* above.
[1438] Ramasastry, *supra* note 1253, at 770; Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GEORGIA LAW REVIEW 82, 42 (2005); Seifert, *supra* note 1421, at 3.
[1439] Dempsey & Flint, *supra* note 1419, at 1470.
[1440] Ramasastry, *supra* note 1253, at 770.
[1441] Seifert, *supra* note 1421, at 21.
[1442] *Id.*
[1443] *Id.*

Besides these reasons that can lead to limited data quality and therefore limited accuracy of the data-mining system, PNR data have an additional problem that can add to limited data quality: they are subjective. Unlike the API data that are found in the machine-readable part of the passport, PNR are filled in by the customers themselves when they make a reservation. This means that they can provide inaccurate or false data or even use fraudulent identification documents. In such instances, not only the patterns drawn are inaccurate; also wrong people might be identified as potential terrorists.[1444]

Finally, as experts point out, the statistical likelihood of false identifications (either false positives or false negatives) in data-mining make it prohibitive.[1445] In particular, even if it is assumed that a terrorist data-mining system works very accurately with a 99% accuracy rate –which is very difficult, taking into account the problems identified above- still the 1% of false negatives is unduly large with regard to the millions of travellers that fly from Europe to the US every year.

7.2 Fundamental rights affected

Unlike marketing data-mining that is normally efficient and with minimal negative effects, counter-terrorism data-mining does not merely have limited effectiveness; it also has serious consequences on fundamental rights. Three rights are mainly affected: the right to privacy, the right to data protection, and the prohibition of discrimination (Article 21 EUCFR).[1446]

Starting from the right to privacy, it has been contended that "data mining ... inevitably raises privacy issues."[1447] In particular, it is argued that

> "the greatest impact of data-mining on individual privacy is that individuals will change their behaviour as a result of their awareness that the government may,

[1444] Cate, *supra* note 1433, at 472.
[1445] Dempsey & Flint, *supra* note 1419, at 1497; Jonas & Harper, *supra* note 1420, at 8; Cate, *supra* note 1433, at 479; Seifert, *supra* note 1421, at 3; Ramasastry, *supra* note 1253, at 774; Steinbock, *supra* note 1438, at 6.
[1446] The EU Fundamental Rights Agency Opinion concerning the establishment of an EU PNR system focused exactly on these three rights. *See* Fundamental Rights Agency, *supra* note 1344, at 1.
[1447] TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE, US DEPARTMENT OF DEFENSE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 48 (TAPAC Report, March 2004).

without probable cause or other specific authorization, obtain access to myriad distributed stores of information about them."[1448]

This argument, which seems reminiscent of fears of a Big Brother surveillance society[1449] or of the concept of Panopticon, is quite general and cannot be tested in the PNR case.

More specific and concrete infringements are found with regard to the right to data protection. Besides, the problems posed on the purpose limitation principle analysed above, data-mining also raises questions regarding the due-process rights of the data subject. As Steinbock notes

"[t]he most striking aspect of virtually all antiterrorist... data mining decisions is the total absence of even the most rudimentary procedures for notice, hearing, or other opportunities for meaningful participation..."[1450]

Setting aside the consequences that data-mining might have on those individuals identified as potential terrorists because they fit the profiles (no-fly lists, terrorist investigations, arrest, greater scrutiny, inclusion in watch-lists,[1451] humiliation[1452]) that call for enhanced due-process rights, terrorist profiles raise more general due-process issues. "Profiling" is generally defined as the systematic association of sets of physical, behavioural or psychological characteristics with particular offences and their use as a basis for making law-enforcement decisions."[1453] How are terrorist profiles drawn up? What characteristics make a terrorist? How can someone disagree with a profile? Profiles are secret, because, the argument goes, that otherwise terrorists would try to evade them.[1454] How are they going to be then controlled that they are not abusive or discriminative? If they cannot be made known to the general public, why cannot they be controlled by the judiciary? For instance, a pattern-based

---

[1448] Cate, *supra* note 1433, at 477.
[1449] *See* Tzanou, *The EU as an Emerging "Surveillance Society": The Function Creep Case Study and Challenges to Privacy and Data Protection*, *supra* note 467; HOUSE OF LORDS, SELECT COMMITTEE ON THE CONSTITUTION, SURVEILLANCE: CITIZENS AND THE STATE (2nd Report of Session 2008–09).
[1450] Steinbock, *supra* note 1438, at 82.
[1451] Dempsey & Flint, *supra* note 1419, at 1471.
[1452] MARTIN SCHEININ, REPORT OF THE SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS WHILE COUNTERING TERRORISM ¶ 56 (A/HRC/4/26, January 29, 2007).
[1453] *Id.*, para. 33. *See* also Daniel Moeckli, *Terrorist Profiling and the Importance of a Proactive Approach to Human Rights Protection* (2006); Tuomas Ojanen, *Terrorist Profiling: Human Rights Concerns*, 3 CRITICAL STUDIES ON TERRORISM 295 (2010).
[1454] Daniel Solove, *Data Mining and the Security-Liberty Debate*, 74 UNIVERSITY OF CHICAGO LAW REVIEW 343, 359 (2008).

analysis could be reviewed by a court.[1455] This raises further questions: What should be the standard of review? When can terrorist data-mining be allowed and when not?

The issue of terrorist profiles was brought up in the seminal *Rasterfahndung* decision of the German Constitutional Court.[1456] The case concerned the notorious 'Rasterfahndung' ('dragnet investigation') implemented by police and intelligence agencies in Germany after the 9/11 terrorists attacks for the purpose of identifying Muslim terrorist sleepers.[1457] The programme was initiated after it became known that some terrorists that participated in the 9/11 attacks had been residing in Germany and attended German Universities.[1458] The criteria used for the screening were: male, aged 18 to 40, student or former student, of Islamic religious affiliation, coming from a country with predominantly Islamic population.[1459] These criteria would then be combined with further information in order to lead to the discovery of terrorist sleepers. In October 2001, the programme was approved by the 'Amtsgericht Düsseldorf' ('Düsseldorf Local Court') after the request of the police department of Düsseldorf pursuant to § 31 of the 'Polizeigesetz des Landes Nordrhein-Westfalen' ('Police law of the state North Rhine-Westphalia').[1460] According to the programme, universities, colleges, health and social insurance agencies, registry offices, the central registry of immigrants, employers and other institutions were asked to provide data,[1461] which were held at the 'Bundeskriminalamt' ('Federal Criminal Police Office'), in a file called 'Schläfer' ('Sleeper').[1462] It is estimated that only within the first four months of the programme the data of more than 30000 male students had been collected in Hamburg.[1463] Overall, around 8 million personal data of up to 300000 persons were gathered,[1464] and approximately 32000 people were identified as potential terrorist sleepers.[1465] It is worth noting that Rasterfahndung,

[1455] Dempsey & Flint, *supra* note 1419, at 1501.
[1456] BVerfGE 115, 320, 1 BvR 518/02, 4 April 2006.
[1457] *Id.,* para 9.
[1458] Verena Zöller, *Liberty Dies by Inches: German Counter-Terrorism Measures and Human Rights*, 5 GERMAN LAW JOURNAL 469, 487 (2004).
[1459] 1 BvR 518/02, *supra* note 516, para 8. *See* also Gabriele Kett-Straub, *Data Screening of Muslim Sleepers Unconstitutional*, 7 GERMAN LAW JOURNAL 967, 970 (2006).
[1460] Felix Müller & Tobias Richter, *Report on the Bundesverfassungsgericht's (Federal Constitutional Court) Jurisprudence in 2005/2006*, 9 GERMAN LAW JOURNAL 161, 179–180 (2008).
[1461] *Id.*
[1462] *Id.*
[1463] Kleine Anfrage der PDS zur Rasterfahndung, 18 Feb. 2002 Bundestagsdrucksache 14/8257. *See* also Zöller, *supra* note 1458, at 487.
[1464] 1 BvR 518/02, *supra* note 516, para 28.
[1465] *Id.*

despite its massiveness, did not lead to the opening of any criminal case for terrorist-related offenses.

The programme was challenged by a Moroccan student that had been screened. After his appeals were rejected in the lower courts, the student filed a complaint before the Federal Constitutional Court. The Constitutional Court held that the Rasterfahndung programme constituted a serious infringement of the fundamental right to informational self-determination.[1466]

According to the Court, all the information collected in the course of the programme was personal data regarding the religious affiliation, the nationality, the family status, and the field of study of the individuals concerned. This information was combined with other data sets in order to produce new information with "very intense personality relevance" ("besonders starke Persönlichkeitsrelevanz").[1467] "Personality profiles" ("Persönlichkeitsbilder") could be, thus, created[1468] and people were made subject to screening methods that had a "stigmatising effect" ("stigmatisierende Wirkung") and increased the risk of discrimination.[1469] The Court stated that a dragnet investigation targeting Muslim people could augment the stereotypes and stigmatise a whole group in the public perception.[1470] The Court also criticised the secrecy covering the programme,[1471] which implicated people that had no information about it[1472] and people that had never aroused any suspicion.[1473] Finally, the Court held that since the infringement of fundamental rights was serious, a "concrete threat" ("*konkret* Gefahr") was needed before such an investigation could be carried out.[1474]

The *Rasterfahndung* case is illuminating for the present discussion as well. The Constitutional Court found that the drawing up of terrorist profiles, such as those used by the programme interfered disproportionately with the right to informational self-determination. Similar concerns apply to the PNR case as well. The drawing up of predictive terrorist profiles interferes with the right to data protection, as understood by the German Constitutional Court through the concept of 'informational

[1466] *Id.,* para 37.
[1467] *Id.,* para 101.
[1468] *Id.,* para 106.
[1469] *Id.,* para 108.
[1470] *Id.*
[1471] *Id.,* para 110.
[1472] *Id.*
[1473] *Id.*
[1474] *Id.,* para 125.

self-determination', which was endorsed by the present study, because it goes against individual autonomy and makes the imbalance between data subject and data processor even greater. Furthermore, the criteria used in the Rasterfahndung programme were clearly discriminatory and could lead to the stigmatisation of a certain group of the population. While we do not know the criteria used for building up terrorist profiles in the case of PNR, a similar danger might exist. The DHS letter states that

> "to the extent that sensitive EU PNR data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual), as specified by the PNR codes and terms which DHS has identified in consultation with the European Commission, are included in the above types of EU PNR data, DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information."[1475]

However, the DHS letter points out that

> "If necessary, in an exceptional case where the life of a data subject or of others could be imperilled or seriously impaired, DHS officials may require and use... sensitive data. In that event, DHS will maintain a log of access to any sensitive data in EU PNR and will delete the data within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law. DHS will provide notice normally within 48 hours to the European Commission (DG JLS) that such data, including sensitive data, has been accessed."[1476]

Sensitive data are particularly important because they contain information, such as nationality, or religious beliefs that could lead to discrimination. In this context, terrorist data-mining might interfere with the prohibition of discrimination as laid down in Article 21 of the Charter.[1477] The FRA in its Opinion concerning the establishment of an EU PNR system is categorical at this point:

[1475] DHS letter Article III.
[1476] *Id.*
[1477] Article 21 (1) EUCFR provides: "Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited."

"[a]ny mass profiling using stereotypical assumptions based on racial or religious criteria should be conceived as unjustifiable."[1478]

Terrorist data-mining and profiling are, therefore, not only ineffective; they also have serious implications on human rights. As the FRA has correctly put it, "they affect thousands of innocent people, without producing concrete results."[1479] There is currently no concrete information on how PNR data are being data-mined and terrorist profiles are drawn, but there is an increased risk that such a practice goes against the essence of the fundamental right to informational self-determination and the prohibition of discrimination.

[1478] Fundamental Rights Agency, *supra* note 1344, paragraph 39. On ethnic profiling in general *see* also EU NETWORK OF INDEPENDENT EXPERTS ON FUNDAMENTAL RIGHTS, ETHNIC PROFILING (CFR-CDF. Opinion 4.2006, December 2006); Olivier De Schutter & Julie Ringelheim, *Ethnic Profiling: A Rising Challenge for European Human Rights Law*, 71 MODERN LAW REVIEW 358 (2008); FUNDAMENTAL RIGHTS AGENCY, TOWARDS MORE EFFECTIVE POLICING UNDERSTANDING AND PREVENTING DISCRIMINATORY ETHNIC PROFILING: A GUIDE (2010); OPEN SOCIETY, JUSTICE INITIATIVE, ETHNIC PROFILING IN THE EUROPEAN UNION: PERVASIVE, INEFFECTIVE, AND DISCRIMINATORY; Daniel Moeckli, *Discriminatory Profiles: Law Enforcement After 9/11 and 7/7*, 5 EUROPEAN HUMAN RIGHTS LAW REVIEW 517 (2005).

[1479] Fundamental Rights Agency, *Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) Data for Law Enforcement Purposes*, *supra* note 1344, paragraph 38.

Chapter 7. Terrorist Finance Tracking Programme

1. The SWIFT Affair: Timeline of Events

> *''We will direct every resource at our command to win the war against terrorists, every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence. We will starve the terrorists of funding.''*[1480]

1.1 Phase I: The secret operations

On 23 September 2001, two weeks after the 11 September attacks, the US President issued Executive Order 13224.[1481] The Order, which was characterised by President Bush as "draconian",[1482] declared national emergency because "the terrorist attacks in New York, Pennsylvania, and the Pentagon committed on September 11, 2001, [...] and the continuing and immediate threat of further attacks on United States nationals or the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States",[1483] and imposed financial sanctions to "foreign persons that support or otherwise associate with foreign terrorists."[1484] The Executive Order also demanded the Secretary of the Treasury to

> "make all relevant efforts to cooperate and coordinate with other countries, including through technical assistance, as well as bilateral and multilateral agreements and arrangements, to achieve the objectives of th[e] order, including

[1480] Statement of US President George Bush, September 24, 2001.
[1481] Executive Order 13224, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism", 66 Fed. Reg. 49,079 (Sept. 23, 2001).
[1482] *See* Laura Donohue, *Anti-terrorist Finance in the United Kingdom and United States*, 27 MICH. J. INT'L L. 303, 377 (2006). President Bush noted with regard to Executive Order 13224: "At 2:01 a.m. this morning, a major thrust of our war on terrorism began with the stroke of a pen. Today, we have launched a strike on the financial foundation of the global terror network... Just to show you how insidious these terrorists are, they oftentimes use nice-sounding, non-governmental organisations as fronts for their activities... If you do business with terrorists, if you support or sponsor them, you will not do business with the United States of America."
[1483] *Id.*
[1484] *Id.* at Section 1.

> [...] the sharing of intelligence about funding activities in support of terrorism."[1485]

Furthermore, Section 314 (a) of the US Patriot Act urged law enforcement authorities

> "to share with financial institutions information regarding individuals, entities and organisations engaged in or reasonably suspected...of engaging in terrorist acts or money laundering activities."[1486]

Based on the International Emergency Economic Powers Act of 1977 (IEEPA) and the Executive Order 13224, as implemented through the Global Terrorism Sanctions Regulations, the United States Department of the Treasury (UST) established the Terrorist Finance Tracking Programme (TFTP). Under the Programme, UST was authorized to require any person to furnish financial transaction data in connection with a terrorism investigation.[1487] The purpose was to identify, track, and pursue terrorists and their networks by unravelling their money flows.[1488] According to the US Treasury Department,

> "terrorists depend on a regular cash flow to pay operatives, arrange for travel, train new members, forge documents, pay bribes, acquire weapons, and stage attacks. In order to send money through the banking system, they often provide information that yields the kinds of concrete leads that can advance a terrorism investigation. This is why counterterrorism officials place a high premium on financial intelligence, including that derived from programs such as the TFTP, which has proved to be of inestimable value in combating global terrorism."[1489]

As James Gurule, Under Secretary for Enforcement of the US Department of Treasury stated at the Hearing before the Committee on Finance of the US Senate, "our

---

[1485] *Id.* at Section 6. The Order authorised the Secretary of Treasury to take such actions employing all powers granted to the President by the International Emergency Economic Powers Act (IEEPA) and the United Nations Participation Act (UNPA). *See Id.* at Section 7.

[1486] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No 107-56, 115 Stat. 272, 307. *See* Daryl Shetterly, *Starving the Terrorists of Funding: How the United States Treasury Is Fighting the War on Terror*, 18 REGENT U. L. REV. 327, 340 (2006); Donohue, *supra* note 1482, at 374.

[1487] According to the US Treasury Department "[t]he TFTP is firmly rooted in sound legal authority, based on statutory mandates and Executive Orders – including the International Emergency Economic Powers Act (IEEPA) and the United Nations Participation Act (UNPA)." *See* US Department of the Treasury, *Terrorist Financing Tracking Program: Fact Sheet*. The legal basis of TFTP is far from clear, not the least because Executive Order 13224 speaks only of freezing terrorist-related funds and asks the UST very broadly to share intelligence about funding activities in support of terrorism.

[1488] *Id.*

[1489] Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes - 'SWIFT'(2007/C166/09)- Terrorist Finance Tracking Program - Representations of the United States Department of the Treasury, OJ C 166/18 of 20.7.2007.

objective is ... to follow the money trail, and dismantle entire financial networks and channels from moving money to finance terror."[1490]

Private law entities of the financial sector were enlisted by UST in this effort.[1491] In particular, the US Treasury Department, seeking information on suspected international terrorist networks under the TFTP, started issuing administrative subpoenas to the US operations centre of the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[1492] SWIFT is a cooperative limited-liability company governed by Belgian law[1493] that operates a worldwide messaging system used to transmit financial transaction information. SWIFT supplies its customers, who are banks or other financial institutions, with automated, standardized messaging services and interface software aimed at transmitting financial messages between financial institutions worldwide.

According to the company's own data, SWIFT is used for the exchange of financial messages by more than 9,700 banking organisations, securities institutions and corporate customers in 209 countries.[1494] SWIFT was regarded by the US administration as the "the mother lode, the Rosetta stone of financial data",[1495] since its database contains billions of financial messages from all over the world. When the US Department of Treasury started targeting SWIFT with administrative subpoenas under the TFTP, the company had two operation centres located in SWIFT branches, one in Europe[1496] and one in the United States.[1497] All messages processed by SWIFT were stored and mirrored at both operation centres for 124 days, as a "back-up recovery tool" for customers in case of disputes between financial institutions or data loss. After this period the data was deleted.

[1490] Financial War on Terrorism: New Money Trails Present Fresh Challenges: Hearing Before the Committee on Finance, US Senate, 107th Cong. 5 (2002).
[1491] Shetterly, *supra* note 1486, at 339.
[1492] US Department of the Treasury, *supra* note 1487.
[1493] Its registered office is in La Hulpe.
[1494] *See* http://www.swift.com/info?lang=en.
[1495] *See* Justin Santolli, *Note: The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive*, 40 THE GEO. WASH. INT'L L. REV. 553, 561 (2008). According to media information, the idea to target SWIFT with administrative subpoenas for counter-terrorism purposes came from a conversation between a senior official of the US administration and a Wall Street broker, who pointed to the former the billions of international financial transactions included in SWIFT database.
[1496] In Zoeterwonde in the Netherlands.
[1497] In Culpepper in Virginia.

Administrative subpoenas are orders "from a government official to a third party, instructing the recipient to produce certain information."[1498] The advantage of using administrative subpoenas is that they can be issued as quickly as the development of an investigation requires, because they are issued directly by an agency official.[1499] The administrative subpoenas addressed to SWIFT by UST were very broad in nature. They demanded information on transactions which related or might relate to terrorism, related to x number of countries and jurisdictions, on y date, or "from … to …" dates ranging from one to several weeks.[1500] The geographical scope of the subpoenas was also very wide covering messages of inter-bank transactions within the US, to or from the US, as well as messages with no territorial connection to the US, such as messages exchanged within the EU.[1501]

As the Belgium Privacy Commission carefully explains, SWIFT messages "can be compared with an 'envelop' and a 'letter'."[1502] The 'envelop' ... contains non-identifying data of the sender, i.e. standardized data of the institution that issues the message, such as its BIC-code, data for the identification of the recipient institutions, and the date and time of the message. The 'letter' contains the actual message, i.e. information on the amount of the transaction, the currency, the value, the date, the beneficiary's name, the beneficiary's financial institution, the customer requesting the financial transaction and the customer's financial institution requesting the transaction. [1503] These data, however, which constitute personal data, are encrypted, and SWIFT does not have access to them. This meant that SWIFT could not search its

---

[1498] Hearing before the United States Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Homeland Security: "Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists" Testimony of Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice June 22, 2004, http://kyl.senate.gov/legis_center/subdocs/062204_brand.pdf. In general, an administrative subpoena is valid when the inquiry is within the authority of the agency, the demand is not too indefinite, and the information sought is reasonably relevant to the enquiry. *See* United States v. Allis-Chalmers Corp., 498 F. Supp. 1027, 1028-1030 (E.D. Wis. 1980), at 29.

[1499] *Id.* Rachel Brand argues that the ability to use an administrative subpoena eliminates "delays caused by factors such as the unavailability of an Assistant United States Attorney to immediately issue a grand-jury subpoena, especially in rural areas; the time it takes to contact an Assistant United States Attorney in the context of a time-sensitive investigation; the lack of a grand jury sitting at the moment the documents are needed (under federal law, the "return date" for a grand-jury subpoena must be on a day the grand jury is sitting); or the absence of an empanelled grand jury in the judicial district where the investigation is taking place, a rare circumstance that would prevent a grand-jury subpoena from being issued at all."

[1500] *See* BELGIUM PRIVACY COMMISSION, OPINION NO. 37/2006 OF 27 SEPTEMBER 2006 ON THE TRANSFER OF PERSONAL DATA BY THE CSLR SWIFT BY VIRTUE OF UST (OFAC) SUBPOENAS.

