


Policy Department C
Citizens' Rights and Constitutional Affairs



**DATA PROTECTION FROM A TRANSATLANTIC
PERSPECTIVE: THE EU AND US MOVE TOWARDS AN
INTERNATIONAL DATA PROTECTION AGREEMENT?**

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

OCTOBER 2008
PE 408.320

EN



PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT EΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU EURÓPSKY PARLAMENT
EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPARLAMENTET

**Directorate-General Internal Policies
Policy Department C
Citizens' Rights and Constitutional Affairs**

DATA PROTECTION

FROM A TRANSATLANTIC PERSPECTIVE:

THE EU AND US MOVE TOWARDS AN

INTERNATIONAL DATA PROTECTION AGREEMENT?

STUDY

Abstract:

Recent years have been marked by a growing demand of personal data for public security purposes. Access and protection of those data are climbing the transatlantic political agenda. They have raised tensions and fostered forms of cooperation. The possible conclusion of an international binding agreement on a common transatlantic framework on data protection would be a further and crucial step ahead. The scope of this study is to pave the way for launching a parliamentary debate on those issues. Therefore, it aims at providing a comparative analysis of the EU and US legislation concerning the protection of personal data collected for public security purposes. It also discusses some of the main challenges posed by new technologies as well as analyses the most relevant cases-studies of transatlantic data exchange. Finally, it takes into consideration the published outcomes of the work of the High Level Contact Group.

PE 408.320

This study was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (**LIBE**).

This paper is published in the following languages: EN, FR.

Authors: **Paul De Hert & Rocco Bellanova for CEPS, Brussels.**

Manuscript completed in **September 2008**

Copies can be obtained through:

Mr Alessandro DAVOLI
Administrator Policy Department C
Tel: 32 2 2832207
Fax: 32 2 2832365
E-mail: alessandro.davoli@europarl.europa.eu

Informations on **DG IPOL publications**:

<http://www.europarl.europa.eu/activities/committees/studies.do?language=EN>

<http://www.ipolnet.ep.parl.union.eu/ipolnet/cms/pid/438>

Brussels, European Parliament

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

TABLE OF CONTENT

INTRODUCTION.....	5
PART ONE – PRINCIPLES OF DATA PROTECTION IN THE EU AND US	
1. Legislation and main principles in the EU covering Third Pillar activities:	
Between a piecemeal approach and a common framework for data protection..	7
1.1. <i>A brief background overview.....</i>	7
1.2. <i>Convention No. 108: Principles and transborder data flows</i>	8
1.3. <i>The current status: A patchwork of ad hoc measures.....</i>	9
1.4. <i>The future Framework Decision on Data Protection under the Third Pillar</i>	9
1.5. <i>The main provisions of the DPFD proposal.....</i>	10
1.6. <i>The European Parliament position on six critical issues.....</i>	11
2. Legislation and main principles in the US: A multilayered scheme	13
2.1. <i>Privacy and data protection in US Constitutional law</i>	13
2.2. <i>US data protection legislation: A short history.....</i>	15
2.3. <i>The Privacy Act of 1974.....</i>	16
2.4. <i>Three main flaws of the Privacy Act from a transatlantic perspective..</i>	17
2.5. <i>Brief overview of other statutory laws.....</i>	18
2.6. <i>Overview of the main US supervisor authorities</i>	19
2.7. <i>Two critical assessments: Privacy agencies and legal redress.....</i>	20
PART TWO – NEW TECHNOLOGIES AND CASE-STUDIES	
1. Data mining: A technology of analysis and the related issues of profiling and risk assessment	22
1.1. <i>What is data mining?</i>	22
1.2. <i>Overview of US data mining programmes in the security field.....</i>	23
1.3. <i>Three concerns raised by data mining</i>	25
1.4. <i>European and US responses to data mining.....</i>	26
2. The growing request of data: Biometrics.....	27
3. The growing request of data: Electronic System of Travel Authorization.....	27
3.1. <i>The introduction of Electronic System for Travel Authorization</i>	27
3.2. <i>Three potential concerns raised by ESTA.....</i>	29
3.3. <i>The proposed EU Electronic System of Travel Authorization</i>	30
4. The growing request of data: Travel data	31
4.1. <i>Overview of the three EU-US agreements and of the ECJ judgment....</i>	31
4.2. <i>Main features of the 2007 PNR agreement.....</i>	33
4.3. <i>The EU PNR Framework Decision: Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes ..</i>	35