[1501] *Id.*

[1502] *Id.*

[1503] BELGIUM PRIVACY COMMISSION, DECISION OF 9 DECEMBER 2008, CONTROL AND RECOMMENDATION PROCEDURE INITIATED WITH RESPECT TO THE COMPANY SWIFT SCRL 33.

database for specific data requested by the Treasury Department, such as for instance on the basis of the name of a particular person.[1504] Furthermore, SWIFT stored copies of financial messages in its archiving system only for a period of 124 days; this storage period was considered too short by the UST for its investigations. For these reasons, a new arrangement had to be negotiated between SWIFT and the Department of Treasury.[1505] Pursuant to this, the messages relating to suspicious periods should be isolated, copied and protected from destruction in order to be usefully exploited by the US authorities.[1506] According to the agreement reached, SWIFT had to deliver from its US operation centre the data required under the subpoena to a so-called 'black box' owned by the US and retained at UST facilities; the US Treasury Department would perform, subsequently, its searches on the data transferred to the 'black box'.[1507] Finally, a number of further arrangements were agreed with the US authorities and SWIFT never challenged the administrative subpoenas before the courts since it appeared in general to be satisfied with the guarantees given by UST regarding the searches performed,[1508] and considered that there existed the risk that the American judge would have ruled that it was obliged to communicate all data without any restrictions.[1509] Ironically, the TFTP was going on secretly for six years and SWIFT had already been targeted and complied with 64 subpoenas by UST until the EU finally realised due to media disclosures.

[1504] *See* Waldemar Hummer, *Die SWIFT-Affaire US-Terrorismusbekämpfung Versus Datenschutz*, 49 ARCHIV DES VÖLKERRECHTS 203, 211 (2011).

[1505] Belgium Privacy Commission, *Decision of 9 December 2008, Control and Recommendation Procedure Initiated with Respect to the Company SWIFT Scrl*, *supra* note 1503, at 12.

[1506] *Id.*

[1507] *See* ARTICLE 29 WORKING PARTY, OPINION 10/2006 ON THE PROCESSING OF PERSONAL DATA BY THE SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION (SWIFT) 8–9.

[1508] Generally, those guarantees comprised: 1) the search orders performed in the black box were possible on the basis of specific, targeted investigation files concerning terrorist activities; 2) the assurances that the US authorities were using a definition of terrorism on the basis of the relevant provisions of international law; 3) the organization of an audit by the American Audit Booz, Allen & Hamilton; 4) the review of the extraction of the data by UST by two employees of Swift; and 5) the determination of confidentiality standards. *See* Belgium Privacy Commission, *Decision of 9 December 2008, Control and Recommendation Procedure Initiated with Respect to the Company SWIFT Scrl*, *supra* note 1503, at 13; Belgium Privacy Commission, *Opinion No. 37/2006 of 27 September 2006 on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas*, *supra* note 1500.

[1509] *See* Belgium Privacy Commission, *Opinion No. 37/2006 of 27 September 2006 on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas*, *supra* note 1500.

1.2 Disclosure and European reactions

On 23 June 2006, a series of articles in the *New York Times,*[1510] the *Wall Street Journal*,[1511] the *Los Angeles Times*,[1512] and the *Washington Post*[1513] revealed the secret TFTP scheme put in place since 2001, under which the US Department of Treasury in collaboration with the Central Intelligence Agency (CIA) had collected and analyzed for counter-terrorism purposes huge amounts of data from SWIFT's database.[1514]

The revelation caused a wave of criticisms[1515] in the EU. In a Resolution of 6 July 2006, the European Parliament having noted that "the information stored by SWIFT to which the US authorities have had access concerns hundred of thousands of EU citizens, as European banks use the SWIFT messaging system for the worldwide transfer of funds between banks, and … SWIFT generates millions of transfers and banking transactions on a daily basis",[1516] stressed that it strongly disapproved of "any secret operations on EU territory that affect the privacy of EU citizens"[1517] and that it was deeply concerned that such operations were taking place without the citizens of Europe and their parliamentary representation having being informed.[1518] In this respect, it asked the Commission, the Council and the European Central Bank (ECB) to "explain fully the extent to which they were aware of the secret agreement between SWIFT and the US government",[1519] and urged "the USA and its intelligence and security services to act in a spirit of good cooperation and notify their allies of any

[1510] Eric Lichtblau & James Risen, *Bank Data Is Sifted by U.S. in Secret to Block Terror*, THE NEW YORK TIMES (2006).
[1511] Glenn Simpson, *Treasury Tracks Financial Data In Secret Program*, THE WALL STREET JOURNAL (2006).
[1512] Josh Meyer & Greg Miller, *U.S. Secretly Tracks Global Bank Data*, LOS ANGELES TIMES (2006).
[1513] Barton Gellman et al., *Bank Records Secretly Tapped*, THE WASHINGTON POST (2006).
[1514] SWIFT responded the same day by issuing a statement on compliance policy, http://www.swift.com/about_swift/legal/compliance/statements_on_compliance/swift_statement_on_compliance_policy/index.page.
[1515] Courtney Shea, *A Need for Swift Change: The Struggle 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*, 8 J. HIGH TECH. L. 143, 155 (2008); Sarah Elisabeth Exten, *Major Developments in Financial Privacy Law 2006: The SWIFT Database Incident, and Updates to the Gramm-Leach-Bliley and Fair Credit Reporting Acts*, 3 ISJLP 649, 656 (2008); Jeremy Shrader, *Secrets Hurt: How SWIFT Shook Up Congress, the European Union, and the U.S. Banking Industry*, 11 NORTH CAROLINA BANKING INSTITUTE 397 (2007).
[1516] European Parliament resolution on the interception of bank transfer data from the SWIFT system by the US secret services (P6_TA-PROV(2006)0317).
[1517] *Id.*
[1518] *Id.*
[1519] *Id.*

security operations they intend to carry out on EU territory."[1520] Concerning the TFTP, the Parliament noted that access to data managed by SWIFT could reveal information on the economic activities of the individuals and the countries concerned with the danger of resulting to "large-scale forms of economic and industrial espionage."[1521]

Along the same lines, the Belgian Data Protection Authority found in its Opinion of 27 September that SWIFT made a "secret, systematic and large scale violation of the basic European principles of data protection, which went on for years",[1522] and as data 'controller' it failed to comply with its obligations, in particular, the duty to provide information to the data subjects, and to notify the Data Protection Authority of the processing.[1523]

In its Opinion of 22 November 2006, the Article 29 Working Party confirmed the finding of the Belgium Privacy Commission that SWIFT was a 'controller' of personal data under EU data protection law.[1524] According to the Party, however, SWIFT was not only to blame because it did not notify the transfer of financial data to UST neither to its customers nor to any data protection supervisory authority.[1525] The criticisms raised by the Working Party were even harsher and concerned SWIFT's own operational architecture. The Working Party held that:

> "By deciding to mirror all data processing activities *in an operating centre in the US*, SWIFT placed itself in a foreseeable situation where it is subject to subpoenas under US law."[1526]

In this regard, the further purpose SWIFT's data are used –i.e. for terrorist investigations- is "completely different from the original purpose and its treatment of the personal data involved, and may have direct consequences for the individuals whose personal data are being processed."[1527] The Working Party found that the principles of purpose limitation and compatibility, proportionality and

---

[1520] *Id.*
[1521] *Id.*
[1522] Belgium Privacy Commission, *Opinion No. 37/2006 of 27 September 2006 on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas*, *supra* note 1500.
[1523] *Id.*
[1524] Article 29 Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, *supra* note 1507, at 11.
[1525] *Id.* at 20.
[1526] *Id.* at 15.
[1527] *Id.*

necessity of the personal data processed were not respected.[1528] Regarding the TFTP, the Working Party held that

> "the hidden, systematic, massive and long-term transfer of personal data by SWIFT to the UST in a confidential, non-transparent and systematic manner for years without effective legal grounds and without the possibility of independent control by public data protection supervisory authorities constitutes a violation of fundamental European principles as regards data protection and is not in accordance with Belgian and European law."[1529]

In this respect, the Working Party called upon SWIFT to immediately take measures in order to remedy the illegal state of affairs, and to return to a situation where international money transfers are "in full compliance with national and European law,"[1530] or otherwise it could be made subject to sanctions imposed by the competent authorities in order to enforce compliance.

The EDPS also entered the discussion but from a slight different perspective: he was asked by the European Parliament to pronounce on the role of the European Central Bank (ECB) in the SWIFT case.[1531] On 1st February 2007, he issued his opinion on the matter.[1532] The EDPS explained that SWIFT is subject to cooperative oversight by the Central Banks of the Group of Ten countries (G-10 Group),[1533] among which the ECB, that is a member of this group.[1534] In 2002, the G-10 Group was informed by SWIFT about the data transfers to US authorities. However, considering that this issue fell outside the scope of its oversight role, and that it was bound by rules of professional secrecy, the ECB "did not address the consequences of the transfers to US authorities for personal data protection, and neither informed relevant authorities nor used its powers of moral suasion to urge

---

[1528] *Id.*
[1529] *Id.* at 26.
[1530] *Id.* at 27.
[1531] It should be recalled that in its Resolution of 6 July 2006, the European Parliament had asked the EDPS to "check as soon as possible whether, in accordance with Regulation (EC) No 45/2001, the ECB was obliged to react to the possible violation of data protection which had come to its knowledge."
[1532] EUROPEAN DATA PROTECTION SUPERVISOR, OPINION ON THE ROLE OF THE EUROPEAN CENTRAL BANK IN THE SWIFT CASE.
[1533] The G-10 Group is composed of the National Bank of Belgium, Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d' Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System (USA), represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System.
[1534] The major instrument for the oversight of SWIFT is 'moral suasion', and overseers can formulate recommendations to SWIFT.

SWIFT to do so."[1535] The EDPS recognised that the participation of ECB in the co-operative oversight on SWIFT as such did not confer to it the responsibilities of a 'controller', but nevertheless,

> "the secrecy that surrounded the data transfers carried out by SWIFT for more than 4 years is regrettable and calls for a clarification of both the oversight on SWIFT and the rules on confidentiality."[1536]

1.3 A temporary solution

What was next for TFTP after the severe EU criticisms following the revelation of the programme by media reports? As astutely put by a commentator, instead of an apology and the imminent termination of the TFTP activities, the US authorities managed to obtain the continuation of the scheme by sending a set of unilateral statements to the EU.[1537]

In particular, on 28 June 2007, UST sent a letter to the EU Council[1538] and the Commission containing eight pages of unilateral representations (the 'Representations') which described the controls and safeguards governing the handling, use and dissemination of data under the Treasury Department's Terrorist Financing Tracking Programme.[1539] Noting that the TFTP "represents exactly what citizens expect and hope their governments are doing to protect them from terrorist threats",[1540] the UST went on to explain why the Terrorist Finance Tracking Program was "grounded in law, carefully targeted, powerful and successful, and bounded by privacy safeguards."[1541] The US Treasury Department assured that:

> "[f]rom its inception, the TFTP has been designed and implemented to meet applicable U.S. legal requirements, to contribute meaningfully to combating global terrorism, and to respect and protect the potential commercial sensitivity

---

[1535] European Data Protection Supervisor, *Opinion on the Role of the European Central Bank in the SWIFT Case*, *supra* note 1532, paragraph 29.
[1536] *Id.* at 11.
[1537] Hummer, *supra* note 1504, at 204.
[1538] Letter from United States Department of the Treasury regarding SWIFT/Terrorist Finance Tracking Programme (2007/C 166/08), OJ C 166/17 of 20.7.2007.
[1539] Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes — 'SWIFT' (2007/C 166/09) Terrorist Finance Tracking Program - Representations of the United States Department of the Treasury, OJ C 166/18 of 20.7.2007.
[1540] *Id.*
[1541] *Id.*

> of and privacy interests in the SWIFT data held in the United States… The programme contains multiple, overlapping layers of governmental and independent controls to ensure that the data, which are limited in nature, are searched only for counterterrorism purposes and that all data are maintained in a secure environment and properly handled."[1542]

According to the US Treasury Department, the assertion that the data processed does not contain sensitive data seems enough for UST to justify that no infringement of the Data Protection Directive took place in the SWIFT case: While the financial transaction records provided by SWIFT under compulsion of subpoena

> "may include identifying information about the originator and/or recipient of the transaction, including name, account number, address, national identification number, and other personal data... [i]t would be highly unusual for SWIFT financial records to include 'sensitive' data as referred to in Article 8 of Directive 95/46/EC."[1543]

For the rest, the Treasury Department guarantees that the data security principle is safeguarded under the TFTP because

> "the SWIFT data are maintained in a secure physical environment, stored separately from any other data, and the computer systems have high-level intrusion controls and other protections to limit access to the data solely as described herein."[1544]

Furthermore, the Representations assure that the TFTP does not involve data mining or any other type of algorithmic or automated profiling or computer-filtering,[1545] and that information derived from the SWIFT data is shared "under strict controls" with other US agencies in the intelligence and law enforcement communities to be used exclusively for counter-terrorism purposes.[1546] Concerning the rights of redress of the data subject the US Representations are quite ambiguous. The Treasury Department contends that such rights are not available because

> "responding to a privacy-related inquiry from a natural person as to whether information about that individual is included in the database would require, in almost all instances, accessing data that would never be accessed in the normal

[1542] *Id.*
[1543] *Id.*
[1544] *Id.*
[1545] *Id.*
[1546] *Id.*

operation of the TFTP. Such access would be inconsistent with the TFTP requirement that every search have a pre-existing nexus to terrorism. Finally, because there is no alteration, manipulation, deletion or addition of the data within the searchable database, there exists no basis to 'rectify' any information."[1547]

This means essentially that individuals do not have any rights of access to their data held under the TFTP, because access to the TFTP system is restricted only to counter-terrorism purposes (!). Uncertainties are also created regarding the period of retention of the SWIFT data as the Representations merely guarantee that this is

"a function of numerous, well-established factors, including investigative requirements, applicable statutes of limitation, and regulatory limits for claims or prosecution."[1548]

In any case, it is provided that non-extracted data received from SWIFT "after the date of publication of these Representations will be deleted by the Treasury Department not later than five years after receipt by the Treasury Department."[1549]

Finally, the UST invited the EU to appoint in consultation with the Treasury Department "an eminent European person" to confirm that the program is implemented consistent with the unilateral representations for the purpose of verifying the protection of EU-originating personal data, and to monitor that processes for deletion of non-extracted data have been carried out.

The EU replied to UST by sending a letter signed by the Commission and the Council welcoming the unilateral Representations and the opportunity that was given to the European Union to "have its views and concerns duly reflected in the Representations."[1550] It further informed the Treasury Department that it would begin the process of identifying appropriate candidates for the position of the "eminent European".[1551]

Indeed, on 7 March 2008, the Commission announced the designation of Judge Jean-Louis Bruguière as the SWIFT/TFTP "eminent European person."[1552]

[1547] *Id.*
[1548] *Id.*
[1549] *Id.*
[1550] Reply from European Union to United States Treasury Department — SWIFT/Terrorist Finance Tracking Programme (2007/C 166/10), OJ C 166/26 of 20.7.2007.
[1551] *Id.*
[1552] Commission press release announcing the designation of Judge Jean-Louis Bruguière as the SWIFT /TFTP "eminent European person" IP/08/400, 7 March 2008,

Judge Bruguière produced two Reports on TFTP in December 2008[1553] and January 2010[1554] where he found that the program was respecting, in general, the safeguards included in the Representations.

Meanwhile on 20 July 2007, SWIFT obtained registration for the Safe Harbor programme of the US Department of Commerce.[1555] The EU welcomed this development as it meant that SWIFT would be in compliance with its respective legal responsibilities under EU data protection law.[1556]

1.4 SWIFT's new architecture: The need for a new arrangement

After the media disclosure of TFTP, both the Belgium Privacy Commission and the Article 29 Working Party found that SWIFT was in breach of its obligations under the Data Protection Directive and the Belgian data protection law. In particular, the Working Party criticised SWIFT for mirroring its data in an operating centre in the US, and thus, placing itself under the jurisdiction of the US authorities.[1557] In order to address these criticisms, SWIFT announced on 4 October 2007 that it would restructure its messaging architecture.[1558] The new architecture, which would start being operational as from 1 January 2010 would store the EU originating financial data solely in Europe,[1559] thus excluding them from being targeted with subpoenas

---

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/400&format=HTML&aged=0&language=en&guiLanguage=en.

[1553] Summary of the First Annual Report on the Processing of EU Originating Personal Data by the United States Treasury Department For Counter Terrorism Purposes, Terrorist Finance Tracking Programme, Judge Jean-Louis Bruguière, http://www.statewatch.org/news/2011/apr/eu-usa-tftp-swift-1st-report-2008-judge-bruguiere.pdf

[1554] Second Report on the Processing of EU-Originating Personal Data by the US Treasury Department for Counter-terrorism purposes, TFTP, Judge Jean-Louis Bruguière, http://www.statewatch.org/news/2010/aug/eu-usa-swift-2nd-bruguiere-report.pdf.

[1555] Press Release, SWIFT completes transparency improvements and obtains registration for Safe Harbor, http://www.swift.com/about_swift/legal/compliance/statements_on_compliance/swift_completes_transparency_improvements_and_files_for_safe_harbor/index.page.

[1556] Reply from European Union to United States Treasury Department SWIFT/Terrorist Finance Tracking Programme, *supra* note 545.

[1557] Belgium Privacy Commission, *Opinion No. 37/2006 of 27 September 2006 on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas*, *supra* note 1500; Article 29 Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, *supra* note 1507.

[1558] Press Release, SWIFT Board approves messaging re-architecture, http://www.swift.com/about_swift/legal/compliance/statements_on_compliance/swift_board_approves_messaging_re_architecture/index.page.

[1559] SWIFT's new operations centre is in Diessenhofen Switzerland.

from the US Treasury Department under the TFTP. Peter Hustinx, the European Data Protection Supervisor noted with satisfaction that this change in the SWIFT architecture

> "was encouraged and welcomed by the European data protection authorities, as it was designed to bring all data originating in Europe within the jurisdiction and control of European authorities and thus ensure that the European standards for the protection of fundamental rights, including the protection of personal data, would fully apply."[1560]

Ironically enough, however, SWIFT's decision on restructuring did not create problems only to the US authorities, since transfers of SWIFT data to UST under administrative subpoenas would no longer be taking place; it affected the EU-side as well that felt compelled to negotiate a new framework for the transfer of such data. This is explained, according to a commentator, by two reasons: First, the EU was subject to political pressure by the US administration that was pointing out that "an important security gap"[1561] might arise if European financial transactions were not available to UST for terrorism investigations under the TFTP, and wanted to demonstrate that it actively cooperates with its transatlantic partner for such a vital purpose as counter-terrorism.[1562] Second, the EU does not have its own TFTP system and the relevant information coming from the US processing of the financial data to EU governments would otherwise be lost.[1563]

On 27 July 2009, the Council authorised the Presidency, assisted by the Commission, to begin negotiations with UST for the conclusion of a short-term Agreement allowing the transfer of EU originating SWIFT data to the US.[1564] The Agreement would fall under the (former) third pillar and in particular Articles 24 and

---

[1560] Peter HUSTINX, European Data Protection Supervisor, Speaking points to Joint Meeting of LIBE and ECON Committees on EU-US interim agreement following the entry into force of the new SWIFT architecture, European Parliament, Brussels, 3 September 2009.
[1561] Council of the European Union, Press Release, EU-US Agreement on the Transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Programme, Brussels, 9 February 2010 6265/10 (Presse 23).
[1562] MARISE CREMONA, JUSTICE AND HOME AFFAIRS IN A GLOBALISED WORLD: AMBITIONS AND REALITY IN THE TALE OF THE EU-US SWIFT AGREEMENT 13 (Austrian Academy of Sciences, Institute for European Integration Research, Working Paper No. 04/2011, March 2011).
[1563] *Id.*
[1564] Council of the European Union, Negotiating directives for negotiations between the European Union and the United States of Am5rica for an international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing.

38 TEU.[1565] The timing was not without relevance: it was the end of July 2009 and the Lisbon Treaty was due to enter into force on 1 December 2009. The Interim's Agreement fate seemed, therefore, closely linked to the new constitutional developments at the EU level.[1566] In this respect, the negotiating directives provided that in the event of the entry into force of the Lisbon Treaty, the "Agreement shall provide that the Contracting parties resume negotiations for a new Agreement under the conditions of the appropriate legal framework."[1567]

The negotiations of the Interim TFTP Agreement were surrounded by secrecy. Both the negotiating mandate of the Commission and the comments of the EDPS were characterised as EU-restricted and were not published. The European Parliament was only briefed on the main lines of the EDPS opinion in a Joint Meeting of the LIBE and ECON Committees on EU-US interim TFTP Agreement, held in Brussels on 3 September 2009.[1568]

In a Resolution of 17 September 2009, the European Parliament noted the fact that a number of negotiating documents, including the draft Agreement were classified as 'EU-restricted' and asked the Commission and the Presidency to ensure that "the European Parliament and all national parliaments will be given full access to the negotiation documents and directives".[1569] It pointed out that a framework for the exchange of data with the US, the EU-US agreement on legal assistance, was already in place and provided for a sounder legal basis for the transfer of SWIFT data than the proposed interim agreement.[1570] In this respect, the Parliament asked the Council and the Commission to explain the need for an interim TFTP agreement.[1571] Finally, it set out a number of data protection safeguards that the Agreement "must as a very minimum ensure."[1572]

On 30 November 2009, one day before the entry into force of the Lisbon Treaty, the Council authorised the Presidency to sign an Agreement between the EU

[1565] *Id.*
[1566] Cremona, *Justice and Home Affairs in a Globalised World: Ambitions and Reality in the Tale of the EU-US SWIFT Agreement*, *supra* note 1562, at 14.
[1567] Council of the European Union Negotiating directives, *supra* note 559.
[1568] Peter HUSTINX, European Data Protection Supervisor, Speaking points to Joint Meeting of LIBE and ECON Committees on EU-US interim agreement following the entry into force of the new SWIFT architecture, *supra* note 555.
[1569] European Parliament resolution of 17 September 2009 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, P7_TA(2009)0016.
[1570] *Id.*
[1571] *Id.*
[1572] *Id.*

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.[1573] The Agreement would apply provisionally as from 1 February 2010 and expire the latest on 31 October 2010.[1574]

1.5 The Interim TFTP Agreement and its 'historic' rejection

The Interim TFTP Agreement has a twofold purpose: on the one hand, to make available to the US Treasury Department financial payment messaging and related data stored in the territory of the European Union by providers of international financial payment messaging services, for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing; and, on the other hand, to make available to law enforcement, public security, or counter terrorism authorities of Member States, or Europol or Eurojust relevant information obtained through the TFTP, for the same counter-terrorism purposes.[1575] The Agreement does not mention SWIFT expressly. Instead, it provides that the data will be made available to the US authorities by "providers of international financial payment messaging services", which will be designated by the Parties ('Designated Providers').[1576]

The procedure envisaged for the transfer of the data to the US is described in Article 4 of the Agreement: First, the US Treasury Department issues a request based on an ongoing terrorist investigation concerning a specific conduct "that has been committed or where there is, based on pre-existing information or evidence, a reason to believe that it could be committed."[1577] The request will be transmitted by the US

[1573] Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the signing, on behalf of the European Union, 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, OJ L 8/9 of 13.1.2010.
[1574] 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 L 8/11 of 13.1.2010.
[1575] Article 1.
[1576] Article 3.
[1577] Article 4(1). According to Article 4(2) of the Agreement, "the request shall identify as clearly as possible data stored by a Designated Provider in the territory of the European Union that are necessary to this end. Data may include identifying information about the originator and/or recipient of the transaction, including name, account number, address, national identification

Department of Justice to the "central authority of the Member State either in which the designated financial provider is based or where it stores the requested data."[1578] A copy of the request will also be simultaneously transmitted to the "central authority of the other Member State," and to the national Members of Eurojust of those Member States.[1579] On receipt of the request, the central authority of the requested Member State will verify that it accords with the TFTP Agreement and the applicable requirements of the bilateral mutual legal assistance agreement. "Where the central authority has so verified, the request shall be transmitted to the competent authority for its execution under the law of the requested Member State."[1580] The request will be executed as a matter of urgency and the data will be transferred "between the designated authorities of the requested Member State and of the United States."[1581] If the provider is not able to identify and produce the specific data that would respond to the request because of technical reasons, "all potentially relevant data shall be transmitted in bulk ... to the competent authority of the requested Member State."[1582]

The procedure could not be more unclear. What is 'central authority of the Member State', which is 'the other Member State', what is 'the competent authority for execution' and which are 'the designated authorities'? The Agreement does not provide any definition of these notions and the whole transfer procedure is fraught with uncertainties. This is not remedied by the safeguards applicable to the processing of provided data,[1583] which in essence repeat the assurances found in the unilateral Representations.[1584]

Insofar as the retention periods are concerned, the Interim Agreement stipulates that non-extracted data would be deleted no later than five years from receipt, while information extracted from Provided Data would be subject to "the retention period applicable to the particular government authority according to its

---

number, and other personal data related to financial messages. The request shall substantiate the necessity for the data and shall be tailored as narrowly as possible in order to minimise the amount of data requested, taking due account of geographic, threat and vulnerability analyses."

[1578] Article 4(3).
[1579] Article 4(4).
[1580] Article 4 (5).
[1581] *Id.*
[1582] Article 4(6).
[1583] Article 5.
[1584] *See* above.

particular regulations and record retention schedules."[1585] Concerning the rights of redress, these are limited to a 'confirmation' obtained from the relevant data protection authority on whether any processing of the individual's personal data has taken place in breach of the Agreement.[1586] In this regard, any person who considers his or her personal data to have been processed in breach of the Agreement "is entitled to seek effective administrative and judicial redress in accordance with the laws of the European Union, its Member States, and the United States, respectively."[1587]

The Interim TFTP Agreement is unduly complex and very weak from the point of view of fundamental rights, but that was not its only problem. With the entry into force of the Lisbon Treaty on 1 December 2009, one day after its signature, the procedure of Article 218 TFEU for the conclusion of international agreements came into application, according to which, the European Parliament's consent would be required for the formal conclusion of the TFTP Agreement. For this reason, on 17 September 2009, the Commission introduced a proposal for a Council Decision on the conclusion of the TFTP Agreement with the US.[1588] On the basis of Article 218 (6) (a) TFEU, the Commission recommended to the Council, to adopt a decision concluding the Agreement, after obtaining the consent of the European Parliament.[1589] The new legal bases for the decision would be Articles 82 (1) (d) (judicial cooperation in criminal matters) and 87 (2) (a) TFEU (police cooperation).[1590]

On 5 February 2010, the LIBE Committee of the Parliament recommended the Parliament to withhold its consent to the conclusion of the TFTP Agreement.[1591] The Rapporteur, Jeanine Hennis-Plasschaert, made several very critical remarks concerning the SWIFT case in the Recommendation:

> "As far as the TFTP is concerned, it must be considered as a departure from European law and practice in how law enforcement agencies would acquire individuals' financial records for law enforcement activities, namely individual

[1585] Article 5 (2) (m).
[1586] Article 11.
[1587] Article 11 (3).
[1588] 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, COM(2009/0703 final) - NLE 2009/0190/ legal bases had changed.
[1589] *Id.*
[1590] *Id.*
[1591] LIBE Committee Recommendation 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 (05305/1/2010REV – C7-0004/2010 – 2009/0190(NLE)).

court-approved warrants or subpoenas to examine specific transactions instead of relying on broad administrative subpoenas for millions of records.

Furthermore, what might have kicked off as an urgent temporary measure (in reply to 9/11) became *de facto* permanent without specific approval or authorisation by EU authorities or a real transatlantic evaluation of its impact and forward looking transatlantic negotiations covering at the same time security, judicial cooperation and data protection impact. Clearly, such proceedings did not help in building up mutual trust for transatlantic cooperation on counter-terrorism purposes."[1592]

Concerning the Interim TFTP Agreement, the Recommendation noted, first, that it violates the basic principles of data protection law, i.e. the principles of necessity and proportionality, because SWIFT is not in a position technically to provide specific data related to an individual. It can only, therefore, provide data in bulk, and, hence, "it is not possible to refer to so-called limited requests."[1593] Furthermore, the LIBE Recommendation identified a number of problems in the Interim Agreement: the transfer requests are not subject to judicial authorisation;[1594] the conditions for sharing TFTP data with third countries are not clearly defined;[1595] the public control and oversight of the authorities' access to SWIFT data is not regulated;[1596] the Agreement provides no indication of the data retention periods;[1597] the rights of access, rectification, compensation and redress are not defined adequately;[1598] and, it is impossible to claim true reciprocity.[1599]

These, however, were not the sole reasons for the rejection of the Interim TFTP Agreement. Inter-institutional relations were at stake, not the least because the Lisbon Treaty gave new powers to the Parliament and the Agreement was adopted one day before its entry into force. The LIBE Recommendation did not fail to mention this:

"By requesting Parliament's consent for the conclusion of the FMDA in conditions in which it was impossible for practical reasons for Parliament to

[1592] *Id.* at 7.
[1593] *Id.* at 8.
[1594] *Id.* at 9.
[1595] *Id.*
[1596] *Id.*
[1597] *Id.*
[1598] *Id.*
[1599] *Id.*

react before the provisional application came into operation, the Council has in effect set Parliament a deadline *in breach of the spirit of Article 218 (6) (a) TFEU*, and *undermined in part the legal effect and the practical impact of Parliament's decision in the consent procedure*, in particular as regards its provisional application."[1600]

The LIBE Report also stressed that the Parliament should have been informed "fully and immediately at all stages of the procedure",[1601] something that did not happen in the negotiations of the Interim TFTP that were in general covered by secrecy.

For these reasons, the LIBE Committee recommended the Parliament to withhold its consent. This meant that the TFTP would not enter into force, and its provisional application would be terminated upon notification to the US.[1602] The Committee noted, however, that other alternative routes for the exchange of information with the US, such as the EU-US Agreement on Mutual Legal Assistance[1603] and bilateral agreements between the Member States and the US, existed.[1604]

On 9 February 2010, two days before the vote of the Parliament on the conclusion of the Interim TFTP Agreement, "in an unusual move",[1605] the Council issued a Press Release, responding essentially to the allegations raised by the LIBE Committee.[1606] It explained that it was impossible to wait for the entry into force of the Lisbon Treaty before starting the negotiations for the TFTP Agreement, which in any case would have a transitional nature and would be applicable for a short term, having a maximum duration of nine months.[1607] The Council also stated diplomatically that it was

"looking forward to the new situation which has been created by the Lisbon Treaty and to work together with the Parliament, which needs to be informed fully and immediately at all stages of the procedure. This will allow the Parliament to fully exercise its role provided in the Treaty, in order to

---

[1600] *Id.*
[1601] *Id.* at 10.
[1602] *Id.*
[1603] Agreement on Mutual Legal Assistance between the European Union and the United States of America, OJ L 181/34 of 19.7.2003.
[1604] LIBE Committee Recommendation, *supra* note 585, at 10.
[1605] Cremona, *Justice and Home Affairs in a Globalised World: Ambitions and Reality in the Tale of the EU-US SWIFT Agreement*, *supra* note 1562, at 16.
[1606] Council of the European Union, Press Release, EU-US Agreement on the Transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Programme, *supra* note 556.
[1607] *Id.*

achieve that the longer term TFTP Agreement meets its concerns regarding the protection of personal data, while ensuring that the TFTP can continue to provide EU Member States with significant lead information to investigate and disrupt terrorism."[1608]

Despite the Council's mobilisation, the Parliament voted on 11 February 2010 against the conclusion of the Agreement (with 378 against, 196 in favour, 31 abstentions) requesting the Commission to immediately submit recommendations to the Council with a view to a long-term TFTP Agreement with the US that should comply with the new legal framework established by Lisbon Treaty and the EUCFR.[1609]

This historic rejection of an almost concluded international agreement with the US is, according to commentators, largely due to how the Council handled the TFTP Agreement.[1610] It presented it to the Parliament as a *fait accompli*,[1611] assuming that the later "would reluctantly, and probably with much verbal protesting, nevertheless agree. The strategy failed and as a result the legislative initiative failed too. Instead of an imperfect agreement there was no agreement."[1612]

1.6 Renegotiating a TFTP Agreement

After the rejection of the Interim TFTP Agreement by the European Parliament, the Commission and the Council had to open a new round of negotiations with the US for a second TFTP Agreement, this time paying due respect to the role of the European Parliament. On 24 March 2010, the Commission asked the Council to

---

[1608] *Id.*

[1609] European Parliament legislative resolution of 11 February 2010 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 (05305/1/2010 REV 1 – C7-0004/2010 – 2009/0190(NLE)) P7_TA(2010)0029.

[1610] Cremona, *Justice and Home Affairs in a Globalised World: Ambitions and Reality in the Tale of the EU-US SWIFT Agreement*, *supra* note 1562, at 17; Jörg Monar, *Editorial Comment: The Rejection of the EU-US TFTP Interim Agreement by the European Parliament: A Historic Vote and Its Implications*, 15 EUROPEAN FOREIGN AFFAIRS REVIEW 143, 146 (2010).

[1611] Monar, *Editorial Comment: The Rejection of the EU-US TFTP Interim Agreement by the European Parliament: A Historic Vote and Its Implications*, *supra* note 1610, at 146.

[1612] Cremona, *Justice and Home Affairs in a Globalised World: Ambitions and Reality in the Tale of the EU-US SWIFT Agreement*, *supra* note 1562, at 17.

authorise the opening of negotiations for a long-term TFTP agreement.[1613] According to the Commission's Recommendation, the legal bases for the new Agreement would be Articles 216, 82, and 87 TFEU.[1614] The Commission stressed that the long- term agreement would address the concerns set out in the European Parliament's Resolution of 17 September 2009, particularly with regard to the protection of personal data.[1615] For this reason, the Commission proposed that a judicial public authority should be designated in the EU with the responsibility to receive requests from UST.[1616] The authority would verify whether the request meets the requirements of the Agreement in order for the transfer to take place.[1617] On 22 April 2010, the Council adopted the Negotiating Directives and on 11 May, it authorised the Commission to open negotiations with the US.

On 5 May 2010, the Parliament adopted a Resolution concerning the opening of negotiations for a second TFTP Agreement.[1618] The Parliament welcomed "the new spirit of cooperation demonstrated by the Commission and the Council and their willingness to engage with Parliament, taking into account their Treaty obligation to keep Parliament immediately and fully informed at all stages of the procedure",[1619] and urged the two institutions "to explore ways of establishing a transparent and legally sound procedure for the authorisation of the transfer and extraction of relevant data as well as for the conduct and supervision of data exchanges ... in full compliance with the principles of necessity and proportionality and the rule of law with full respect for fundamental rights requirements under EU law."[1620] Along the lines of the Commission's Recommendation on the negotiating Directives, the Parliament requested that "a judicial public authority should be designated in the EU with the responsibility to receive requests from the United States Treasury Department."[1621]

[1613] Recommendation from the Commission to the Council to authorize the opening of negotiations for an agreement between the EU and the USA to make available to the US Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing, Brussels, 24.3.2010, SEC (2010) 315 final.
[1614] *Id.* at 2.
[1615] *Id.* at 3.
[1616] *Id.* at 5.
[1617] *Id.*
[1618] European Parliament resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorise 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 P7_TA-PROV(2010)0143.
[1619] *Id.*
[1620] *Id.*
[1621] *Id.*

On 15 June 2010, the Commission introduced a Proposal for a Council Decision on the conclusion of a TFTP Agreement with the US.[1622] On 28 June, the Council adopted a decision on the signing of the TFTP Agreement, subject to its conclusion at a later stage.[1623]

On 5 July, the LIBE Committee recommended the Parliament to give its consent to the conclusion of the Agreement.[1624] The Rapporteur, Alexander Alvaro, explained that compared to the Interim Agreement, rejected by Parliament, the second TFTP represented

> "an improvement that has been achieved due to Parliament's consistent demands for solutions to … key issues…"[1625]

Following the Recommendation of the LIBE Committee, and the political pressure exercised by the US on the European Parliament that had become now an important actor of the negotiations,[1626] on 8 July, the Parliament voted in favour of the Agreement.[1627] Having received the consent of the Parliament, the Council adopted on 13 July a decision on the conclusion of the TFTP Agreement between the EU and the US.[1628] The Agreement entered into force for five years on 1st August 2010.

[1622] *Id.*

[1623] Council Decision of 28 June 2010 on the signing, on behalf of the Union, 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 (2010/411/EU), OJ L 195/1 of 27.7.2010.

[1624] LIBE Committee Recommendation on the draft 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 (11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE)) A7-0224/2010, Rapporteur: Alexander Alvaro.

[1625] *Id.*

[1626] Several MEPs were invited to Washington DC and Vice-President Joe Biden addressed the European Parliament on 6 May 2010.

[1627] European Parliament legislative resolution of 8 July 2010 on the draft 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 (11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE)) P7_TA(2010)0279.

[1628] Council Decision of 13 July 2010 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 (2010/412/EU), OJ L 195/3 of 27.7.2010.

1.7 The long-term TFTP Agreement: An Improvement?

The 2nd TFTP Agreement[1629] was received with enthusiasm and considered as an improvement compared to its predecessor that was rejected in the beginning of 2010. In fact, the Parliament gave its consent for the conclusion of the long-term TFTP Agreement, as the LIBE Committee had identified in its report eight major improvements of the 2nd TFTP Agreement: access to and extraction of data on US soil by US agencies will be monitored and when required blocked by a European official; the procedure regarding judicial redress for European citizens is regulated in greater detail; the right to rectification, erasure, or blocking is more comprehensive; the regulation on transparency of the US TFTP has become more detailed; the procedure regarding onward data transfers to third countries is regulated more precisely; the scope for fighting terrorism is defined and clarified; Europol shall verify whether the US request for financial data meets the requirements of the Agreement as well as whether it is tailored as narrowly as possible, before the data provider is authorized to transfer the data; the US Treasury Department is obliged to delete financial data transmitted that was not requested; and, SEPA (Single Euro Payments Area) data are excluded from the transfers.[1630]

In order to assess whether the 2nd TFTP Agreement introduces actually an improvement, a closer look at the Agreement is required. The purpose of the long-term TFTP Agreement is identical with the Interim one: on the one hand, the transfer of financial payment data to UST for counter-terrorism objectives, on the other hand, the making available of information obtained through the TFTP to law enforcement, public security, or counter-terrorism authorities of Member States or Europol or Eurojust for the same objectives.[1631] It has been argued that the scope of defining terrorism has been clarified,[1632] as the notion of terrorism found in Article 2 of the 2nd

---

[1629] 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 L 195/5 of 27.7.2010.

[1630] LIBE Committee Recommendation on the draft 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, *supra* note 619, at 7-8.

[1631] Article 1.

[1632] EUROPEAN DATA PROTECTION SUPERVISOR, OPINION 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) (June 22, 2010).

TFTP Agreement builds on the definition of terrorism[1633] found in the Council Framework Decision 2002/475/JHA.[1634] The alleged improvement is, however, minimal since the Interim Agreement contains the same definition with small differences. Similarly to its predecessor, the long-term TFTP Agreement stipulates that "providers of international financial payment messaging services" will be jointly designated by the Parties ('Designated Providers') in order to provide the relevant data to UST.[1635] Unlike the Interim Agreement, however, this time in the Annex of the Agreement we find the name of the 'designated provider': SWIFT.

A clear improvement introduced by the 2nd TFTP is that it excludes data relating to SEPA,[1636] and it lays down more clearly the requirements with which a request by UST should comply: a) identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing; b) clearly substantiate the necessity of the data; and, c) be tailored as narrowly as possible in order to minimise the amount of data requested.[1637]

The solution found on the judicial authority entrusted with the task to receive requests is disappointing: it is Europol that will receive the requests by UST and verify that they comply with the requirements in order for the transfer to take place.[1638] Europol is no judicial authority, however, and it has interests on its own on the financial data.[1639]

Furthermore, the Agreement stipulates that data transmitted while not requested will be deleted "promptly and permanently" by UST,[1640] and that all non-extracted data shall be deleted not later than five years from receipt.[1641] The retention period of extracted data is much more unclear. In this respect, the Agreement provides merely that "information extracted from provided data ... shall be retained for no longer than necessary for specific investigations or prosecutions for which they are

[1633] Article 2.
[1634] Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA), OJ L 164/3 of 22.6.2002.
[1635] Article 3.
[1636] Article 4 (2) (d).
[1637] Article 4 (2).
[1638] Article 4 (3) (4) and (5).
[1639] For a detailed discussion *see* below.
[1640] Article 6 (2).
[1641] Article 6 (4).

used."[1642] This provision, besides the proportionality issues that it raises, which will be discussed below, is equally unclear as its equivalent in the Interim Agreement.[1643]

While the Interim Agreement spoke only of sharing "terrorist leads" obtained through the TFTP with law enforcement, public security, or counter terrorism authorities in the United States, EU, or third States; the 2nd TFTP Agreement contains a whole new Article on onward transfers of "information extracted from the provided data."[1644] In the case that such information involves a citizen or a resident of a Member State, the Agreement provides that sharing will be subject to the prior consent of competent authorities of the concerned Member State, unless the sharing of the data is essential for the prevention of an immediate and serious threat to public security.[1645]

Concerning the individual rights of the data subject, the long-term TFTP Agreement does not introduce any significant improvements. A right of access is granted to individuals through their data protection authorities in the EU to verify whether any processing of their data has taken place in breach of the Agreement.[1646] The person must send a relevant request to her national data protection authority, which will transmit it to the Privacy Officer of UST, who shall make all necessary verifications pursuant to the request.[1647] Such a procedure, however, as the Article 29 Working Party has pointed out limits the national data protection authorities to the role of

> "a postbox for assessments made by US Treasury Department's employees, instead of being able to obtain themselves all relevant information, to independently assess such information and to assess full data protection compliance."[1648]

Individuals have the right to seek rectification, erasure, or blocking of their data processed by UST, following a procedure similar to the one regarding the right to

[1642] Article 6 (7).
[1643] *See* above.
[1644] Article 7.
[1645] Article 7 (d).
[1646] Article 15.
[1647] Article 15 (3).
[1648] Article 29 Working Party & Working Party on Police and Justice, Press Release, EU-US TFTP Agreement not in line with privacy legislation: European Data Protection Authorities not satisfied with safeguards in EU-US financial transactions agreement, Brussels, 28 June 2010.

access described above.[1649] Concerning the redress rights, there seems to introduce an improvement with regard to the Interim Agreement, as the 2nd TFTP provides that:

> "Any person who considers his or her personal data to have been processed in breach of this Agreement is entitled to seek effective administrative and judicial redress in accordance with the laws of the European Union, its Member States, and the United States, respectively... All persons, regardless of nationality or country of residence, shall have available under US law a process for seeking judicial redress from an adverse administrative action."[1650]

Despite the improvement that this provision introduces, there are questions about its enforceability since the Agreement states at the same time that it does not create or confer any right or benefit on any person or entity, private or public.[1651] Finally, the new transparency provisions that were much welcomed by the European Parliament refer only to the posting of detailed information concerning the TFTP on the Department of Treasury's website.[1652]

Besides the provision on joint review[1653] that existed in the Interim TFTP Agreement, the new Agreement provides for the monitoring of the TFTP by independent overseers, who will have the authority to review "in real time and retrospectively all searches made of the provided data, and the authority to query such searches and ... to request additional justification of the terrorism nexus."[1654] Independent overseers also have the authority to block any or all searches that do not respect the data protection safeguards set out in the Agreement.[1655]

Is the long-term TFTP an improvement compared to its predecessor? A closer look shows that it does not introduce significant changes. The only difference seems to be that the 2nd TFTP is longer and more detailed. Even so, the Agreement remains silent concerning the main issue of concern of the Parliament, the EDPS,[1656] and the Article 29 Working Party: the bulk transfers of data. Since SWIFT's system does not

---

[1649] Article 16.
[1650] Article 18 (2).
[1651] Article 20 (1).
[1652] Article 14.
[1653] Article 13.
[1654] Article 12 (1).
[1655] *Id.*
[1656] European Data Protection Supervisor, *Opinion 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)*, *supra* note 1632.

allow targeted researches, it is questionable to what extent the principles of proportionality and purpose limitation are respected under the current TFTP.