4.4. <i>Content of the EU PNR proposal</i>	35
4.5. <i>Two considerations on the proposed EU-PNR system</i>	37
5. The growing request of data: Banking data	38
5.1. <i>Access to banking data: SWIFT</i>	38
5.2. <i>Three considerations on PNR and SWIFT</i>	39
PART THREE – THE WORK OF THE HIGH LEVEL CONTACT GROUP ON DATA PROTECTION AND THE MOVE TOWARDS A TRANSATLANTIC DATA PROTECTION AGREEMENT	
1. The context and the goal of the works of the High Level Contact Group	41
2. The common principles	42
3. Five pending questions, High Level Contact Group policy options and previous position of the European Parliament	43
PART FOUR – FINAL CONSIDERATIONS	
1. EU and US: partners with common principles but different attitudes?	45
2. Lessons learned from case studies analysis	46
3. Which possible way forward?	47
REFERENCES	48

INTRODUCTION

Accessing data for security purposes is acquiring a growing importance both in the European Union and the United States. Several measures have been already proposed or set up before 9-11. Since then, they have been multiplied by both the development of new technological capacities and the political will of several institutional actors. Political pressure has been frequently exercised on easing the access and the sharing of data, with the set up of national, European and transatlantic agendas on the enhancement of police and internal security cooperation. Even if the US could appear as the leading actor in this field, the role of the EU cannot be disregarded, especially since the approval of The Hague Program in 2004. Moreover, the establishing of several measures in the US, such as the Passenger Name Record (PNR) system or the reform of the Visa Waiver Program, has directly involved EU and Member States. The introduction of security measures based on access to personal data raises concerns about privacy, data protection and other civil liberties. The debate on the balance, or correlation, between liberty and security has become a central issue, and has shaped all the negotiations at European and transatlantic level.

The European Parliament has always adopted a position of reconciliation between the two values of liberty and security, inviting Member States and EU institutions to develop efficient measures able to safeguard the higher standards of civil liberties and data protection. The transatlantic debate on these issues has not been trouble-free. Divergences between the two systems of privacy and data protection have been already discussed, and partially settled, after the adoption of the Data Protection Directive in 1995. Such transatlantic discussions generated divisions and legal conflicts within the EU, as in the case of the PNR agreement brought before the European Court of Justice. Finally, the unveiling of “secret” data mining activities in the US, and especially the SWIFT case that involved a EU cooperative society, has raised concerns on transparency and foreign surveillance. At present, it seems that EU and US are on the edge of a new, major step towards transatlantic cooperation. On June 2008, the EU-US summit Declaration expressed the common will to conclude an international agreement on data protection.

Given the present context, this study focuses on a comparison of data protection legislations and principles covering third pillar activities, therefore excluding a comparison of the frames of the legislation covering the private sector activities. The goal is to contribute to pave the way to parliamentary debate on the possible conclusion of a transatlantic agreement on data protection. The study is divided in three parts. The first is dedicated to a comparison of the two legal frameworks. Particular attention is dedicated to the last developments of the EU Framework Decision of Data Protection and to the US legal system. Part two analyses data mining, one of the main technologies introduced in support of security measures, illustrating some of most relevant programs proposed. This section also discusses the growing demand for access to personal data by law enforcement authorities, focusing on the main transatlantic challenges: among others the introduction of the Electronic System of Travel Authorization and the EU PNR system. Finally, the final report and the High Level Contact Group is presented and discussed in the third part.

In addition, the study presents a series of considerations and a set of recommendations aimed at providing advice in respect of possible future negotiations.

PART ONE – PRINCIPLES OF DATA PROTECTION IN THE EU AND US

The EU and US data protection regimes are generally perceived and discussed as completely divergent. Most of the scientific articles dealing with both systems express a judgement a value, aiming at underlining the positive assets of one of the two. Notwithstanding a wide scientific literature, the most part of comparative analysis focuses on protection of the private sector, probably fostered by the impact of the discussions that brought to Safe Harbour. Therefore, it seems important offer some insights on the data protection frames applicable to the so-called third pillar activities.