1.8 The role of Europol under the 2nd TFTP: 'A fox guarding the henhouse'?

Despite not being a judicial authority, Europol has been assigned the task to verify the US requests and give the green light for the transmission of the data by SWIFT. In particular, as discussed above, Europol examines whether a) the UST request identifies the data as clearly as possible, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing; b) the necessity of the data is clearly substantiated; c) the request is tailored as narrowly as possible in order to minimise the amount of data requested, taking due account of past and current terrorism risk analyses focused on message types and geography as well as perceived terrorism threats and vulnerabilities, geographic, threat, and vulnerability analyses; and d) the request does not seek any data relating to the Single Euro Payments Area (SEPA).[1657]

Europol has two further interests under the Agreement concerning the TFTP data. On the one hand, it can receive spontaneously by UST information obtained through the TFTP that may contribute to the investigation, prevention, detection, or prosecution by the EU of terrorism or its financing.[1658] On the other hand, it can request for searches of the TFTP data if it determines that there is a reason to believe that a person or entity has a nexus to terrorism.[1659]

Given that Europol has an interest in the TFTP data for its own counter-terrorism purposes, it is difficult to see how its verification task on the necessity and proportionality of the US requests can be reconciled with its own interest on the financial data. Specific questions on Europol's level of scrutiny regarding the TFTP were raised by the Europol Joint Supervisor Body (JSB) in its inspection concerning Europol's implementation of the TFTP Agreement. In particular, pursuant to Article

[1657] Article 4.
[1658] Article 9.
[1659] Article 10.

34 (1) of the Europol Council Decision,[1660] the JSB has the task of reviewing the activities of Europol in order to ensure that the rights of the individual are not violated by the storage, processing and utilisation of data by Europol. In its inspection of 11 November 2010, the findings of which were classified as EU-Secret,[1661] the JSB stated that due to the abstract nature and terms of the UST requests – broad types of data, also involving EU Member States' data-

> "proper verification of whether the requests are in line with the conditions of Article 4 (2) of the TFTP Agreement –on the basis of the available documentation- is impossible."[1662]

A problem highlighted by the JSB was the provision of information orally to certain Europol staff by the US Treasury Department, "with the stipulation that no written notes are made."[1663] In this respect, the JSB notes in its Report:

> "where requests lack the necessary written information to allow proper verification of compliance with Article 4 (2) of the TFTP Agreement, it is impossible to check whether this deficiency is rectified by the orally provided information. The significant involvement of oral information renders proper internal and external audit, by Europol's Data Protection Office and the JSB respectively, impossible."[1664]

The report on the joint review of the implementation of the TFTP Agreement[1665] seemed more satisfied with Europol's role. In particular, the EU review team noted that

---

[1660] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol),OJ L 121/37 of 15.5.2009. Article 34 (1) provides: "An independent Joint Supervisory Body shall be set up to review, in accordance with this Decision, the activities of Europol in order to ensure that the rights of the individual are not violated by the storage, processing and use of the data held by Europol. In addition, the Joint Supervisory Body shall monitor the permissibility of the transmission of data originating from Europol. The Joint Supervisory Body shall be composed of a maximum of two members or representatives, where appropriate assisted by alternates, of each of the independent national supervisory bodies, having the necessary abilities and appointed for five years by each Member State. Each delegation shall be entitled to one vote."

[1661] Report on the Inspection of Europol's Implementation of the TFTP Agreement, Conducted in November 2010 by the Europol Joint Supervisory Body, JSB Europol inspection report 11-07, Brussels, 1 March 2011.

[1662] *Id.*

[1663] *Id.*

[1664] *Id.*

[1665] Commission Staff Working Paper, 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 Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program 17-18 February 2011, Brussels, 30.03.2011, SEC(2011) 438 final.

"the procedures required under the Agreement have been put in place to ensure that, in principle, the requests for information are tailored as narrowly as possible, and are also in line with the other requirements of the Agreement."[1666]

Concerning Europol, the report found that it

"clearly takes its role under the Agreement very seriously, and has put in place all the necessary elements to fulfil its role in accordance with the Agreement and its implementing technical modalities."[1667]

However, following JSB's report, the EU joint review team urged the US authorities

"to provide as much information as possible to Europol in writing, even where such information is classified, in order to allow further verification of the way in which Europol fulfils its role under the Agreement..."[1668]

On 8 April 2011, Europol issued an Information Note to the European Parliament, where it explained its activities in relation to the TFTP Agreement.[1669] The long-term TFTP does not mention anything on bulk transfers of data, but Europol's explanations are illuminating on the nature of the data transfers. According to Europol,

"Article 4 regulates the transfer of *bulk data* from the Designated Provider (based on standardised data categories) to the US Department of the Treasury, as clearly understood during the negotiation of the Agreement. Strictly within the context of Article 4 the provisions aim at transferring information on a bulk and generic level according to the criteria established (limited in geographical scope, time period, and list of data categories). Identifying a nexus to terrorism in specific cases is a requirement under other provisions in the Agreement and forms no part of the request as submitted by the US Department of the Treasury to the Designated Provider under Article 4... Europol does not see or manage the provided data, which is transmitted directly from the Designated Provider to the US Department of the Treasury."[1670]

Furthermore, replying essentially to the allegations raised by JSB that most information related to a UST request is transmitted to certain Europol officials orally,

---

[1666] *Id.* at 11.
[1667] *Id.* at 12.
[1668] *Id.*
[1669] Europol Activities in Relation to the TFTP Agreement, Information Note to the European Parliament 1 August 2010 – 1 April 2011, The Hague, 8 April 2011, File no. 2566-566.
[1670] *Id.* at 4.

Europol describes in its Note the set of documents that it receives from the Treasury Department on the basis of a request under Article 4.[1671] According to Europol,

> "the information package provided to Europol by the US authorities, in support of its requests, is substantial and well documented, running to an average of 56 pages per request. By the time Europol has completed its internal assessment of the request and recorded all available judgments and advice the whole package runs to an average 67 pages."[1672]

As Europol explains, the request for financial messaging data usually covers a period of four weeks.[1673] Europol had received eight requests until April 2011 and verified all of them, asking for additional information in five out of them.[1674] Normally, Europol is required to complete its verification task in 48 hours from the receipt of the request, but as it states in its Information Note to the Parliament in six cases it has failed to meet this deadline, taking 16 days to complete its work in one case.[1675]

There are many problems with the long-term TFTP Agreement and the fact that the task of the verification of the necessity and proportionality of the US requests was assigned not to a judicial authority, but to Europol is one of them. What seems more problematic, however, is that Europol is found in a conflict of interests situation when it has to verify the UST request, but at the same time is interested in the financial messaging information. This necessarily affects its –in any case minimal- verification role.

[1671] According to Europol's Information Notice to the European Parliament, the set of documents sent by UST and supporting the verification process at Europol comprises: a cover letter from the US Department of the Treasury; a copy of the request submitted by the US Department of the Treasury to the Designated Provider, setting out the: geographical sphere (list of countries) and the relevant period to which the request refers; list of data categories the US authorities are seeking to retrieve (from the full repository of financial transactions processed by the Designated Provider); a set of documentation which constitutes the substantiated reasoning for the request (sent only to Europol and not to the Designated Provider), outlining: reasons (based on analysis findings and results from investigations) for the selection of the geographical sphere (list of countries) and data categories referred to in the request; an overview of current and past terrorism investigations carried out by US authorities, mentioning targets of investigation including personal data.

[1672] *Id.* at 7.

[1673] *Id.*

[1674] *Id.* at 8.

[1675] *Id.*

1.9 Can a European terrorist finance tracking system bring the spring?

Since SWIFT does not have the technical capability to transfer individualised data, and as discussed above, Europol does not perform a strict scrutiny in the US requests, European financial messaging data are available in bulk to the US Treasury Department for its searches. A solution that has been proposed in the EU for the problem of the lack of an effective minimisation of financial data is the establishment of a "legal and technical framework for the extraction of data on EU territory"[1676] with the overall aim to ensure that the processing of such data would take place in accordance with EU data protection legislation and principles, and in accordance with the EU Charter of Fundamental Rights.

Following the PNR precedent and the more general trend to internalise highly controversial counter-terrorism policies in the EU, the Commission, on 13 July 2011, tabled a proposal for the development of an EU Terrorist Financing Tracking System (TFTS).[1677] The difference with PNR is that this time the EU system is considered necessary, both by the Council[1678] and the Parliament,[1679] not only to fight terrorism, but also to achieve an effective minimisation of data at the EU level. In this regard, the EU-US TFTP Agreement provides that the Commission will carry out a study into the possible introduction of "an equivalent system allowing for a more targeted transfer of data."[1680] The paradox is that the EU TFTS appears, therefore, as a path

---

[1676] Article 2 of Council Decision of 13 July 2010 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, *supra* note 623.

[1677] Communication from the Commission to the European Parliament and the Council, A European terrorist finance tracking system: available options, Brussels, 13.7.2011, COM(2011) 429 final.

[1678] *See* Council Decision of 13 July 2010 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, *supra* note 623.

[1679] *See* for instance European Parliament resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorise 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, *supra* note 613.

[1680] Article 11. The Agreement recognises that an EU TFTP will have consequences on the EU-US TFTP Agreement: "Since the establishment of an EU system could substantially change the context of this Agreement, if the European Union decides to establish such a system, the Parties should consult to determine whether this Agreement would need to be adjusted accordingly. In that regard, US and EU authorities shall cooperate to ensure the complementariness and efficiencies of the U.S. and EU systems in a manner that further enhances the security of citizens of the United States, the European Union, and elsewhere. In the spirit of this cooperation, the Parties shall actively pursue, on the basis of reciprocity and appropriate safeguards, the cooperation of any relevant international financial payment messaging service providers which are based in their respective territories for the purposes of ensuring the continued and effective viability of the U.S. and EU systems."

towards the proportionality of the EU-US TFTP Agreement. Hence, ironically, it is not merely a measure internalising external security needs –as it was the case concerning PNR-, it is also presented as a measure rationalising these security needs.

In its proposal, the Commission lays down two reasons for establishing an EU TFTS: the system must provide an effective contribution to the fight against terrorism and its financing within the EU; and, the system must contribute to limiting the amount of personal data transferred to third- countries.[1681] The US influence, seen with regard to the EU PNR system, is evident also in the EU TFTS. According to the Commission,

> "[t]he system should not be set up just to provide relevant information to US authorities – the authorities of the Member States have a real interest in the results of such a system as well. This approach also implies that whilst the US TFTP could certainly provide inspiration as to how such a system could be set up, a European equivalent system would not necessarily have to copy all elements of the US TFTP."[1682]

That being said, the EU TFTS might be going even further than the US TFTP in a number of aspects. First, the Commission is wondering whether access to financial messaging data would be useful not only to combat terrorism but also other forms of serious crime, in particular organised crime and money laundering.[1683] Second, the Commission is considering, whether, besides SWIFT, which is clearly the most important world-wide provider of financial messaging services, other providers that operate on the market should be requested to transmit their data.[1684] A third question that arises with regard to the EU TFTS is whether it should be limited to requesting international transactions financial data or whether the option of including financial messaging services exchanged between Member States could be considered.[1685] Finally, the Commission is reflecting on whether besides the particular type of financial messaging data that is currently requested, other different types of financial messaging data used in the international banking system might be useful for the purposes of the TFTS.[1686]

[1681] Communication from the Commission to the European Parliament and the Council, A European terrorist finance tracking system: available options, *supra* note 672, at 2.
[1682] *Id.* at 4.
[1683] *Id.* at 7.
[1684] *Id.*
[1685] *Id.* at 8.
[1686] *Id.* at 8.

The Commission sets out in its Communication three options for an EU TFTS depending on whether a centralised EU solution or a decentralised model will be adopted.[1687] The first option envisages the establishment of an EU central TFTS unit, with most of the tasks and functions being implemented at the EU level.[1688] The second option would involve the establishment of an EU central TFTS unit, whose tasks would comprise issuing requests for "raw" data to the Designated Providers, verification of these requests, running searches, and handling requests for searches. However, under this option, the EU TFTS unit would not be allowed to analyse the search results and compare them with other available information or intelligence when such searches are made at the request of the authorities of the Member States – in such cases its role would be limited to preparing and distributing search results in a presentable manner.[1689] The third and more decentralised option would comprise the establishment of an upgraded Financial Intelligence Unit (FIU) Platform, made up of all the FIUs of the Member States. The EU level authority would issue requests for "raw" data to the Designated Providers, by compiling the needs specified by the national FIUs into a single request, which would also be verified and authorised at central level. However, the national FIUs would be responsible for running searches and managing search results on behalf of their Member States.[1690]

2. Does the Terrorist Finance Tracking Programme pose a Privacy or a Data Protection problem?

The 'SWIFT affair' bares many similarities with the PNR case, discussed in Chapter 7. In both cases, private commercial entities (airline companies, SWIFT) that provide services (operation of flights, financial messaging) are obliged to transfer their customers data to the US authorities (DHS, UST) for law enforcement purposes (in TFTP only for counter-terrorism, in PNR for broader law enforcement, but also further purposes). The fundamental rights concerns in the two cases are also similar: the rights to privacy and personal data protection are alleged to be infringed in the

[1687] *Id.*
[1688] *Id.* at 9.
[1689] *Id.* at 10.
[1690] *Id.* at 11.

SWIFT affair as well. Surprisingly enough, however, EU and national data protection bodies and most commentators focus mainly on the alleged infringements of the right to data protection in the TFTP case.[1691] This focus on the right to data protection can be explained most probably by the fact that TFTP has not been subject to judicial review –yet-, and hence the known pattern of the juridical assessment of the two rights, though the prism of privacy, as the Advocate General's analysis in PNR demonstrates,[1692] was not followed. This does not mean that the general misconceptions between the two fundamental rights do not apply.

Does TFTP present an infringement to privacy or to data protection? The analysis of PNR above, demonstrated that the transfer of Passenger Name Record data to the US authorities interferes primarily with the right to data protection. Taking into account the similarities between PNR and TFTP, it could be assumed that the same conclusion should apply in the present case. Before discussing whether this is actually the case, let us take a closer look at the right to data protection. The messages transmitted through the SWIFT platform contain personal data, which are found to the so-called 'content' of the message. As explained by the Belgium Privacy Commission, the 'content' of the financial message contains the name and the account number of the payee; the name and the bank details of the beneficiary; the amount transferred and the currency; and in some cases, an unstructured (free format) text.[1693] This information constitutes 'personal data' to the extent that it relates to an identified person. The fact that SWIFT does not have the technical capacity to make individual searches in its databases is not important in the context of the present analysis. The data are transmitted in bulk to the 'black box' owned by UST and the later performs searches on certain entities or individuals. As in the case of PNR, the main problem posed to the right to data protection is once again the deviation of the purpose limitation principle. Data initially collected for a commercial purpose (for the performance of the money transfer) are being used for a totally unrelated objective (to combat terrorism). The data protection principle of proportionality is also interfered with: due to SWIFT's technical organisation there is no minimisation of data taking

[1691] *See* for instance Article 29 Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, *supra* note 1507; Cremona, *Justice and Home Affairs in a Globalised World: Ambitions and Reality in the Tale of the EU-US SWIFT Agreement*, *supra* note 1562.
[1692] *See* above.
[1693] Belgium Privacy Commission, *Opinion No. 37/2006 of 27 September 2006 on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas*, *supra* note 1500, at 4.

place since the information has to be transmitted in bulk, and the retention periods are uncertain depending on whether the data have been 'extracted' or not, and in any case unduly long. In addition, the due process rights of the data subject are almost non-existent, and as analysed above, the supervision of the terrorist tracking system is minimal, since Europol is not a judicial authority and has its own interests on the data. The right to data protection is, thus, applicable in the case of TFTP, which interferes with a number of data protection principles.

Does TFTP also interfere with the right to privacy? In the case of PNR, the analysis concluded that such interference is to be found when sensitive data, revealing information on the personal and family life of the individual are at stake. This is possible in the case of the TFTP to the extent that the data might reveal racial or ethnic origin (on the basis of the personal details of the payee and the currency used for the transfer), or religious beliefs or trade-union membership (if the beneficiary is a church or a foundation).[1694] But, contrary to what was concluded with regard to PNR, the right to privacy in the present context does not only cover sensitive data. As in the case of the Data Retention Directive, analysed in Chapter 4, the transfer of financial data constitutes a form of communication before the payee and the beneficiary. This communication, albeit limited to financial information enjoys confidentiality. As in the case of the Data Retention Directive, data obtained from TFTP can reveal a person's financial movements, her potential network of business associates, family and friends to whom she transfers money, or even her donations to charitable organisations and NGOs. This, besides being confidential information of the payee, it involves necessarily also the beneficiary, who is a passive subject of the intercommunication relationship.[1695] In this way, charities organisations or other entities and individuals are made subject of suspicion before law enforcement authorities.[1696] Thus, the mapping of money transfers may be a valuable tool to fight terrorism, but it interferes both with the rights to privacy and personal data protection.

As in the case of PNR, the US Constitutional law with its 'third party doctrine'[1697] does not offer much help here either.[1698] The case of *United States v.*

[1694] *See* Donohue, *supra* note 1482, at 379.
[1695] *See* the Romanian court's pronouncements with regard to the Data Retention Directive.
[1696] Donohue, *supra* note 1482, at 379. According to Donohue, "by September 2002 the [US] government was monitoring more than 500 hundred Arab and Muslim businesses in the United States. This scrutiny, and the federal government's rather loose standards, led to a drop in contributions to Islamic charities."
[1697] For a detailed analysis *see* Solove, *A Taxonomy of Privacy*, *supra* note 261, at 528.

Miller, mentioned in Chapter 1 should be recalled here, because it bears many similarities with the TFTP issue under discussion. In that case, federal law enforcement officials issued subpoenas to two banks to produce a customer's financial records. The Supreme Court rejected the customer's complaint that the subpoenas violated his Fourth Amendment rights, on the basis that he had already voluntarily conveyed that information to a third party, i.e. his banks, and therefore he lacked any reasonable expectation of privacy.[1699] This rationale can be easily transposed to the TFTP case. Customers provide their data to their banks, which, in order to effectuate a money transfer, use the SWIFT platform.[1700] Consequently, they do not enjoy any Fourth Amendment protection, because they have already voluntarily revealed the data to third parties.

Federal legislation does not seem to be of much help either. In particular, two years after the Supreme Court's decision in *United States v. Miller* and in order to remedy the situation, Congress passed the Right to Financial Privacy Act (RFPA),[1701] that makes the access of government authorities to financial information subject to certain conditions.[1702] Among them, government authorities are required to obtain a warrant or an administrative subpoena before accessing financial records. According to RFPA, the subpoena should provide "a reason to believe that the records sought are relevant to a legitimate law enforcement inquiry."[1703] In this case, a copy of the subpoena must be given to the customer, alongside with the opportunity to file a motion before the US courts.[1704] However, the notification obligation does not apply when the disclosure of financial records is required by a government authority "authorised to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses."[1705] RFPA was also amended by the Patriot Act to permit

---

[1698] *See* above Chapter 2.
[1699] *See* above.
[1700] It should be noted that customers transferring money are often not aware that their bank uses the SWIFT platform.
[1701] Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq.* (1978). For an analysis *see* George Trubow & Dennis Hudson, *The Right to Financial Privacy Act of 1978: New Protection from Federal Intrusion*, 12 J. MARSHALL J. PRAC. & PROC. 487 (1979).
[1702] Access is permitted when 1) the customer has authorised the disclosure; 2) the financial records are disclosed in response to an administrative subpoena or summons; 3) the financial records are disclosed in response to a search warrant; 4) the financial records are disclosed in response to a judicial subpoena; or 5) the financial records are disclosed in response to a formal written request.
[1703] Right to Financial Privacy Act § 3404.
[1704] *Id.*
[1705] *Id.* § 3413. *See* also Santolli, *supra* note 1495, at 575.

the disclosure of financial information to any intelligence in any investigation related to international terrorism.[1706]

3. TFTP: A Substantive Assessment

TFTP interferes with both the rights to privacy and data protection. The interference is justified if it complies with the requirements laid down in Article 52 (1) EUCFR. In particular, a) it should be provided for by law; b) meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; c) be necessary d) be proportionate; and, e) respect the essence of the right. This formula will be employed below with regard to the rights to privacy and data protection. To the extent that the same concerns pertain to both rights, the analysis will treat them uniformly in order to avoid repetitions.

a. Provided by law

The transfer of financial messaging data from SWIFT to the US Department of Treasury is provided by law since the TFTP Agreement entered into force on 1st August 2010.

However, the Terrorist Finance Tracking Programme was operating since 2001. The secret operations were disclosed by media reports only in 2006, but they were not terminated. A kind of 'soft law' solution was opted for through the unilateral Representations sent to the EU by UST. It is settled case-law of the ECtHR that secret state schemes, whatever their purpose, cannot be tolerated in a democratic entity operating under the rule of law.[1707] The Court stated in *Klass* that the Contracting States do not

> "enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it,

[1706] Section 358 of the US Patriot Act.
[1707] *See* for instance *Malone v United Kingdom*, (1984), Series A, No 82, para 66.

affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[1708]

The TFTP was operating without any 'law' as understood by the Strasbourg Court for nine years, among which for five under total secrecy. Besides the repercussions that this might have in the EU-US relations (which in any case did not appear to be very serious, as the EU accepted both the unilateral Representations and to negotiate a TFTP framework), huge amounts of financial data were being transferred to the US authorities without any foreseeable and accessible law whatsoever.

b. Objectives of general interest recognised by the Union

According to the EU-US TFTP Agreement, the "exclusive"[1709] purpose of the transfer of financial messaging data is the "prevention, investigation, detection, or prosecution of terrorism or terrorist financing."[1710] This constitutes an objective of general interest recognised by the Union.

c. Necessary

The assessment of the necessity of the TFTP presents the same problems discussed in the case of PNR, since such an analysis has to be based on the US authorities' assertions on the necessity of the SWIFT data in the fight against terrorism. Concerning the Programme's effectiveness the US officials could not be more positive:

"The TFTP has proven to be a powerful investigative tool that has contributed significantly to protecting US citizens and other persons around the world and to safeguarding America's and other countries' national security. The programme has been instrumental in identifying and capturing terrorists and their financiers,

[1708] *Klass and Others v Germany*, (1978), Series A, No 28, paras 48-49.
[1709] *See* Article 1 of the TFTP Agreement.
[1710] *Id.*

> and it has generated many leads that have been disseminated to counterterrorism experts in intelligence and law enforcement agencies around the world."[1711]

Besides general statements, however, any concrete information on the effectiveness of TFTP is missing. Leaving aside the difficulties that exist on getting a grasp on terrorist financing,[1712] SWIFT data do not seem to capture the various alternative systems of money remittance alleged to be used by terrorists.[1713] For instance, an official of the US Treasury Department explains that 'hawala' (which is used as a synonym of ''trust'' in Arabic) refers to a

> "fast and cost-effective method for the worldwide remittance of money or value, particularly for persons who may be outside the reach of the traditional financial sector."[1714]

In particular, "hawala relies upon personal connections to transfer money across international borders."[1715] The alternative ways of money transfer alleged to be used by Al-Qaeda terrorists are very different from the mainstream financial messaging systems that use SWIFT's platform, and the effectiveness, therefore, of the counter-terrorism searches of SWIFT data is questionable.

But even if it is accepted that the TFTP is actually effective in fighting terrorism and has generated many leads, as the US authorities claim, the question of the availability of less extensive alternatives should be examined in order to assess its effectiveness. As the European Parliament has pointed out, there are indeed other alternative routes for the exchange of information with the US.[1716] Besides the various bilateral agreements between the Member States and the US, the EU-US Agreement on Mutual Legal Assistance[1717] allows the exchange of bank information for wider purposes than counter-terrorism and without being limited to the data contained in a specific provider's databases, such as the SWIFT company. In particular, Article 4 of the EU-US Agreement on Mutual Legal Assistance provides:

[1711] *See* UST Representations and the Preamble of the TFTP Agreement.
[1712] Donohue, *supra* note 1482, at 359.
[1713] HEARING BEFORE THE COMMITTEE ON FINANCE US SENATE, FINANCIAL WAR ON TERRORISM: NEW MONEY TRAILS PRESENT FRESH CHALLENGES 35 (107th Congress, October 09, 2002); Donohue, *supra* note 1482, at 365.
[1714] Hearing before the Committee on Finance US Senate, Statement of Under Secretary for Enforcement US Department of the Treasury, James Gurule, *supra* note 771.
[1715] Donohue, *supra* note 1482, at 366.
[1716] *See* above.
[1717] Agreement on Mutual Legal Assistance between the European Union and the United States of America, OJ L 181/34 of 19.7.2003.

"Upon request of the requesting State, the requested State shall, in accordance with the terms of this Article, promptly ascertain if the banks located in its territory possess information on whether an identified natural or legal person suspected of or charged with a criminal offence is the holder of a bank account or accounts. The requested State shall promptly communicate the results of its enquiries to the requesting State."[1718]

The same action may also be taken for the purpose of identifying information in the possession of non-bank financial institutions; or financial transactions unrelated to accounts.[1719] According to the Agreement, such assistance cannot be refused on grounds of bank secrecy.[1720]

The alternative ways of exchange of financial information are not only limited to the EU (or Member States) agreements with the US. At the international level, there exists a framework of financial information exchange based primarily on initiatives against money-laundering, such as for instance, the forty recommendations for fighting money laundering and promoting good financial governance issued by the Financial Action Task Force (FATF),[1721] and the Egmont Group.[1722]

It seems, therefore, that not only there were alternative ways of financial information exchange for counter-terrorism purposes available, which makes the

[1718] Article 4 (1).
[1719] Article 4 (1) (b).
[1720] Article 4 (5).
[1721] The Financial Action Task Force (FATF) is an inter-governmental body founded in 1989, whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. In 1990, FATF adopted 40 Recommendations that "provide a complete set of counter-measures against money laundering (ML) covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation." On 31 October 2001, the FATF issued the 9 Special Recommendations on terrorist financing. The Recommendations require States to 1) ratify the UN International Convention for the Suppression of the Financing of Terrorism and implement relevant UN Resolutions against terrorist financing; 2) criminalize the financing of terrorism, terrorist acts and terrorist organisations; 3) freeze and confiscate terrorist assets; 4) require financial institutions to report suspicious transactions linked to terrorism;
5) provide the widest possible assistance to other countries' laws enforcement and regulatory authorities for terrorist financing investigations; 6) impose anti-money laundering requirements on alternative remittance systems; 7) require financial institutions to include accurate and meaningful originator information in money transfers; 8) ensure that non-profit organisations cannot be misused to finance terrorism; and 9) detect the physical cross-border transportation of currency. *See* http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html.
[1722] The Egmont Group is a group of Financial Intelligence Units (FIUs) established in 1995, whose aim is to improve co-operation in the fight against money laundering and financing of terrorism
and to foster the implementation of domestic programs in this field. The FIU is a "central, national agency responsible for receiving , (and as permitted, requesting) analyzing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation, in order to combat money-laundering or terrorism financing." *See* Interpretative Note concerning the Egmont definition of a Financial Intelligence Unit.

necessity of the TFTP questionable; but the US deliberately chose to circumvent them and adopted a secret system in order to obtain the SWIFT data.

d. Proportionate

Since the EU-US TFTP Agreement interferes, as explained above, with both the rights to privacy and data protection, the analysis of the proportionality of the Agreement will discuss the two fundamental rights separately.

Concerning the interference with the right to privacy, it should be reminded that due to SWIFT's technical capacities the data have to be transferred to the US Treasury Department in bulk. This means that vast amounts of financial communications of people totally unrelated to terrorism are available to UST. This is very worrying, despite the assurances of the Treasury Department that the data are exclusively searched for counter-terrorism purposes.[1723] It is all the more puzzling, that non-extracted data, namely data that are not used for counter-terrorism investigations will be deleted five years after the receipt. Why do these data have to be retained for five years since they are not necessary for the purposes of the Agreement?

Concerning the interference with the right to data protection, the analysis will examine the proportionality of the interference with the various data protection principles. Starting from the purpose limitation principle, the usual problem encountered in the cases of the Data Retention Directive and PNR applies here as well. As in the above mentioned cases, the use of financial messaging data for counter-terrorism investigations is a purpose incompatible with their initial collection necessary in order to effectuate a money transfer.

Furthermore, since the data are transmitted in bulk without any minimization and Europol's control role is very limited the adequacy principle is also interfered with. As noted above with regard to the right to privacy, such interference, to the extent it concerns personal data totally unrelated to terrorism is disproportionate. The same applies to the data retention periods. Besides the fact that non extracted data have to be retained for five years for no obvious reason; the relevant provision on the

[1723] *See* Article 5 (2) of the EU-US TFTP Agreement.

retention periods of the extracted data is even more unclear.[1724] An indeterminate retention time depending on the usefulness of the information for investigations without any meaningful supervision from independent data protection authorities or courts raises questions regarding its proportionality.

Notwithstanding this, the data subjects lack any kind of meaningful participation to the processing of their personal data. Before the media disclosure of the SWIFT case in 2006, EU citizens did not even have the basic right to know that their data might have been transferred to the US for law enforcement purposes. The current TFTP Agreement only guarantees the provision of information to the data subjects, by posting on the website of UST information concerning the TFTP.[1725] The rest due-process rights of the data subjects are mere proclamations. The right to access is turned to a right to obtain confirmation by the US authorities, through a request by the national data protection authority, that no processing has taken place in breach of the Agreement. The same applies to the right of rectification, while the enforceability of the right to redress is very uncertain since the Agreement does not create or confer any right or benefit on any person or entity.[1726]

Finally, an integral part of the right to data protection, as this is laid down in Article 8 EUCFR, is the control of the compliance with the data protection principles by independent authorities.[1727] Such a control is not guaranteed by the TFTP Agreement that grants to Europol a minimal verification role and turns essentially the national data protection authorities to mere "post-boxes of assessments made by the US authorities" in the words of the Article 29 Working Party.[1728]

e. Respect the essence of the right

The bulk transfer of SWIFT financial messaging data to UST, without the possibility of minimisation or effective supervision as to whether they are related to counter-terrorism purposes seems to touch the very essence of the right to data protection. Even if it is accepted that TFTP, unlike PNR, does not involve any data

[1724] Article 6 (7) provides: "Information extracted from Provided Data... shall be retained for no longer than necessary for specific investigations or prosecutions for which they are used."
[1725] Article 14 of the TFTP Agreement.
[1726] Article 20 (1) of the TFTP Agreement. For an analysis *see* above.
[1727] *See* Article 8 (3) EUCFR.
[1728] *See* above.

mining or profiling, as Article 5 (3) of the Agreement stipulates, the interference is disproportionate with regard to the purpose limitation, the adequacy, and the proportionality principles. Furthermore, the procedural rights of the data subject are almost non-existent and an independent supervision is lacking. To the extent that such disproportionate interference affects third parties, such as the beneficiaries of the financial message that might have nothing to do with the person under investigation, the TFTP goes against the 'hard core' of the right to data protection, even if it is assumed that it does not touch the essence of the right to privacy.

Conclusions

This thesis sought to investigate whether data protection as a new fundamental right at the EU constitutional order adds something to the protection provided by the old and venerable right to privacy in the context of law enforcement. The quest undertaken was not easy, since the paradox of data protection in EU law is remarkable. First, its fate has always been inextricably linked with that of privacy, so that it seems almost natural to speak of the two rights together, as a package, rather than to observe them alone in different contexts and circumstances. This means that it is very difficult to assess the very notion of data protection, its purposes and its underlying values without falling back to privacy. Second, while a plethora of data protection laws, either general or sector-specific exist in the EU (Data Protection Directive, ePrivacy Directive, Data Protection Regulation, Data Protection Framework Decision, the specific data protection rules of SIS, VIS, EURODAC) giving the impression that data protection is an omnipresent concern of the EU legislator; the constitutional entrenchment of data protection as a fundamental right next to privacy, albeit welcomed with enthusiasm, raised the question if something had actually changed. There is a third paradox concerning data protection in the EU legal order. The EU may praise itself for being the leader of data protection legislation in the world, but its main counter-terrorism and law enforcement measures affect this right more than any other.

The first Chapter set out the theoretical foundations for the analysis. It attempted to bring clarity on the concept of data protection, its underlying values and aims, and the approaches to this right. Data protection may not pose as many conceptual difficulties as privacy, but its notion is not without problems itself. To understand data protection, one should go to the definitions of 'personal data' and 'processing'. Essentially, data protection describes the set of principles (normally referred to as 'information' or 'data protection' principles) that aim to safeguard certain rights and remedies for individuals when their personal data (information that can be linked to them) are processed (collected, stored, exchanged, etc).

The understanding of data protection in the present thesis, however, went beyond the concept of the management or control over personal information. Data protection should be understood as informational autonomy which ensures that the individuals enjoy a right to dignity when their personal information is processed using

modern technological tools. Leaving aside its philosophical underpinnings, the understanding of data protection as informational autonomy rather than informational control means that this has strong links with the fundamental right to dignity and is not deduced to a mere aspect of privacy, expressed through the control over personal information conceptualisation of privacy.

Based on this premise, the research did not purport to examine the nature of the relationship between privacy and data protection, keeping a distance from discussions on the 'separateness' or 'autonomy' of a right to data protection. This does not mean, however, that privacy and data protection are identical rights. On the one hand, what privacy protects is not irreducible to personal information. The concept of privacy embodies a range of further values, such as intimacy, seclusion, secrecy, personhood, etc. On the other hand, data protection differs from privacy for three main reasons. First, not all personal data are necessarily data that affect an individual's private life. Second, data protection does not pursue only privacy aims. On the contrary, it transcends privacy and extends to cover further values and functions. Third, unlike privacy that has an elusive and, therefore, subjective nature, data protection displays a certain degree of objectivity as this right is essentially *procedural* by nature. Despite all these differences, it cannot be denied that data protection compared to privacy is a relatively new right, and that historically the common justification used for the enactment of data protection legislation referred to the right to privacy. This explains why conceptual confusions arose since the birth of the infant of the two rights and (still) continue to exist.

The research went on to examine in detail the underlying values behind the right to data protection. What does data protection aim to protect and how are its principles constructed? It was argued that privacy is one of the main values that data protection aims to safeguard. This statement has to be further qualified. Which of the various conceptions of privacy do data protection laws aim to advance? Is it all about control over personal information? A closer look at the data protection principles reveals that, beyond informational privacy, they express further privacy concerns, such as non-interference, limited access to oneself, and even conceptions of privacy such as intimacy. This is seen, for instance, in the rule that prohibits the processing of sensitive data.

It should be stressed, however, that the story does not end there. Data protection pursues several further purposes, distinct from privacy. One important

function that data protection laws aim to safeguard is data security. Data security is the interest of keeping the data secure against certain risks, such as the risks of data being lost or accessed by unauthorised persons. In the age of information technology, data security has acquired a particular importance for the general public, as data protection concerns are most commonly associated with fears of loss or unwarranted access to personal data files, reinforced by relevant scandals exposed by the media. A further interest pursued by data protection is data quality. Data quality refers to the accuracy, adequacy, relevance and up-to-dateness of the personal information. Data quality is not merely an important safeguard for the data subjects, it is also a major interest for data controllers that might have to face erroneous results –and significant losses- if the data they process are not accurate. At the very heart of data protection legislation lie the values of transparency, foreseeability in data processing, accountability of data controllers, and meaningful participation of the data subject in the processing of his/ her information. These values are voiced in different fair information principles, mainly, in the principle of fair and lawful processing, in the purpose specification principle, and in the individual participation principle. These principles aim to address the inequalities and power asymmetries between data controllers and data subjects concerning the collection and processing of their personal information. Data protection legislation pursues also other values, such as non-discrimination and proportionality. These purposes are enshrined in the prohibition of the processing of data revealing ethnic or racial origin, political opinions, religious beliefs, sexual orientation and health, the prohibition of decisions based on automated processing of personal data, and the principle that personal data should not be retained longer than necessary.

Nevertheless, questions still remain concerning the exact nature of data protection. Is it a human right, a factor of economic growth, a consumer concern, or something else? The different approaches to data protection were discussed and it was explained that data protection in the EU did not exactly appear as a human right. Instead, it was initially conceived as a necessary factor that would permit freedom of movement (of data), and therefore economic growth. This "factor" happened to be, however, closely connected with a fundamental human right: the right to privacy. Data protection, therefore, rose in the EU to the status of a right thanks to its closeness to privacy, but this meant that it was never fully disassociated from this, even after its constitutional entrenchment.

The thesis then turned to discuss the two current theories on data protection. The first, which I called 'separatist' considers privacy and data protection as two distinct tools of power control that perform different functions. Privacy, on the one hand, is the 'opacity' tool that protects individuals against the illegitimate use of power, while data protection is the 'transparency' tool, which regulates the legitimate use of power. The second, which was referred to as the 'instrumentalist' approach contends that data protection cannot be put at the same level as privacy because that would endanger the latter fundamental right and its anchoring in further values, such as dignity and autonomy.

Both theories have problems, not the least because both view data protection through privacy, even if their end results are diametrically different: the 'separatist' approach glorifies the constitutional entrenchment of the right to data protection; the 'instrumentalist' approach negates it.

Attempting to build a new theory on data protection, the thesis started from the basic premise that this must have focus, and its focus must be the right to data protection itself. This was identified as the main problem of the current approaches on data protection: they both see data protection through the lens of privacy and they end up developing a theory on the relationship and the respective functions of the two rights. Such an approach was criticised, nevertheless the present thesis accepted that it is not easy to look at the two rights separately taking into account their close relationship that essentially made the two theories discussed unable to disassociate the one right from the other.

The thesis, here, encountered some difficulties. Trying to see data protection alone presupposes that this has a function of its own and can operate as a fully-fledged fundamental right. This means that data protection, if it were to add something to privacy; it should be able to regulate, but also to prohibit power. However, as the right is currently interpreted, it faces limitations: it can function positively –as a regulator of power-, but it cannot function negatively –imposing a rule of non-interference. These limitations, whether they are attributed to the drafters of the right, or the particularities of its genesis and its initial drafting to take into account economic concerns, demonstrate that data protection is not 'mature' to operate alone, as it currently stands.

It was argued, therefore, that data protection needs to be *reconstructed* if it is to be recognised as a *bona fide* fundamental right with a value of its own. There are

certain conditions for reconstructing the right to data protection. First, this must have an *'essential core'* that cannot be overridden. This necessarily raises a difficult question: What is the 'essential core' of the right to data protection? The answer is not easy, but this thesis argued that there is a 'core' of data protection principles that must be ensured under all circumstances so that data protection can guarantee the dignity and autonomy of our personality when our personal data are processed.

The second condition is that, recognising that data protection is not an absolute right, this must be balanced against opposing interests *as such* and *not* through the proxy of privacy. This means that insofar as the right to data protection is applicable - when the case at hand involves the processing of personal data- and there is a *prima facie* interference with one or more data protection principles, then the assessment of whether this is justified or not should be carried out on the basis of the data protection principles themselves, with the application of the principle of proportionality, without the need to recourse to the right to privacy. Determining disproportionate processing on the basis of the right to privacy and not of the specific data protection principle that this goes against, is not only an unnecessary circumvention of the existing law that renders data protection virtually useless, but it is also dangerous, because there could be instances of disproportionate processing of personal data that hardly, however, constitute disproportionate interferences with the right to privacy.

Having set out a new theory on data protection, the thesis turned to examine in detail how this right is seen by the European courts. The Strasbourg Court has recognised in a series of judgments data protection as an aspect of the right to private and family life found in Article 8 ECHR. The situation should be different in the EU, where data protection is expressly recognised as a fundamental right. The data protection paradox, however, is present here. While the Luxembourg Court has recognised that there is a fundamental right to data protection in the EU legal order, when it comes to balancing this with opposing interests or rights, the Court cannot disassociate it from privacy. The case-law of the Court demonstrates that when the need to balance data protection with other rights and interests is at stake, the Court essentially creates a new right, which it calls 'the right to respect for private life with regard to the processing of personal data.'

This is certainly regrettable, all the more because the EU Charter of Fundamental Rights, which is binding after the entry into force of the Lisbon Treaty, provides the necessary tool for the reconstruction of data protection to be able to

operate as a fully-fledged fundamental right. This can be found in Article 52 (1) EUCFR, which sets out the conditions under which a right of the Charter can be limited. If the Court followed this path, instead of having to go back to the right to privacy in conjunction with Article 8 (2) ECHR, it would allow data protection to rise from the shadow of privacy.

Having introduced a new theory on data protection (Part I), the thesis attempted to test the added value of the right in the most difficult context: law enforcement and counter-terrorism (Part II). For this purpose, three specific case-studies of data processing in the field of counter-terrorism that involve different instances of data processing were employed: 1) the information collection; 2) the information storage; and, 3) the information transfer case.

Before entering in this discussion, however, it was necessary to lay down more in detail the EU data protection legal framework. It was argued that this is (still) profoundly affected by the EU pillar structure, even if the Lisbon Treaty abolished it since the 1st December 2009. While at the constitutional level, Article 16 TFEU applies to processing of the (former) first and the (former) third pillar; the secondary legal framework is divided to different measures applying to Community and police and judicial cooperation in criminal matters. In this respect, the Commission's proposal for a new (and hopefully improved) data protection legal framework is anticipated with great interest.

The third Chapter set the background of EU counter-terrorism policies. The EU's counter-terrorism strategy changed dramatically since the September 11 attacks in the US from a loose intergovernmental cooperation to the adoption of numerous policy instruments at the higher level (Strategies, Action Plans, Conclusions, Recommendations) that were implemented into concrete legislative instruments. The EU's commitment in the fight against terrorism increased even more after Europe itself became a target in the Madrid and London terrorist bombings. Despite this commitment, the EU's power in combating terrorism is limited not the least because the EU is not a State with police and executive powers itself. This means that the main way in which the EU can fight terrorism is by enhancing and facilitating the Member States' law enforcement initiatives.

For this reason, the EU's main contribution to counter-terrorism is found in the exchange of information channels it has established based on a *proactive* and *intelligence-led* approach that purports to unravel terrorist networks and identify

potential terrorists before they act. The information network organised at the EU is vast and it comprises numerous actors and a plethora of ways of information exchange. The EU itself, Member States, third countries, and private actors are involved in an extensive information-sharing. Privacy and data protection are the main fundamental rights challenged by the EU's counter-terrorism policies.

Part II of the thesis examined the added value of data protection as a fundamental right by utilising four specific EU counter-terrorism measures that involve information processing: the Data Retention Directive, the exchange of information through the EU large-scale databases (SIS II, VIS, EURODAC), the EU-US PNR Agreements, and the EU-US TFTP Agreement. The four cases were grouped in three categories that concern different instances of information processing: the information collection case (Data Retention Directive), the information storage case (SIS II, VIS, EURODAC), the information transfer case (PNR, TFTP). It should be noted, however, that all the measures discussed concern different types of processing that are not limited to the category under which they were analysed.