This part of the paper will, first of all, give a brief background overview of relevant privacy and data protection legislations and secondly analyse the relevant dispositions of the last tabled proposal for a Framework Decision on Data Protection under the Third Pillar.

1. Legislation and main principles in the EU covering Third Pillar activities: Between a piecemeal approach and a common framework for data protection

1.1. A brief background overview

The protection of individual privacy at the EU level is mainly governed by Article 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedom (ECHR) and Article 7 of the 2000 Charter of Fundamental Rights of the European Union. In addition, data protection in the EU is governed by 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 (the so-called Data Protection Directive), Directive 2002/58/EC on privacy and electronic communications (the so-called e-privacy Directive), by Article 8 of the Charter of Fundamental Rights of the European Union and by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the so-called Convention No. 108).

Notwithstanding such abundance of privacy and data protection legislation, when it comes to third pillar activities, the European legislation framework seems to become more complex and less coherent. In the context of a growing use of information technologies and tendency towards mutual access to private and public databases, the EU pillar structure is a major obstacle to the definition of a more effective framework. For instance, the main piece of EU legislation on data protection, the Data Protection Directive of 1995, does not apply to “the processing of personal data: in the course of an activity which falls outside the scope of Community law, such as those provided for by Title V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security [...] and the activities of the State in areas of criminal law” (Directive 95/46/EC, Art. 3(2)). Furthermore, as has been underlined by the Court of Justice in its PNR judgement, the Data Protection Directive does not apply to the processing of data firstly collected by private actors and later accessed for public security purposes.¹ This aspect is even more worrying, because it risks leaving the access of public authorities to commercial data in a sort of no man’s land (see *in extenso* De Hert, Papakonstantinou & Riehle, 2008)

¹ See European Court of Justice, Joined Cases C-317/04 and C-318/04, 30.05.2006.

One of the less regulated aspects of privacy and data protection in Europe is data exchange between law enforcement authorities, at both EU and international level. Nonetheless it does not cease to be the object of proposed and approved legislation. Several of these laws attempt to fix the lack of an appropriate framework by providing *ad hoc* data protection provisions in their texts. Thus, despite the fact that security-related processing within Europe lacks a common regulatory basis, specific sectors did go ahead alone: most notably the Schengen Agreement,² but also Europol³ and Eurojust⁴ Agreements, all include detailed data protection rules and procedures in their respective texts (using admittedly as basic principles and procedures those introduced in the Data Protection Directive). Therefore, what is actually in place at present within the EU in relation to Third Pillar processing is a series of sector-specific approaches that co-exists together with the 1981 Council of Europe Convention on data protection.⁵ This Convention, that only broadly regulates the field, will be discussed more in detail in the next paragraph.

1.2. Convention No. 108: Principles and transborder data flows

The core of the 1981 Convention *for the Protection of individuals concerning the automatic processing of personal data* of the Council of Europe, generally referred to as Convention 108, is a legally binding enumeration of data protection principles:

Article 5, on “Quality of data”, establishes the principles of fair and lawfully processing; purpose limitation; adequacy and minimization and data retention.

Article 6, “Special categories of data”, prohibits the processing of sensitive data such as “racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life”. Processing of those data, as well as data relating to criminal convictions, may be processed only if “domestic law provides appropriate safeguards”.

Article 7 defines the principle of “data security” and article 8 provides for “additional safeguards for the data subject”, such as the respect of the principles of openness; access to own data; rectification and remedy.

Article 9 delimits the possible legitimate exemptions to the previous provisions. For the scope of this study, it is important to recall art. 9(2):

“Derogation from the provisions of Article 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by law of the Party and constitutes a necessary measure in a democratic society in the interests of: (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences [...]”.

Convention 108 also defines the transborder data flows among the Parties by prohibiting, as a general rule, the recourse to protection of privacy argumentations to block transborder data flows. Further rules on transborder data flows are introduced

² Actually referring to Schengen I (Agreement 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, entered in 1985) and Schengen II or CIS (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, entered in 1990).

³ See The EUROPOL Convention (consolidated text) at <http://www.europol.europa.eu/index.asp?page=legal>

⁴ See Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA), OJ L 63/1

⁵ Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS no. 108, Strasbourg, 18 January 1981.

by the 2001 “Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows”.⁶ Article 2 introduces the concept of adequate level of protection as a condition for transborder flow of data towards a third country not part of the Convention 108.

The same Additional Protocol also recognizes the need for Member States to install a supervisory authority

1.3. The current status: a patchwork of ad hoc measures

Along with Convention 108, a complex of other instruments coexists in the sector of JHA. Among them, it is important to recall:

- national legislation rules and national oversight provided by independent data protection authorities;
- *ad hoc* data protection rules of a series of law enforcement initiatives, both at EU level, as the Prüm Council Decision, and at transatlantic level, the PNR agreements and SWIFT;
- *ad hoc* data protection rules of EU or European-wide agencies: Eurojust, and Europol; as well as data protection rules of transatlantic agreement among Europol and the US;⁷
- the European Convention for the Protection of Human Rights and Fundamental Freedom (ECHR), in particular article 8, and the relative European Court of Human Rights case law;
- the Charter of Fundamental Rights of the European Union, as soon as the Treaty of Lisbon will into force.

Convention 108 still represents the juridical base of data protection covering third pillar activities. Although its general principles are still valid, it is important to note that it has been drafted before the massive development of information technologies. If not integrated or substituted at EU-wide level by a new frame, it risks becoming outdated and overwhelmed by the growing application of technological instruments (De Hert, Papakonstantinou & Riehle, 2008). This fact explains, for instance, the elaborated data protection rules in the Europol Convention that complement Convention 108, and the recent EU initiative to draft a (new) general framework for data protection in the Third Pillar.

1.4. The future Framework Decision on Data Protection under the Third Pillar

The Commission proposed a draft Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters in October 2005. A long process of negotiations started. The following discussion is based on the last public version available.⁸

⁶ Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, Strasbourg, 8 November 2001.

⁷ See on this remarkable initiative to transfer personal data to the US on the basis of the Europol Convention, De Hert & De Shutter, 2008.

⁸ Council of the European Union, *Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, doc. 9260/08, Brussels, 24 June 2008. Hereinafter: DPDF or Framework Decision. The European Parliament (EP) is called to vote its last report on a previous draft version on its second plenary session in September 2008.

Almost three years have passed since the tabling of the initial Commission proposal. Several changes have been made to the initial text, due to difficulties encountered by Member States in finding a common ground as well as to critiques advanced by the EP and the European Data Protection Supervisor.⁹ When approved, this Framework Decision will become one of the main instruments of data protection covering Third Pillar activities.¹⁰

Art. 1(1) states the purpose of the DPF: “to ensure a high level of protection of the fundamental rights and freedom of natural persons, and including 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”. Art.1(2) defines the scope of the DPF. Personal data covered by this instrument are data that transmitted or made available among Member States, and to authorities and information systems established on the basis of Title VI of the TEU, or received or made available by the same. Furthermore, art.1(3) limits the scope 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”. Finally, article 1 leaves to Member States the possibility to provide higher safeguards for the protection of personal data collected or processed at national level.

1.5. The main provisions of the DPF proposal

The key definitions of the terms in the Framework Decision are listed in article 2. Among them it is worth to note, the fairly comprehensive definition of “filing system” including “structured set of personal data centralised, decentralised or dispersed on a functional or geographical basis” (art. 2(d)). The definition of “personal data” recalls the one established in the Data Protection Directive, including direct and indirect identification (art. 1(a)).

Articles 3-6, 8, 10 and 16-22 define and address the main principles of data protection. Article 3 translates the principles of lawfulness; proportionality and purpose. It also submits “further processing” to the respect of the same principles.

Article 4 provides for the principles of rectification, erasure and blocking.

Article 5 establishes time-limits for erasure and review.

Article 6 defines rules of processing of special categories of data (*below*).

Article 8 requires the competent authority to take “all reasonable steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available”. Therefore it enshrines the principle of data quality.

Article 10 provides for the obligation of logging and documentation, contributing to address the principle of transparency.

Articles 16 to 20 provide for data subjects’ rights: information; access; rectification erasure and blocking; compensation; judicial remedy.

Articles 21 and 22 ensure the principles of confidentiality and security of processing.

⁹ To the date, the EDPS submitted three different opinions on three different versions of the DPF: OJ C/2006/47/27; OJ C/2007/91/9 and OJ C/2007/139/1.