The four specific counter-terrorism measures addressed bear more similarities than differences between each other. Three of them use data collected by the private sector ('commercial data') in the course of commercial activities in order to fight terrorism and/or crime (the Data Retention Directive, PNR, TFTP). Despite this similarity, one measure was considered to fall under the internal market competence (Data Retention Directive), while the other two under police cooperation in criminal markets. In the case of the EU databases, two of them (VIS, EURODAC) have nothing to do with police cooperation and law enforcement purposes, yet it was considered that access should be granted to law enforcement authorities in order to fight terrorism. SIS II is more particular: the system has always been used for law enforcement purposes along with other objectives concerning mainly the fortification of the EU's external borders. Furthermore, both the PNR and TFTP cases have a 'unilateral' element in that they concern the transfer (and, not the exchange) of data to third countries (the US). However, despite the severe criticisms raised against these two measures by various voices within the EU, it is being currently contemplated whether the Union should establish its own PNR and TFTP systems.

Chapter 4 discussed the Data Retention Directive. The Directive was adopted as a response to the Madrid and London terrorist attacks and obliged the telecommunications' service providers to retain the traffic and location data of every

communication carried out by their customers for a period of 6 months to 2 years for the purposes of fighting serious crime. Applying the theory developed in the first Part, the research attempted to examine separately whether the Directive interferes with the right to privacy and the right to data protection. In this regard, it was argued that the Data Retention Directive poses above all a privacy issue since it interferes directly with the confidentiality or secrecy of communications. The fact that the content of the data is not retained does not change this conclusion. Employing case-law from the European Court of Human Rights, it was submitted that the interference posed to the right to privacy is disproportionate already at the level of the Directive (and without having to go into the various implementation laws of the different Member States).

The right to data protection is also implicated, not the least because data intended to be used by service providers for billing purposes are being utilised for utterly different purposes, i.e. to fight crime under the Directive. However, it was contended that the analysis should not accept straightforwardly an interference with data protection just because an interference with the right to privacy exists. However, it was contended that the analysis should not accept straightforwardly an interference with data protection just because an interference with the right to privacy exists. If it is to be accepted that data protection is a different fundamental right, then it has to be examined independently. In this respect, it had to be assessed, first, whether the retention of traffic and location data constitutes processing of personal data; and, second, which data protection principles were interfered with by the Directive. With some nuances concerning Internet communications, it was accepted that the retention of such data to be used for law enforcement purposes constitutes processing, and that this interfered with two specific data protection principles: purpose limitation and data minimisation. Besides the changing of purposes of the traffic and location data retained, the data minimisation is a real problem of the Directive, taking into account that it imposes the retention of *all* communications, of *every* person, without any further criteria or basis of suspicion, and for quite considerable time periods.

Not surprisingly, the Data Retention Directive has been the object of litigation before courts (EU and national). The Court of Justice has focused its attention on one particular, technical aspect: the question of its legal base. When this was challenged by Ireland, the Court confirmed that the Directive falls indeed under internal market competences. On the contrary, the national courts focused their attention on the fundamental rights' questions raised by the transposing laws of the Directive. The

German Constitutional Court in its decision found a number of problems in the implementing law of the Directive in Germany and annulled it. It was submitted that this Court's decision is very welcome, all the more because it poses the fundamental rights' problem at the correct basis: the issue concerns above all the secrecy of telecommunications. The Romanian Constitutional Court's analysis is also very interesting, especially where the Court opined (surprisingly enough) that the legal obligation for the retention of the data is more problematic than its justified use by law enforcement authorities. The Czech Constitutional Court's decision, despite its important fundamental rights' pronouncements, fell in the normal fallacy, criticised numerous times in this thesis, of treating privacy and data protection as the same right, which was called by the Czech Constitutional Court as "the right to privacy in the form of informational self-determination."

The storage and exchange of information through three EU-large databases (SIS II, VIS, EURODAC) was addressed in the fifth Chapter. The Schengen Information system was created as one of the main compensatory measures for the abolition of the internal borders laid down by the Schengen Convention. It is a database that stores data for immigration and law enforcement purposes and it can be accessed by a wide range of authorities. The Second Generation system grants access also to Europol and Eurojust, and increases the capabilities of the database by including biometric data and providing for the interlinking of alerts. In this respect, fears have been raised that the system, when it becomes operational, might turn into a multipurpose search tool for police and law enforcement authorities.

The Visa Information System was established in order to store in a centralised database the data of visa applicants that want to enter the EU Member States. In 2008 a Council Decision was adopted allowing access to VIS data for law enforcement purposes. This thesis criticised severely such a measure because the initially purpose of creating the database is totally frustrated in a way that cannot be foreseen by individuals applying for a visa. A similar measure was proposed with regard to EURODAC that constitutes an EU database storing the data of asylum seekers and illegal cross borders. In this regard, it was stressed that the concerns about 'function creep' raised with regard to VIS apply *a fortiori* in the case of EURODAC. Fortunately, the proposed measure was dropped from the Commission's agenda, at least for the time being. A further problem concerning all three databases is the proposed establishing of interoperability between them. The plan may be abandoned

for the moment, but the creation of an Agency as a Management Authority of the three databases raises questions on whether a form of interoperability might be introduced from the back door.

Having discussed the three databases in detail, it was time to assess the question whether the databases pose a privacy or a data protection problem. Starting from the premise that the storage and exchange of personal data through EU centralised large-scale IT systems constitutes processing of personal data, this thesis argued that the problem posed by the databases is better dealt by the right to data protection. This is, first, because the information stored in the databases does not seem to pose an obvious privacy problem, since it refers mostly to data that, while personal, they are not private. From this category we should exclude certain sensitive data (for instance, ethnicity or criminal convictions) that might raise privacy problems. Second, it is because the data protection principles can deal better with each one of the different problems raised by the databases: data security, data quality, purpose limitation, data minimisation, rights and remedies of the data subject, accountability of the data processor, independent supervision. For this reason, each database has its own set of data protection rules that attempt to address the different problems this poses with regard to the processing of personal data. In the case of the EU systems and in particular SIS II and VIS, these rules were not considered by the present thesis as adequate or complying with the EU's data protection standards.

Chapter 6 examined in detail the EU-US Passenger Name Record saga that commenced in 2001 and is still to be continued. When EU airlines companies were faced with the dilemma to lose landing rights in the US soil or to violate EU data protection legislation if they refused to transmit data of their customers regarding the flight, the Commission had to start negotiations with the US. The result was that the EU confirmed in 2004 the adequacy of the CBP Undertakings- 48 assurances issued by the US Customs and Border Protection. When the Commission's and the Council's adequacy decisions were annulled in 2006 by the Court of Justice for being adopted under the wrong pillar, the EU entered into a second round of negotiations that resulted this time in an Interim Agreement followed by a letter from the US Department of Homeland Security interpreting unilaterally a number of its provisions. When the Interim Agreement was about to expire, a third Agreement was concluded with the US, which was basically built around a DHS letter. Currently, a new PNR Agreement is being negotiated with the US authorities.

The discussion on privacy and data protection has been at the heart of the EU-US PNR. The thesis argued that despite the conceptual misconceptions between the two rights, PNR interferes primarily with the right to data protection. While PNR are not data that particularly *affect the individual's private sphere*, in the words of Advocate General Léger,[1729] they are personal data, and consequently their transfer constitutes an interference with the right to data protection not the least because they are used for purposes entirely different from the ones for which they were provided by the individuals wishing to book an airline ticket. The specific data protection principles are, thus, the right forum to discuss whether such interference is disproportionate, instead of the general privacy right that cannot catch all the problems posed by the PNR transfer. In particular, besides the purpose limitation principle, the transfer of PNR data to the DHS and their processing for law enforcement purposes poses limitations to the adequacy principle, the fairness principle concerning the period of the retention of the data, and possibly the data subject's due process rights. The analysis concluded that many of these principles are not sufficiently safeguarded in the latest EU-US PNR Agreement. Furthermore, many issues are raised from the fact that the PNR data are mostly used for the purpose of drawing up terrorist profiles based on certain characteristics and applying them to the general group of travellers in order to identify potential dangerous people.

Chapter 7 focused on another information transfer case, the Terrorist Finance Tracking Programme. TFTP has a number of similarities with PNR, but also important differences. As in the case of PNR, soon after the September 11, 2001 attacks the US authorities demanded from SWIFT, a Belgian company that operates a worldwide messaging system used to transmit financial transaction information to transmit a substantial part of its data concerning the financial transactions carried out using its platform to the US Department of Treasury. The purpose was to unravel the cash flows of terrorist networks and "starve terrorists of funding."[1730] SWIFT was delivering financial transactions' data to the US authorities secretly for more than five years, until the programme was revealed by a series of newspaper articles in the US. The revelation caused a wave of criticisms in Europe, but the US did not terminate the scheme. Instead, a temporary solution was sought, under which the US sent a set of unilateral statements to the EU which described the controls and safeguards governing

[1729] Opinion of Advocate General *Léger,* Joined Cases C-317/04 and C-318/04 *PNR*, para 229.
[1730] *See* Statement of US President George Bush, September 24, 2001.

the handling, use and dissemination of data under the Treasury Department's Terrorist Financing Tracking Programme. When SWIFT announced the restructuring of its architecture, the EU and the US had to enter into negotiations to conclude an Agreement that permitted the continuation of the transfer of SWIFT data to the US authorities. The Agreement was signed on 30 November 2009, one day before the entry into force of the Lisbon Treaty. Feeling that it was sidestepped in the negotiations, the Parliament refused to give its consent to the conclusion of the Agreement under its new powers acquired after the Lisbon Treaty entered into force. After the Parliament's rejection, new negotiations had to be reopened with the US, which resulted this time in an Agreement that was duly concluded with the consent of the Parliament. Contrary to the general impression that the 2nd Agreement was improved compared to the first, this thesis submitted that there were not significant changes.

It was argued that, unlike PNR that poses above all a data protection issue, TFTP raises a privacy problem. In this respect, it resembles more to the Data Retention Directive discussed in the forth Chapter. The transfer of financial messaging data constitutes a form of communication before the payee and the beneficiary. This communication, albeit limited to financial information, it might reveal a lot on a person's financial movements, the people she transfers money to, even her donations to charitable organisations and NGOs. Therefore, it should enjoy confidentiality, which means that its processing for counter-terrorism purposes interferes with the right to privacy. Furthermore, TFTP poses data protection problems as well: above all, the purpose limitation principle is put, here again, under question.

Having discussed the different case-studies, we should go back to the main question of this thesis: "does data protection have an added value as a fundamental right in the context of law enforcement?" It is submitted that it does for two main reasons. First, data protection has a *practical significance* (both actual and potential). Data protection with its fair information principles can provide specific guidance *ex ante* and *ex post* on the problems posed by different instances of processing. In this respect, some could contend that it operates as the *lex specialis* of privacy. This approach, however, was rejected in the present thesis because it was demonstrated that data protection pursues further values than privacy. Second, if data protection is to be understood as a fully-fledged fundamental right, as it was reconstructed in the

first Chapter, it acquires a *normative importance* in the context of law enforcement.[1731] This is crucial in cases that privacy, despite its wide notion is not applicable, for instance, because there is no obvious privacy problem. But even if a privacy issue exists, data protection does not lose its added value. As the case-studies demonstrated, privacy and data protection questions might co-exist without referring to the same problem of a particular measure. This was seen in the case of the Data Retention Directive and the TFTP.

A closely related critical remark that was advanced in this thesis concerned the way privacy and data protection are currently viewed by most courts and legal scholars. It was argued that it is erroneous to see the two rights as a package and to assume that an interference with the one means also necessarily an interference with the other. This is unacceptable, first, because the EU Charter of Fundamental Rights recognises clearly a right to data protection as well as a right to privacy. Second, the conceptual confusions between the two rights should be avoided because they cause problems especially in the cases where there is no interference with privacy, but there is with data protection (or vice-versa) as the analysis of the Opinion of the Advocate General in PNR has demonstrated. The thesis illustrated that this issue is not merely theoretical, but it can also have important practical implications.

Finally, a further lesson learnt from the analysis of the case studies is that when European Courts assess the permissibility of interferences with data protection, they should follow a different pattern, namely this provided in Article 52 (1) of the EU Charter of Fundamental Rights. Surely, using Article 8 (2) ECHR instead might come more handy because of the guidelines offered by the extensive case-law of the Strasbourg Court, but this means that in the end one must fall back to privacy and attempt to justify why there is an interference with this right. This path unduly complicates the analysis and might produce erroneous results. A new path is, however, available after the entry into force of the Lisbon Treaty. Since the EU Charter of Fundamental Rights provides now for a tool, such as Article 52 (1), this should be used by the Courts if they want to avoid problematic judgments based on confusions between the two rights.

[1731] *See* BYGRAVE, DATA PROTECTION LAW, *supra* note 8, at 3.

Bibliography

Abel, Wiebke, and Burkhard Schafer, 'The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822' (2009) 6 SCRIPT-ed, 106.

ACLU, 'Why the 'Registered Traveler' Program Will Not Make Airline Passengers Any Safer', August 2006.

Arai-Takahashi, Yutaka, *The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR* (Intersentia 2002).

Arendt, Hannah, *The human condition* (2nd ed. University of Chicago Press 1998).

Argomaniz, Javier, 'When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms' (2009) 31 Journal of European Integration, 119.

Article 29 Working Party, 'Working Document Privacy on the Internet - An integrated EU Approach to On-line Data Protection', November 21, 2000.

——, 'Working document on biometrics', August 1, 2003.

——, 'Opinion 4/2007 on the concept of personal data', no date.

——, 'Opinion 1/2010 on the concepts of 'controller' and 'processor'', no date.

——, 'Opinion 10/2001 on the need for a balanced approach in the fight against terrorism', no date.

——, 'Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Council doc. 8958/04 – April 28, 2004)]', no date.

——, ‘Opinion 113/2005 on the 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 of 21.09.2005)’, no date.

——, ‘Opinion 3/2006 on the Directive 2006/XX/EC 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, as adopted by the Council on 21 February 2006’, no date.

——, ‘Opinion 4/2005 on the 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 of 21.09.2005)’, no date.

——, ‘Opinion 6/2005 on the Proposals for a Regulation of the European Parliament and of the Council (COM (2005) 236 final) and a Council Decision (COM (2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final)’, no date.

——, ‘Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)’, no date.

——, ‘Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States’, no date.

——, ‘Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States’ Bureau of Customs and Border Protection (US CBP)’, no date.

——, ‘Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States’, no date.

——, ‘Opinion 5/2007 on the follow-up 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 concluded in July 2007’, no date.

——, ‘Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data’, no date.

——, ‘Opinion 10/2011 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’, no date.

——, ‘Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’, no date.

Article 29 Working Party, Working Party on Police and Justice, ‘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’, December 1, 2009.

——, ‘Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007’, no date.

Assey, James, and Demetrios Eleftheriou, ‘The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters’ (2001) 9 CommLaw Conspectus, 145.

AuBuchon, Michael, ‘COMMENT: CHOOSING HOW SAFE IS ENOUGH: INCREASED ANTITERRORIST FEDERAL ACTIVITY AND ITS EFFECT ON THE GENERAL PUBLIC AND THE AIRPORT/AIRLINE INDUSTRY’ (1999) 64 J. Air L. & Com., 891.

Aus, Jonathan, 'Supranational Governance in an 'Area of Freedom, Security and Justice': Eurodac and the Politics of Biometric Control', 2003.

Bailey, Joe, 'From Public to Private: The Development of the Concept of the 'Private'' (2002) 69 Social Research: An International Quarterly, 15.

Baker, Ellen, 'FLYING WHILE ARAB- RACIAL PROFILING AND AIR TRAVEL SECURITY' (2002) 67 J. Air L. & Com., 1375.

Bakker, Edwin, 'Differences in Terrorist Threat Perceptions in Europe' in Dieter Mahncke and Jörg Monar (eds), *International terrorism : a European response to a global threat?* (P.I.E.-Peter Lang 2006), 47.

Baldaccini, Anneliese, 'Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases' (2008) 10 European Journal of Migration and Law, 31.

Balzacq, Thierry, 'The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies' (2007) 46 Journal of Common Market Studies, 75.

Barcelo, Rosa, 'Seeking Suitable Options for Importing Data from the European Union' (2002) 36 Int'l L., 985.

Barnes Morey, Elizabeth, 'Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive' (2007) 27 Nw. J. Int'l L. & Bus., 171.

Bayo Delgado, Joaquín, 'The Area of Freedom, Security and Justice and the role of national courts in the EU data protection system' in Elspeth Guild and others (eds), *THE AREA OF FREEDOM, SECURITY AND JUSTICE TEN YEARS ON SUCCESSES AND FUTURE CHALLENGES UNDER THE STOCKHOLM PROGRAMME*, 2010, 31.

Beaney, William, 'The Right to Privacy and American Law' (1966) 31 L. & Contemp. Probs., 253.

Belgium Privacy Commission, 'Opinion No. 37/2006 of 27 September 2006 on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas', no date.

——, ‘Decision of 9 December 2008, Control and recommendation procedure initiated with respect to the company SWIFT scrl’, no date.

Bennett, Colin, and Charles Raab, *The governance of privacy : policy instruments in global perspective* (MIT Press 2006).

Berčič, Boštjan, and Carlisle George, ‘Investigating the legal protection of data, information and knowledge under the EU data protection regime’ (2009) 23 International Review of Law, Computers & Technology, 189.

Bergkamp, Lucas, ‘EU Data Protection Policy - The Privacy Fallacy: Adverse Effects of Europe’s Data Protection Policy in an Information-Driven Economy’ (2002) 18 Computer Law & Security Report, 31.

Bertozzi, Stefano, ‘Schengen: Achievements and Challenges in Managing an Area Encompassing 3.6 million km^2’, February 2008.

BeVier, Lillian, ‘Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection’ (1995) 4 William and Mary Bill of Rights Journal, 455.

Bezanson, Randall P., ‘The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990’ (1992) 80 California Law Review, 1133.

Bignami, Francesca, ‘Privacy and Law Enforcement in the European Union: The Data Retention Directive’ (2007) 8 Chicago Journal of International Law, 233.

——, ‘European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining’ (2007) 48 Boston College Law Review, 609.

——, ‘The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts’ (2008) 41 Cornell International Law Journal, 211.

Bigo, Didier, and Sergio Carrera, ‘From New York to Madrid: Technology as the Ultra-Solution to the Permanent State of Fear and Emergency in the EU’, 2004.

Birnhack, Michael, ‘The EU Data Protection Directive: An engine of a global regime’ (2008) 24 Computer Law & Security Report, 508.

Blanke, Jordan, 'Safe Harbor and the European Union's Directive on Data Protection' (2001) 11 Alb. L.J. Sci. & Tech., 57.

Bloustein, Edward J., 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 N.Y.U. L. Rev., 962.

Blume, Peter, 'Transborder Data Flow: Is There a Solution in Sight' (2000) 8 Int'l J.L. & Info. Tech., 65.

Boehm, Franziska, *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 2012).

Boer, Monica den, 'Fusing the Fragments. Challenges for EU Internal Security Governance on Terrorism' in Dieter Mahncke and Jörg Monar (eds), *International terrorism : a European response to a global threat?* (P.I.E.-Peter Lang 2006), 83.

Boer, Monica den, Claudia Hillebrand, and Andreas NöLke, 'Legitimacy under Pressure: The European Web of Counter-Terrorism Networks' (2007) 46 Journal of Common Market Studies, 101.

Boer, Monica den, ed., *Schengen, judicial cooperation and policy coordination* (European Institute of Public Administration 1997).

——, *The implementation of Schengen: first the widening, now the deepening* (European Institute of Public Administration 1997).

Bok, Sissela, *Secrets : on the ethics of concealment and revelation* (Vintage Books ;;Random House 1989).

Bossong, Raphael, 'The Action Plan on Combating Terrorism: A Flawed Instrument of EU Security Governance' (2007) 46 Journal of Common Market Studies, 27.

Botta, Marco, and Mario Viola de Azevedo Cunha, 'LA PROTEZIONE DEI DATI PERSONALI NELLE RELAZIONI TRA UE E USA, LE NEGOZIAZIONI SUL TRASFERIMENTO DEI PNR' (2010) XXVI IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA, 315.

Breckenridge, Adam Carlyle, *The Right to Privacy* (University of Nebraska Press 1970).

Brenner, Susan, 'Constitutional Rights and New Technologies in the United States' in Ronald Leenes and others (eds), *Constitutional rights and new technologies : a comparative study* (T.M.C. Asser Press ;;Distributed by Cambridge University Press 2008), 225.

Breyer, Patrick, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) 11 European Law Journal, 365.

Broeders, Dennis, 'The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants' (2007) 22 International Sociology, 71.

Brouwer, Evelien, 'Eurodac: Its Limitations and Temptations' (2002) 4 European Journal of Migration and Law, 231.

——, 'Immigration, Asylum and Terrorism: A Changing Dynamic Legal and Practical Developments in the EU in Response to the Terrorist Attacks of 11.09' (2003) 4 European Journal of Migration and Law, 399.

——, 'Data surveillance and border control in the EU: Balancing efficiency and legal protection of third country nationals', 2005.

——, *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System* (M. Nijhoff 2008).

——, 'The EU Passenger Name Record System and Human Rights: Transferring passenger data or passenger freedom?', September 2009.

Brown, Ian, 'Communications Data Retention in an Evolving Internet' (2010) 19 International Journal of Law and Information Technology, 95.

Brown, Ian, and Douwe Korff, 'Terrorism and the Proportionality of Internet Surveillance' (2009) 6 European Journal of Criminology, 119.

Burkert, Herbert, 'Towards a New Generation of Data Protection Legislation' in *Reinventing data protection?* (Springer 2009), 335.

Busser, Els de, *Data protection in EU and US criminal cooperation: a substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities* (Maklu Publishers ; International Specialized Book Services 2009).

——, 'EU data protection in transatlantic cooperation in criminal matters: Will the EU be serving its citizens an American meal ?' (2010) 6 Utrecht Law Review, 86.