¹⁰ Even if the aim of this study is not to produce an in-depth analysis of this Framework Decision, it is important to offer an overview of the main content of the present draft. It will permit to underline the most relevant provisions for a comparison between the EU and US system and it will highlight possible issues within transatlantic dialogue. Such overview will be followed by a brief overview of the EP position on the draft DPF.

The role and powers of national supervisory authorities are described in art. 23 and 25. Article 25 prescribes that national supervisory authorities must have the powers to investigate, to intervene and the power to engage in legal proceedings.

This overview of the main principles seems to confirm that the Framework Decision reflects the same principle of the Convention No. 108. However, a closer analysis reveals some differences, as the one concerning sensitive data (*below*).¹¹ Of particular interest is article 14 on the transmission of personal data to private parties. The very existence this provision seems to confirm the idea of a growing interaction, and integration, of private and public databases in the management of security.

Of particular relevance for this study are the rules on the transfer of personal data to third countries (art. 13) and the relationship with agreements with third States (art. 26). Article 13 (1) defines the conditions of transmission, and in particular the need of prior consent of the Member State that originally transmitted or made available the data (art. 13(1)(c) and a sort of *ad hoc* adequacy finding (“the third State or international body concerned ensures an adequate level of protection for the intended data processing”, art. 13(1)(d)). However, such a strict framework of data protection is weakened by the following paragraphs. Article 13(2) permits a transfer without prior consent if this is essential for the prevention of an immediate and serious threat. Moreover, recital 24 further eases the prior consent leaving to each Member State the possibility to determine the modalities of such consent, including a general consent for categories of information or for specified third States. Article 13(3) states that it is possible to derogate from the adequacy criteria 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”.

Finally, article 26 on relationship to agreements with third States ensures that the Framework Decision is without prejudice to any obligations and commitments incumbent by virtue of bilateral and/or multilateral agreements already existing. Recital 38 further clarifies that “further agreements should comply with the rules on exchange with third States”.

1.6. The European Parliament position on six critical issues

The European Parliament is called to vote on the last report on the proposal for a Framework Decision during its second plenary session in September 2008. The draft report of Ms. Roure, the LIBE Rapporteur since the tabling of the commission proposal in October 2005, has obtained a quite unanimous support when it was adopted in the LIBE Committee on July 2008⁽¹²⁾. Therefore, it is foreseeable that the position expressed there will be backed and adopted by the EP. The report advances a series of amendments to the Council proposal that deserve attention for their potential impact, if adopted, on the legal frame of EU data protection regime. Some of them are also highly relevant in the transatlantic context.

¹¹ Moreover, rights of data access are limited in art. 17(2) which introduces the possibility to set up further restrictions by Member States.

¹² European Parliament – LIBE Committee, *Report on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters* [16069/2007 - C6-0010/2008 - 2005/0202(CNS)].

I. The first issue addressed in the report is the question of the scope of the Framework Decision. As it was analysed in the previous session, the Framework Decision should apply only to data transferred or made available between Member States. Amendments 4 and 9 of the EP reaffirm the principle that the Framework Decision should also apply to national data processing, thus avoiding different levels of data protection within the EU.

II. The second issue concerns the principles of proportionality and purpose limitation. In order to strengthen these principles the EP proposes to limit further processing of personal data received by other Member States by excluding the possibility for Member States to express a general consent for categories of information or categories of further processing (AM 7).

III. The third important issue is the protection of sensitive data. Article 6 defines rules of processing of special categories of data. Those data are those “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership [...] [and] data concerning health or sex life”. Even if those categories recall and respect the wording of art. 6 of Convention no. 108 of the Council of Europe, it is important to note that the wording has been “reversed”. Instead of setting as a general rule the prohibition of data processing, and then setting exemptions, art. 6 of the Framework Decision avoids the ban and prefers to establish only the limits of the processing “when it is strictly necessary and when national law provides adequate safeguards”. In line with Convention 108, the Parliament report proposes to re-insert the prohibition, establishing only in a second moment a list of possible exceptions and strict rules to be respected.