Busser, Els de, and Gert Vermeulen, 'Towards a coherent EU policy on outgoing data transfers for use in criminal matters? The adequacy requirement and the framework decision on data protection in criminal matters' in *EU and International Crime Control: Topical Issues* (Governance of Security (Gofs) Research Paper Series, Vol. 4. Maklu Pub 2010), 95.

Buttarelli, Giovanni, 'Legal Restrictions – Surveillance and Fundamental Rights', June 19, 2009.

——, 'What future for the Data Retention Directive', May 4, 2011.

Bygrave, Lee, 'Data protection pursuant to the right to privacy in human rights treaties' (1998) 6 International Journal of Law and Information Technology, 247.

——, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law' (2000) 7 Privacy Law & Policy Reporter, 11.

——, 'The Place of Privacy in Data Protection Law' (2001) 24 University of New South Wales Law Journal, 277.

——, 'Automated Profiling. Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 Computer Law & Security Report, 17.

——, *Data protection law : approaching its rationale, logic, and limits* (Kluwer Law International 2002).

——, ‘International agreements to protect personal data’ in James Rule and Graham Greenleaf (eds), *Global privacy protection the first generation* (Edward Elgar, 2008), 15.

Bygrave, Lee, and Dag Wiese Schartum, ‘Consent, Proportionality and Collective Power’ in *Reinventing data protection?* (Springer 2009), 157.

Cannataci, Joseph, and Jeanne Pia Bonnici Mifsud, ‘The end of the purpose-specification principle in data protection?’ (2010) 24 International Review of Law, Computers & Technology, 101.

Carrera, Sergio, ‘What Does Free Movement Mean in Theory and Practice in an Enlarged EU?’ (2005) 11 European Law Journal, 699.

Casale, Davide, ‘EU Institutional and Legal Counter-terrorism Framework’ (2008) 1 Defence Against Terrorism Review, 49.

Castor, David, ‘Treading Water in the Data Privacy Age: An Analysis of Safe Harbor’s First Year’ (2002) 12 Ind. Int’l & Comp. L. Rev., 265.

Cate, Fred H, ‘Government Data Mining: The Need for a Legal Framework’ (2008) 43 Harvard Civil Rights - Civil Liberties Law Review, 435.

Center for International Legal Studies, *Data transmission and privacy* (Dennis Campbell (ed), M. Nijhoff ;;Sold and distributed in the U.S.A. and Canada by Kluwer Academic Publishers 1994).

Chaban, Natalia, Ole Elgstrom, and Martin Holland, ‘The European Union as Others See It’ (2006) 11 European Foreign Affairs Review, 245.

Chandrasekhar, Charu, ‘Flying While Brown: Federal Civil Rights Remedies to Post-9/1 1 Airline Racial Profiling of South Asians’ (2003) 10 Asian L.J., 215.

Charlesworth, Andrew, ‘Clash of the Data Titans - US and EU Data Privacy Regulation’ (2000) 6 Eur. Pub. L., 253.

——, ‘Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?’ (2003) 54 Hastings L.J., 931.

Chertoff, Michael, 'A Tool We Need to Stop the Next Airliner Plot', August 29, 2006.

Cholewinski, Ryszard, 'The Criminalisation of Migration in EU Law and Policy' in Anneliese Baldaccini and others (eds), *Whose Freedom Security and Justice? EU Immigration and Asylum Law and Policy* (Hart 2007), 301.

Christou, Vasiliki, 'The Council Decision of 12 June 2007 on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II)' (2008) 14 Colum. J. Eur. L., 649.

Clarke, Roger, 'The Digital Persona and its Application to Surveillance' (1994) 10 The Information Society, 77.

——, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' [no date] .

——, 'Biometrics' Inadequacies and Threats, and the Need for Regulation', no date.

Classen, Claus Dieter, 'Joined Cases C-465/00, C-138/01 & C-139/01, Österreichischer Rundfunk, Judgment of 20 May 2003, Full Court, [2003] ECR I-4989' (2004) 41 Common Market Law Review, 1377.

Cohen, Julie E., 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stan. L. Rev., 1373.

Commission Staff Working Paper, '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, Washington, 20-21 September 2005', December 12, 2005.

Connolly, Thomas, and Carolyn Begg, *Database systems: a practical approach to design, implementation, and management* (5th ed. Addison-Wesley 2010).

Counter-terrorism Coordinator, 'Implementation of the EU Counter-terrorism strategy - Discussion paper', November 23, 2007.

Crandall, Robert, 'Security for the Future: Let's Get Our Airlines Flying, 2001 Airline Security and Economic Symposium' (2002) 67 J. Air L. & Com., 9.

Cremona, Marise, 'Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement' (Austrian Academy of Sciences March 2011).

——, 'EU External Action in the JHA Domain: A legal perspective', no date.

Currie, David, 'Positive and Negative Constitutional Rights' (1986) 53 U. Chicago. L. Rev., 864.

Delany, Hilary, and Eoin Carolan, *The right to privacy : a doctrinal and comparative analysis* (Thomson Round Hall 2008).

Dempsey, James, and Lara Flint, 'Commercial Data and National Security' (2004) 72 The George Washington Law Review, 1459.

DeSimone, Christian, 'Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive' (2010) 11 German Law Journal, 291.

DiLascio, Tracey, 'How Safe Is the Safe Harbor - U.S. and E.U. Data Privacy Law and the Enforcement of the FTC's Safe Harbor Program' (2004) 22 B.U. Int'l L.J., 399.

Donke, Wim van de, Colin Bennett, and Charles Raab, 'The politics and policy of data protection: experiences, lessons, reflections and perspectives' (1996) 62 International Review of Administrative Sciences, 459.

Donohue, Laura, 'ANTI-TERRORIST FINANCE IN THE UNITED KINGDOM AND UNITED STATES' (2006) 27 Mich. J. Int'l L., 303.

Dougan, Michael, 'The Treaty of Lisbon 2007: Winning Minds, not Hearts' (2008) 45 Common Market Law Review, 617.

Douglas-Scott, Sionaidh, 'The rule of law in the European Union - putting the security into the area of freedom, security and justice' (2004) 29 E.L. Rev., 219.

Dummer, Stephen, 'COMMENT: Secure Flight and Dataveillance, A New Type of Civil Liberties Erosion: Stripping Your Rights When You Don't Even Know It' (2006) 75 Miss. L.J., 583.

Dumortier, Jos, 'The Protection of Personal Data in the Schengen Convention' (1997) 11 International Review of Law, Computers & Technology, 93.

Eckes, Christina, *EU counter-terrorist policies and fundamental rights: the case of individual sanctions* (Oxford University Press 2009).

Edwards, Lilian, 'Taking the 'Personal' Out of Personal Data: Durant v FSA and its Impact on the Legal Regulation of CCTV' (2004) 1 SCRIPT-ed, 341.

Eger, John, 'Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non- Tariff Barriers?' (1978) 10 Law and Policy in International Business, 1065.

Electronic Privacy Information Center, 'Spotlight on Surveillance: Secure Flight Should Remain Grounded Until Security and Privacy Problems Are Resolved', August 2007.

Etzioni, Amitai, *The limits of privacy* (Basic Books 1999).

EU Network of Independent Experts on Fundamental Rights, 'Commentary of the EU Charter of Fundamental Rights', 2006.

——, 'Ethnic Profiling', December 2006.

EUROPEAN DATA PROTECTION AUTHORITIES, 'OPINION ON THE TRANSFER OF PASSENGERS' DATA TO THE UNITED STATES', no date.

European Data Protection Supervisor, 'Comments on the Communication of the Commission on interoperability of European databases', March 10, 2006.

——, 'PNR: EDPS first reaction to the Court of Justice judgment', May 30, 2006.

——, 'Opinion on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection', November 11, 2008.

——, ‘Opinion 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)’, June 22, 2010.

——, ‘Opinion on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)’, May 31, 2011.

——, ‘Opinion on the 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)’, no date.

——, ‘Opinion on the role of the European Central Bank in the SWIFT case’, no date.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, ‘REPORT 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 (2006/2193(INI))’, July 19, 2006.

Ewing, Mike, ‘The Perfect Storm: The Safe Harbor and the Directive on Data Protection’ (2002) 24 Hous. J. Int’l L., 315.

Exten, Sarah Elisabeth, ‘Major Developments in Financial Privacy Law 2006: The SWIFT Database Incident, and Updates to the Gramm-Leach-Bliley and Fair Credit Reporting Acts’ (2008) 3 ISJLP, 649.

Farrell, Henry, ‘Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement’ (2003) 57 International Organization, 277.

Faure Atger, Anaïs, ‘The Abolition of Internal Border Checks in an Enlarged Schengen Area: Freedom of movement or a scattered web of security checks?’, March 2008.

Fenwick, Helen, ‘Proactive counter-terrorist strategies in conflict with human rights’ (2008) 22 International Review of Law, Computers & Technology, 259.

Flaherty, David H., ‘On the Utility of Constitutional Rights to Privacy and Data Protection’ [1990] Case Western Reserve Law Review, 831.

Foucault, Michel, *Discipline and punish : the birth of the prison* (2. Vintage Books ed. Vintage Books 1995).

Fried, Charles, ‘Privacy’ (1968) 77 Yale L.J., 475.

——, *An anatomy of values problems of personal and social choice.* (Harvard University Press 1970).

Froomkin, Michael, ‘The Death of Privacy?’ (2000) 52 Stanford Law Review, 1461.

Fundamental Rights Agency, ‘Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes’, October 28, 2008.

——, ‘Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide’, 2010.

Fuster, Gloria González, Paul De Hert, and Serge Gutwirth, ‘The Law-Security Nexus in Europe: State-of the-art report’, no date.

Garside, Alice, ‘The political genesis and legal impact of proposals for the SIS II: what cost for data protection and security in the EU?’, March 2006.

Gavison, Ruth, ‘Privacy and the Limits of Law’ (1979) 89 Yale L.J., 421.

Gellman, Barton, Paul Blustein, and Dafna Linzer, ‘Bank Records Secretly Tapped’, June 23, 2006.

Geyer, Florian, ‘Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice’, May 2008.

Gladstone, Julia, 'The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy' (2000) 7 Willamette J. Int'l L. & Dis. Res., 10.

Godkin, El, 'The Rights of the Citizen-IV-To His Own Reputation', 1890, 58.

Goemans, Caroline, and Jos Dumortier, 'ENFORCEMENT ISSUES - Mandatory retention of traffic data in the EU: possible impact on privacy and on-line anonymity' in *Digital Anonymity and the Law* (T.M.C. Asser Press no date), 161.

Gómez-Arostegui, Tomás, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2005) 35 Cal. W. Int'l L. J., 153.

González Fuster, Gloria, Paul De Hert, Erika Ellyne, and Serge Gutwirth, 'Huber, Marper and Others: Throwing New Light on the Shadows of Suspicion', June 2010.

Guild, Elspeth, 'International Terrorism and EU Immigration, Asylum and Borders Policy: The Unexpected Victims of 11 September 2001' (2003) 8 European Foreign Affairs Review, 331.

——, 'Inquiry into the EU-US Passenger Name Record Agreement' (CEPS March 2007).

Guild, Elspeth, and Anneliese Baldaccini, eds., *Terrorism and the foreigner : a decade of tension around the rule of law in Europe* (Martinus Nijhoff 2007).

Guild, Elspeth, and Evelien Brouwer, 'The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US' (CEPS July 2006).

Guild, Elspeth, and Sergio Carrera, 'The European Union's Area of Freedom, Security and Justice ten years on' in Elspeth Guild and others (eds), *THE AREA OF FREEDOM, SECURITY AND JUSTICE TEN YEARS ON SUCCESSES AND FUTURE CHALLENGES UNDER THE STOCKHOLM PROGRAMME*, 2010, 1.

Gutwirth, Serge, *Privacy and the information age* (Rowman & Littlefield Publishers 2002).

Gutwirth, Serge, and Mireille Hilderbrandt, 'Some Caveats on Profiling' in Serge Gutwirth and others (eds), *Data protection in a profiled world* (Springer 2010), 31.

Gutwirth, Serge, Yves Poullet, Paul De Hert, and Ronald Leenes, eds., 'The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)' in *Computers, privacy and data protection : an element of choice* (Springer 2011), 3.

Hahn, Robert, 'The Economics of Airline Safety and Security: An Analysis of the White House Commission's Recommendations' (1997) 20 Harv. J. L. & Pub. Pol'y, 791.

Harris, Edward, 'Tradeoffs in Personal Data Privacy: A Swedish Church Lady, Austrian Public Radio Employees and Transatlantic Air Carriers Show that Europe Does Not Have the Answers' (2007) 22 American University International Law Review, 745.

Hasbrouck, Edward, 'What's in a Passenger Name Record?', no date.

Hearing before the Committee on Finance US Senate, 'Financial War on Terrorism: New Money Trails Present Fresh Challenges', October 9, 2002.

Heisenberg, Dorothee, *Negotiating privacy : the European Union, the United States, and personal data protection* (Lynne Rienner Publishers 2005).

Hert, Paul De, 'The Case of Anonymity in Western Political Philosophy- Benjamin Constant's Refutation of Republican and Utilitarian Arguments Against Anonymity' in C Nicoll and others (eds), *Digital anonymity and the law: tensions and dimensions* (T.M.C. Asser Press 2003), 47.

——, 'Biometrics: legal issues and implications', January 2005.

Hert, Paul De, and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Claes and others (eds), *Privacy and the criminal law* (Intersentia 2006), 61.

——, 'Interoperability of police databases within the EU: An accountable political choice?' (2006) 20 International Review of Law, Computers & Technology, 21.

——, ‘Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action’ in *Reinventing data protection?* (Springer 2009), 3.

Hert, Paul De, and Vagelis Papakonstantinou, ‘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’ (2009) 25 Computer Law & Security Report, 403.

Hert, Paul De, Wim Schreurs, and Evelien Brouwer, ‘Machine-readable identity documents with biometric data in the EU- Overview of the legal framework’ (2006) 21 Keesing Journal of Documents & Identity, 3.

Hert, Paul De, and Bart de Schutter, ‘International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift’ in Bernd Martenczuk and Servaas Van Thiel (eds), *Justice, liberty, security : new challenges for EU external relations* (VUBPRESS 2008), 303.

Hijmans, Hielke, ‘The European Data Protection Supervisor: The Institutions of the EC controlled by an independent Authority’ (2006) 43 Common Market Law Review, 1313.

Hijmans, Hielke, and Alfonso Scirocco, ‘Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?’ (2009) 46 Common Market Law Review, 1485.

Hixson, Richard, *Privacy in a public society: human rights in conflict* (Oxford University Press 1987).

Hobbing, Peter, ‘An assessment of the proposals of regulation and decision which define the purpose, functionality and responsibilities of the future SIS II’, February 15, 2006.

Hobby, Seth, ‘The EU Data Protection Directive: Implementing a Worldwide Data Protection Regime and How the U.S. Position Has Progressed’ (2005) 1 Int’l L. & Mgmt. Rev., 155.

Hondius, Frits, *Emerging data protection in Europe* (North-Holland Pub. Co. ;American Elsevier Pub. Co. 1975).

——, 'A decade of international data protection' [1983] Netherlands International Law Review, 103.

Hondius, Frits W., 'Data Law in Europe' (1980) 16 Stan. J. Int'l L., 87.

Hoofnagle, Chris, 'Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement' (2004) 29 N.C.J. Int'l L. & Com. Reg., 595.

House of Lords European Union Committee, 'After Madrid: the EU's response to terrorism', no date.

——, 'Schengen Information System II (SIS II)', no date.

——, 'Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamm', no date.

——, 'The EU/US Passenger Name Record (PNR) Agreement', no date.

——, 'The Passenger Name Record (PNR) Framework Decision', no date.

House of Lords, Select Committee on the Constitution, 'Surveillance: Citizens and the State', no date.

Huie, Marsha Cope, Stephen Laribee, and Stephen Hogan, 'The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues' (2002) 9 Tulsa. J. Comp. & Int'l L., 391.

Hummer, Waldemar, 'Die SWIFT-Affaire US-Terrorismusbekämpfung versus Datenschutz' (2011) 49 Archiv des Völkerrechts, 203.

Hustinx, Peter, 'Data Protection in the EU' [2005] P& I, 62.

——, 'The moment of truth for the Data Retention Directive', December 3, 2010.

Inness, Julie, *Privacy, intimacy and isolation* (Oxford University Press 1996).

Joint Research Centre- Institute for Prospective Technological Studies (DG JRC), 'Biometrics at the Frontiers: Assessing the Impact on Society - For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE)', no date.

Jonas, Jeff, and Jim Harper, 'Effective Counterterrorism and the Limited Role of Predictive Data Mining', 2006.

Justice, *The Schengen information system : a human rights audit* (JUSTICE 2000).

Kaifa-Gbanti, Maria, 'Surveillance Models in the Security State & Fair Criminal Trial (in Greek)' [2010] Nomiki Vivliothiki, 43.

Kalven, Harry, 'Privacy in Tort Law- Were Warren and Brandeis Wrong?' (1966) 31 L. & Contemp. Probs., 326.

Karanja, Stephen, *Transparency and proportionality in the Schengen information system and border control co-operation* (Martinus Nijhoff Publishers 2008).

Keohane, Daniel, 'The EU and counter-terrorism', May 2005.

——, 'Implementing the EU's Counter-Terrorism Strategy. Intelligence, Emergencies, and Foreign Policy' in Dieter Mahncke and Jörg Monar (eds), *International terrorism : a European response to a global threat?* (P.I.E.-Peter Lang 2006), 63.

Kerchove, Gilles de, and Serge de Biolley, 'The EU Counter-Terrorism Coordinator' in Jörg Monar (ed), *The institutional dimension of the European Union's area of freedom, security and justice* (P.I.E. Peter Lang 2010), 233.

Kett-Straub, Gabriele, 'Data Screening of Muslim Sleepers Unconstitutional' (2006) 7 German Law Journal, 967.

Kierkegaard Mercado, Sylvia, 'Safe Harbor Agreement - Boon or Bane' (2004) 1 Shidler J. L. Com. & Tech., 1.

Kilkelly, Ursula, 'The right to respect for private and family life - A guide to the implementation of Article 8 of the European Convention on Human Rights', 2001.

Kite, Leigh A., 'Red Flagging Civil Liberties and Due Process Rights of Airline Passengers: Will a Redesigned CAPPS II System Meet the Constitutional Challenge?' (2004) 61 Wash. & Lee L. Rev., 1385.

Kleiner, Yevgenia, 'Racial Profiling in the Name of National Security: Protecting Minority Travelers' Civil Liberties in the Age of Terrorism' (2010) 30 B.C. Third World L.J., 103.

Koops, Bert-Jaap, 'Law, Technology, and Shifting Power Relations' (2010) 25 Berkeley Tech. L.J., 973.

Kosta, Eleni, and Peggy Valcke, 'Retaining the data retention directive' (2006) 22 Computer Law & Security Report, 370.

Kuijper, Pieter Jan, 'Some Legal Problems Associated with the Communitarization of Policy on Visas, Asylum and Immigration under the Amsterdam Treaty and Incorporation of the Schengen Acquis' (2000) 37 Common Market Law Review, 345.

Kuner, Christopher, 'Beyond Safe Harbor: European Data Protection Law and Electronic Commerce' (2001) 35 Int'l L., 79.

——, 'An international legal framework for data protection: Issues and prospects' (2009) 25 Computer Law & Security Review, 307.

Leathers, Daniel, 'Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement' (2009) 41 Case W. Res. J. Int'l L., 193.

Leon, Pablo Mendes De, 'The Fight Against Terrorism Through Aviation : Data Protection Versus Data Production' (2006) XXXI Air & Space Law, 320.

Lessig, Lawrence, 'Privacy As Property' (2002) 69 Social Research: An International Quarterly, 247.

Liberatore, Angela, 'Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union' (2007) 13 European Journal on Criminal Policy and Research, 109.

Lichtblau, Eric, and James Risen, 'Bank Data Is Sifted by U.S. in Secret to Block Terror', June 23, 2006.

Lodge, Juliet, 'EJustice, Security and Biometrics: The EU's Proximity Paradox' (2005) 13 European Journal of Crime, Criminal Law and Criminal Justice, 533.

Lowy, Joan, 'Jet fuel-tank protection ordered U.S. cites 1996 explosion of 747', July 16, 2008.

Lugna, Lauri, 'Institutional Framework of the European Union Counter-Terrorism Policy Setting' (2006) 8 Baltic Security & Defence Review, 101.

Lyon, David, *Surveillance after September 11* (Polity Press in association with Blackwell Pub. Inc. 2003).

Martin, D., 'Comments on Förster (Case C-158/07 of 18 November 2008), Metock (Case C-127/08 of 25 July 2008) and Huber (Case C-524/06 of 16 December 2008)' (2009) 11 European Journal of Migration and Law, 95.

McCarthy, J, *The rights of publicity and privacy* (C. Boardman, 1987).

Mendez, Fernando, and Mario Mendez, 'Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States' (2009) 40 Publius: The Journal of Federalism, 617.

Mendez, Mario, 'Passenger Name Record Agreement – European Court of Justice' (2007) 3 European Constitutional Law Review (EuConst), 127.

Meyer, Josh, and Greg Miller, 'U.S. Secretly Tracks Global Bank Data', June 23, 2006.

Miller, Arthur, *The assault on privacy: Computers, data banks, and dossiers* (New American Library 1972).

Mitsilegas, Valsamis, 'Contrôle des étrangers, des passagers, des citoyens : surveillance et anti-terrorisme' (2005) 58 Cultures et Conflits, 155.

——, ‘Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance’ in Elspeth Guild and others (eds), *Whose Freedom Security and Justice? EU Immigration and Asylum Law and Policy* (Hart 2007), 359.

——, *EU criminal law* (Hart Pub. 2009).

Mitsilegas, Valsamis, and Anneliese Baldaccini, ‘Interdependence of the Various Initiatives and Legislative Proposals in the Fields of Counter-Terrorism and Police Co-operation at the European Level’, October 2007.

Mitsilegas, Valsamis, Jörg Monar, and Wyn Rees, *The European Union and internal security : guardian of the people?* (Palgrave Macmillan 2003).

Moeckli, Daniel, ‘Discriminatory profiles: law enforcement after 9/11 and 7/7’ (2005) 5 European Human Rights Law Review, 517.

——, ‘Terrorist Profiling and the Importance of a Proactive Approach to Human Rights Protection’ [2006] .

Monar, Jörg, ‘The Dynamics of Justice and Home Affairs: Laboratories, Driving Factors and Costs’ (2001) 39 Journal of Common Market Studies, 747.

——, ‘International Terrorism- A ‘European Response’ to a Global Threat?’ in Dieter Mahncke and Jörg Monar (eds), *International terrorism : a European response to a global threat?* (P.I.E.-Peter Lang 2006), 151.

——, ‘Common Threat and Common Response? The European Union’s Counter-Terrorism Strategy and its Problems’ (2007) 42 Government and Opposition, 292.

——, ‘The Institutional Framework of the AFSJ Specific Challenges and Dynamics of Change’ in Jörg Monar (ed), *The institutional dimension of the European Union’s area of freedom, security and justice* (P.I.E. Peter Lang 2010), 21.

——, ‘Editorial Comment: The Rejection of the EU-US TFTP Interim Agreement by the European Parliament: A Historic Vote and its Implications’ (2010) 15 European Foreign Affairs Review, 143.

Moore, Adam, *Privacy rights : moral and legal foundations* (Pennsylvania State University Press 2010).

Müller, Felix, and Tobias Richter, 'Report on the Bundesverfassungsgericht's (Federal Constitutional Court) Jurisprudence in 2005/2006' (2008) 9 German Law Journal, 161.

Murphy, Cian, 'Fundamental Rights and Security: The Difficult Position of the European Judiciary' (2010) 16 European Public Law, 289.

——, 'Romanian Constitutional Court, Decision No. 1258 of 8 October 2009 regarding the unconstitutionality exception of the provisions of Law No. 298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers, as well as for the modification of Law No. 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area' (2010) 47 Common Market Law Review, 933.

Murphy, Richard S., 'Property Rights in Personal Information: An Economic Defense of Privacy' (1996) 84 Geo. L.J., 2381.

NATIONAL TRANSPORTATION SAFETY BOARD, 'AIRCRAFT ACCIDENT REPORT In-flight Breakup Over the Atlantic Ocean Trans World Airlines Flight 800 Boeing 747-131, N93119 Near East Moriches, New York July 17, 1996', 200AD.

Neuhold, Hanspeter, 'International Terrorism. Definitions, Challenges and Responses' in Dieter Mahncke and Jörg Monar (eds), *International terrorism : a European response to a global threat?* (P.I.E.-Peter Lang 2006), 23.

Newman, Abraham, *Protectors of privacy : regulating personal data in the global economy* (Cornell University Press 2008).

——, 'Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive' (2008) 62 International Organization, 103.

Nijhawan, David Raj, 'The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States' (2003) 56 Vand. L. Rev., 939.

Nilsson, Hans G., 'The EU Action Plan on Combating Terrorism. Assessment and Perspectives' in Dieter Mahncke and Jörg Monar (eds), *International terrorism : a European response to a global threat?* (P.I.E.-Peter Lang 2006), 73.

Nissenbaum, Helen, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy, 559.

Nouwt, Sjaak, 'Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union' in *Reinventing data protection?*, no date, 275.

Ntouvas, I., 'Air Passenger Data Transfer to the USA: the Decision of the ECJ and latest developments' (2007) 16 International Journal of Law and Information Technology, 73.

Nugter, A, *Transborder flow of personal data within the EC: a comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom, and the Netherlands and their impact on the private sector* (Kluwer Law and Taxation Publishers 1990).

Ojanen, Tuomas, 'Terrorist profiling: human rights concerns' (2010) 3 Critical Studies on Terrorism, 295.

Open Society, Justice Initiative, 'Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory', no date.

Ozcan, Mehmet, and Fatma Yilmaz, 'Pendulum Swings in between Civil Rights and Security: EU Policies against Terrorism in the Light of the PNR Case' (2008) 1 USAK Y.B. Int'l Pol. & L., 51.

Papakonstantinou, Vagelis, and Paul de Hert, 'The PNR Agreement and Transatlantic Anti-Terrorism Co-operation: No Firm Human Rights Framework on either Side of the Atlantic' (2009) 46 Common Market Law Review, 885.

Parker, Richard B., 'A Definition of Privacy' (1974) 27 Rutgers L. Rev., 275.

Parkin, Joanna, 'The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law', April 2011.

——, 'The Schengen Information System and the EU Rule of Law', June 2011.

Patton, Christopher, 'No Man's Land: The EU-U.S. Passenger Name Record Agreement and What It Means for the European Union's Pillar Structure' (2008) 40 Geo. Wash. Int'l L. Rev., 527.

Pawlak, Patryk, 'Made in the USA ? The Influence of the US on the EU 's Data Protection Regime', November 2009.

Pearce, Graham, and Nicholas Platten, 'Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective' (1999) 22 Fordham Int'l L.J., 2024.

Peers, Steve, 'Key Legislative Developments on Migration in the European Union: SIS II' (2008) 10 European Journal of Migration and Law, 77.

——, 'Finally 'Fit for Purpose'? The Treaty of Lisbon and the End of the Third Pillar Legal Order' (2008) 27 Yearbook of European Law, 47.

——, 'The 'Third Pillar acquis' after the Treaty of Lisbon enters into force', November 3, 2009.

——, *EU justice and home affairs law* (3rd ed. Oxford University Press 2011).

Polcak, Radim, 'Aims, methods and achievements in European data protection' (2009) 23 International Review of Law, Computers & Technology, 179.

Poli, Sara, and Maria Tzanou, 'The Kadi Rulings: A Survey of the Literature' (2009) 28 Yearbook of European Law, 533.

Posner, Richard, *Economic analysis of law* (5th ed. Aspen Law & Business 1998).

Posner, Richard A, 'Privacy and Related Interests' in *The economics of justice* (Harvard University Press 1983), 229.

Post, Robert C., 'Three Concepts of Privacy' (2000) 89 Georgetown Law Journal, 2087.

Poullet, Yves, 'The Directive 95/46/EC: Ten years after' (2006) 22 Computer Law & Security Report, 206.

——, 'Transborder Data Flows and Extraterritoriality: The European Position', March 26, 2007.

Prins, Corien, 'Making our body identify for us: Legal implications of biometric technologies' (1998) 14 Computer Law & Security Review, 149.

Privacy International, 'MEMORANDUM OF LAWS CONCERNING THE LEGALITY OF DATA RETENTION WITH REGARD TO THE RIGHTS GUARANTEED BY THE EUROPEAN CONVENTION ON HUMAN RIGHTS', October 10, 2003.

Raab, C. D., and C. J. Bennett, 'Taking the measure of privacy: can data protection be evaluated?' (1996) 62 International Review of Administrative Sciences, 535.

Ramasastry, Anita, 'Lost in Translation - Data Mining, National Security and the Adverse Inference Problem' (2006) 22 Santa Clara Computer & High Tech. L.J., 757.

Rasmussen, Richard, 'Is International Travel per se Suspicion of Terrorism? The Dispute between the United States and European Union over Passenger Name Record Data Transfers' (2009) 26 Wis. Int'l L.J., 551.

Rauhofer, Judith, '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' [2006] SCRIPT-ed, 322.

Ravich, Timothy, 'Is Airline Passenger Profiling Necessary?' (2007) 62 U. Miami L. Rev., 1.

Rees, Wyn, *Transatlantic counter-terrorism cooperation : the new imperative* (Routledge 2006).

Regan, Priscilla, *Legislating Privacy: Technology, Social Values, and Public Policy* (The University of North Carolina Press 1995).

Reidenberg, Joel, 'E-Commerce and Trans-Atlantic Privacy' (2002) 38 Hous. L. Rev., 717.

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

Rhee, Jamie, 'Comment, Rational And Constitutional Approaches To Airline Safety In The Face Of Terrorist Threats' (2000) 49 DEPAUL L. REV., 847.

Rijken, Conny, 'Re-Balancing Security and Justice: Protection of Fundamental Rights in Police and Judicial Cooperation in Criminal Matters' (2010) 47 Common Market Law Review, 1455.

Rijpma, Jorrit J., and Gráinne Gilmore, 'Joined Cases C-317/04 and C-318/04, European Parliament v. Council and Commission, Judgment of the Grand Chamber of 30 May 2006, [2006] ECR I-4721' (2007) 44 Common Market Law Review, 1081.

Rizer, Arthur, 'Dog Fight: Did the International Battle over Airline Passenger Name Records Enable the Christmas-Day Bomber' (2010) 60 Cath. U. L. Rev., 77.

Rodotà, Stefano, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing data protection?* (Springer 2009).

Rodriguez- Ruiz, Blanca, 'Protecting the secrecy of telecommunications : a comparative study of the European Convention on Human Rights, Germany and United States' (European University Institute 1995).

Roos, Megan, 'Definition of the Problem: The Impossibility of Compliance with Both European Union and United States Law' (2005) 14 Transnat'l L. & Contemp. Probs., 1137.

Rosen, Jeffrey, *The unwanted gaze : the destruction of privacy in America* (1st Vintage Books ed. Vintage Books 2001).

——, 'Continental Divide: Americans see privacy as a protection of liberty, Europeans as a protection of dignity. Will one conception trump the other—or are both destined to perish?' [2004] Legal Affairs.

Rouvroy, Antoinette, and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing data protection?* (Springer 2009).

Rowland, Diane, 'Data Retention and the War Against Terrorism – A Considered and Proportionate Response?' (2004) 3 The Journal of Information, Law and Technology (JILT).

Salbu, Steven, 'The European Union Data Privacy Directive and International Relations' (2002) 35 Vand. J. Transnat'l L., 655.

Santolli, Justin, 'Note: The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive' (2008) 40 The Geo. Wash. Int'l L. Rev., 553.

Sartor, Giovanni, 'Privacy, Reputation, and Trust: Some Implications for Data Protection' (European University Institute no date).

Scandamis, Nicolas, Frantzis Sigalas, and Sofoklis Stratakis, 'Rival Freedoms in terms of Security: The Case of Data Protection and the Criterion of Connexity' (CEPS, CHALLENGE December 2007).

Scannell, Bill, 'TSA cannot be trusted', September 27, 2004.

Scheinin, Martin, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', January 29, 2007.

Scheinin, Martin, and Mathias Vermeulen, 'DETECTER, Detection Technologies, Terrorism, Ethics and Human Rights', no date.

Schengen Joint Supervisory Authority, 'Activity Report – December 2005 – December 2008', no date.

——, 'Opinion on the Proposed Legal Basis for SIS II', no date.

——, 'Report Jan 2002 – Dec 2003', no date.

Schneier, Bruce, 'An easy path for terrorists', August 24, 2004.

Schriver, Robert, 'You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission' (2002) 70 Fordham L. Rev., 2777.

Schutter, Olivier De, and Julie Ringelheim, 'Ethnic Profiling: A Rising Challenge for European Human Rights Law' (2008) 71 Modern Law Review, 358.

Schutze, Robert, 'Three 'Bills of Rights' for the European Union' (2011) 30 Yearbook of European Law, 131.

Schwartz, Paul, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1995) 80 Iowa L. Rev., 553.

Seifert, Jeffrey, 'Data Mining and Homeland Security: An Overview', 2007.

Serrano, Vanessa, 'Comment: The European Court of Justice's Decision to Annul the Agreement between the United States and European Community regarding the Transfer of Personal Name Record Data, Its Effects, and Recommendations for a New Solution' (2007) 13 ILSA J. Int'l & Comp. L., 453.

Shaffer, Gregory C., 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards' (2000) 25 Yale Journal of International Law, 1.

——, 'Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance through Mutual Recognition and Safe Harbor Agreements' (2002) 9 Colum. J. Eur. L., 29.

Shea, Courtney, 'A NEED FOR SWIFT CHANGE: THE STRUGGLE 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' (2008) 8 J. HIGH TECH. L., 143.

Shetterly, Daryl, 'Starving the Terrorists of Funding: How the United States Treasury Is Fighting the War on Terror' (2006) 18 Regent U. L. Rev., 327.

Shoenberger, Allen, 'Privacy Wars: EU Versus US: Scattered Skirmishes, Storm Clouds Ahead' (2007) 17 Ind. Int'l & Comp. L. Rev., 375.

Shrader, Jeremy, 'Secrets Hurt: How SWIFT Shook Up Congress, the European Union, and the U.S. Banking Industry' (2007) 11 North Carolina Banking Institute, 397.

Siemen, Birte, *Datenschutz als europäisches Grundrecht* (Duncker & Humblot 2006).

Simitis, Spiros, 'Datenschutzrecht' in Hans Meyer and Michael Stolleis (eds), *Hessisches Staats- und Verwaltungsrecht : (HessStVwR)* (2. Aufl. Metzner 1986), 111.

——, 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania Law Review, 707.

——, 'New developments in National and International Data Protection Law' in J Dumortier (ed), *Recent developments in data privacy law : Belgium's Data Protection Bill & the European Draft Directive* (Leuven University Press 1992), 1.

——, 'SYMPOSIUM: DATA PROTECTION LAW AND THE EUROPEAN UNION'S DIRECTIVE: THE CHALLENGE FOR THE UNITED STATES: From the Market To the Polis: The EU Directive on the Protection of Personal Data' (1995) 80 Iowa L. Rev., 445.

——, 'Privacy– An Endless Debate?' (2010) 98 California Law Review, 1989.

Simpson, Glenn, 'Treasury Tracks Financial Data In Secret Program', 23 2006.

Slobogin, Christopher, *Privacy at risk : the new government surveillance and the Fourth Amendment* (University of Chicago Press 2007).

Slobogin, Christopher, and Joseph E. Schumacher, 'Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society' (1993) 42 Duke L.J., 727.

Solove, Daniel, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 Stan. L. Rev., 1393.

——, 'The Origins and Growth of Information Privacy Law' (2003) 748 PLI/PAT, 29.

——, 'A Taxonomy of Privacy' (2006) 154 U. Pa. L. Rev., 477.

——, 'A Brief History of Information Privacy Law' [2006] PROSKAUER ON PRIVACY, GWU Law School Public Law Research Paper No. 215, 1.

——, *Understanding privacy* (Harvard University Press 2008).

——, 'Data Mining and the Security-Liberty Debate' (2008) 74 University of Chicago Law Review, 343.

Solove, Daniel J., 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy' (2002) 75 Southern California Law Review, 1083.

Solove, Daniel, and Paul Schwartz, *Information privacy law* (3rd ed. Wolters Kluwer Law & Business ;;Aspen Publishers 2009).

Soma, John, Stephen Rynerson, and Britney Beall-Eder, 'An Analysis of the Use of Bilateral Agreements between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor' (2004) 39 Tex. Int'l L.J., 171.

Stein, Torsten, 'European and German Security Policy, Especially Border Controls, with Regard to International Terrorism' (2005) 35 Israel Yearbook on Human Rights, 231.

Steinbock, Daniel J., 'Data Matching, Data Mining, and Due Process' (2005) 40 Georgia Law Review, 82.

Sun, Chuan, 'The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective' (2003) 2 Nw. J. Tech. & Intell. Prop., 99.

Sunosky, James, 'Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles' (2000) 9 Currents: Int'l Trade L.J., 80.

Surveillance Studies Network, 'A Report on the Surveillance Society', September 2006.

Sykes, Charles, *The end of privacy* (1st St. Martin's Griffin ed. St. Martin's Griffin 2000).

Taipale, K. A., 'Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data' (2003) 5 COLUM. SCI. & TECH. L. REV., 1.

Tallman, David, 'Financial Institutions and the Safe Harbor Agreement: Securing Cross-Border Financial Data Flows' (2003) 34 Law & Pol'y Int'l Bus., 747.

Taylor, Mark, 'The EU Data Retention Directive' (2006) 22 Computer Law & Security Review, 309.

Technology and Privacy Advisory Committee, US Department of Defense, 'Safeguarding Privacy in the fight against terrorism', March 2004.

Terwangne, Cécile de, 'Is a Global Data Protection Regulatory Model Possible?' in *Reinventing data protection?*, no date, 175.

Thai, Joseph, 'Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?' (2006) 74 Fordham L. Rev., 1731.

Thym, Daniel, 'The Schengen Law: A Challenge for Legal Accountability in the European Union' (2002) 8 European Law Journal, 218.

Tromp, 'Schengen's Final Days? The Incorporation of Schengen into the New EU, External Borders and Information Systems' in Monica den Boer (ed), *Schengen, judicial cooperation and policy coordination*, 1997.

Trubow, George, and Dennis Hudson, 'The Right to Financial Privacy Act of 1978: New Protection from Federal Intrusion' (1979) 12 J. Marshall J. Prac. & Proc., 487.

Tsiftsoglou, Anna, and Spyridon Flogaitis, 'Transposing the Data Retention Directive in Greece: Lessons from Karlsruhe', May 21, 2011.

Tukdi, Irfan, 'Transatlantic Turbulence: The Passenger Name Record Conflict' (2008) 45 Hous. L. Rev., 587.

Tzanou, Maria, 'Case-note on Joined Cases C-402/05 P & C-415/05 P Yassin Abdullah Kadi & Al Barakaat International Foundation v Council of the European Union & Commission of the European Communities' (2009) 10 German Law Journal, 121.

——, 'Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection' (2010) 6 Croatian Yearbook of European Law & Policy, 53.

——, 'The EU as an emerging 'Surveillance Society': The function creep case study and challenges to privacy and data protection' (2010) 4 Vienna Online Journal of International Constitutional Law, 407.

——, 'Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence' in Christina Akrivopoulou and Athanasios Psygkas (eds), *Personal data privacy and protection in a surveillance era : technologies and practices* (Information Science Reference 2011), 273.

——, 'The EU Data Protection Directive as a Model for Global Regimes' in Sabino Cassese and others (eds), *Global Administrative Law: Cases, Materials, Issues Third Edition*, no date.

Tzanou, Maria, and Sufyan Droubi, 'Case -note on Case T-318/01 Omar Mohammed Othman v Council of the European Union and Commission of the European Communities, judgment of the Court of First Instance of 11 June 2009 (Seventh Chamber)' (2010) 47 Common Market Law Review, 1233.

U.S. Department of Homeland Security, Privacy Office, 'A REPORT CONCERNING PASSENGER NAME RECORD INFORMATION DERIVED FROM FLIGHTS BETWEEN THE U.S. AND THE EUROPEAN UNION', December 18, 2008.

UK Information Commissioner, 'The Legal Framework: An analysis of the 'constitutional' European approach to issues of data protection law', no date.

United States General Accounting Office, 'Report to Congressional Committees, AVIATION SECURITY Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges', February 2004.

——, 'Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security, Committee on Governmental Affairs, U.S. Senate, Data Mining- Federal Efforts Cover a Wide Range of Uses', May 2004.

United States Government Accountability Office, 'Testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate, AVIATION SECURITY, Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program', February 9, 2006.

——, 'TERRORIST WATCH LIST SCREENING Efforts to Help Reduce Adverse Effects on the Public', September 2006.

United States National Commission for Terrorist Attacks, 'The Aviation Security System and the 9/11 Attacks' [no date] Staff Statement No. 3.

US Department of the Treasury, 'Terrorist Financing Tracking Program: Fact Sheet', no date.

Viola de Azevedo Cunha, Mario, Luisa Marin, and Giovanni Sartor, 'Peer-to-Peer Privacy Violations and ISP Liability: Privacy Violations in the User-Generated Web' [2011] International Data Privacy Law.

Vitale, Angela, 'The EU Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet' (2002) 35 Vand. J. Transnat'l L., 321.

Vries, Gijs de, 'European Strategy in the Fight Against Terrorism and the Co-operation with the United States', May 13, 2004.

——, 'The European Union's Role in the Fight Against Terrorism: [Opening Address - The Role of the EU in the Fight Against Terrorism]' (2005) 16 Irish Studies in International Affairs, 3.

Wagner, Eckart, 'The Integration of Schengen into the Framework of the European Union' (1998) 25 Legal Issues of European Integration, 1.

Walker, Clive, and Yaman Akdeniz, 'Anti-terrorism Laws and Data Retention: War Is Over?' (2003) 54 Northern Ireland Legal Quarterly, 159.

Warren, Samuel D., and Louis D. Brandeis, 'Right to Privacy' (no date) 1890 Harv. L. Rev., 193.

Westin, Alan, *Privacy and freedom* (Bodley Head 1970).

White House Commission on White House Commission on Aviation Safety and Security Aviation Safety and Security, 'Final Report to President Clinton', 1997.

Whitman, James Q, 'Two Western Cultures of Privacy: Dignity versus Liberty' (2003) 113 Yale Law Journal, 1151.

Witte, Bruno de, 'Too much constitutional law in the European Union's Foreign Relations?' in Marise Cremona and Bruno de Witte (eds), *EU foreign relations law : constitutional fundamentals* (Hart 2008), 3.

Working Party on Information Security and Privacy, 'The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines', April 30, 2011.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Working Document, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive', July 24, 1998.

Yano, Marjorie J., 'Come Fly the (Unfriendly) Skies: Negotiating Passenger Name Record Agreements between the United States and European Union' (2008) 5 ISJLP, 479.

Zaidi, Kamaal, 'Harmonizing U.S.-EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data' (2003) 12 Mich. St. J. Int'l L., 169.

Zimmermann, Doron, 'The European Union and Post-9/11 Counterterrorism: A Reappraisal' (2006) 29 Studies in Conflict & Terrorism, 123.

Zöller, Verena, 'Liberty Dies by Inches: German Counter-Terrorism Measures and Human Rights' (2004) 5 German Law Journal, 469.

'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 Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) 8-9 February 2010', April 7, 2010.