IV. The fourth difference with the Council approach emerges in the provisions concerning national supervisor authorities. The EP report asks for the setting up of a Working Party on the Protection of Individuals with regard to the Processing of Personal Data for the purpose of the Prevention, Investigation, Detection and Prosecution of Criminal Offences (AM. 30). It also defines the tasks and the responsibilities of the said Working Party: providing opinion in national and international matters related to data protection; advise the Commission and the Member States on any amendment of the Framework Decision; informing the Council and the Commission on different levels of protection within the EU; formulating, even on its own initiative, recommendations on matters related to data protection and law enforcement; annually reporting before the Council, the Commission and the EP (AM. 31).

Such a modification of the final text would create not only a strong system of oversight, but would also empower the EU in international negotiations on security and law enforcement matters.

V. The Framework Decision Council text introduces a provision on the transfer of personal data to private actors. However, such transfer does not cover completely the increasing development of security measures based on access of data initially collected for economic purposes. The report of the EP modifies in this regard the relevant Council provision (AM 21-24), in order to cover both data transfer and data access. It also reduces such activities to a case-by-case approach (AM. 22 and 23) and bounds private controllers and processors to be subject to, at least, the same requirements imposed on competent authorities.

-Finally, the sixth set of issues highlighted by the report covers the transfer of personal data to third countries. In particular, Amendments 17 to 20 intervene on the two main rules of international transfers; adequacy and prior consent. Amendment 18 maintains the permission of exceptional transfer without prior consent, but data received may be “processed by the recipient only if absolutely necessary for the specific purpose for which the data were supplied”. Moreover, such data transfers have to be notified to the competent national supervisory authority. Amendment 20 identifies who is in charge of assessing the adequacy of the level of protection of a third country, conferring this responsibility to an independent authority. Amendment 17 establishes the guidelines of equivalence, by referring to Article 2 of the Additional Protocol to the Convention 108, “and the corresponding case-law under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms”. Finally, amendment 19 strongly limits the derogation from the adequacy criteria and obliges to maintain records of such transfers.

The integration of these amendments in the final text could bring major changes to the present legal frame under the third pillar. They would also have a future influence on the transatlantic and international level, with the possible effect of stopping the proliferation of ad hoc agreements.

2. Legislation and main principles in the US: A multilayered scheme

2.1. Privacy and data protection in US Constitutional law

The first layer of privacy protection in the US is at the Federal Constitutional level. Even if the United States Constitution does not explicitly refer to privacy, at least four provisions protect, and have been interpreted as providing, a right to privacy. The First, the Third, the Fourth and the Five Amendment offer several forms of protection from government intrusion into people’s life. Notwithstanding the fact that each of these Amendments seem to offer a special kind of protection, the greatest part of the case law and the literature has focused on the Fourth and First Amendment. Given their strong relevance in the development of the information privacy law in the US, it could be worth to recall them. The First Amendment states:

“Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances”.¹³

The Fourth Amendment states:

“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”.¹⁴

The First Amendment is relevant for privacy purposes, since it provides for the right of speaking anonymously as well as not being compelled to disclose own groups’ affiliation (Solove, D.J., et al., 2006, p.33). But it is especially the Fourth Amendment that has provided, and still provides, the main constitutional reference to the

¹³ Congress of the United States, *Bill of Rights*, 1789, I Amendment. Available at: http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html

¹⁴ Congress of the United States, *Bill of Rights*, 1789, IV Amendment. Available at: http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html

protection of privacy in the US. In *Schmerber v. California*, in 1966, the Supreme Court stated that “[t]he overriding function of the Fourth Amendments to protect personal privacy and dignity against unwarranted intrusion by the State”.¹⁵

However, the application of the Fourth Amendment is not unproblematic, because of the interpretation of its wording in a modern context of technological developments (Gellman, 2005, p. 11). Especially the use by the Supreme Court of the criterion of ‘reasonable expectations of privacy’ seems, and this contrary to the use of it by the European Court on Human rights, to deny constitutional protection in most cases. After a promising ‘birth’ of the criterion in *Katz* case,¹⁶ followed a long series of cases in which no constitutional protection was granted to privacy issues, for instance in the *Pen Register* case (¹⁷). The recent *Kyllo* case however seems to suggest that a more constructive application of the criterion, in line with *Katz* and the case law of the European Court on Human Rights, is still possible (¹⁸).

The application of the criterion of “reasonable expectation of privacy” could be tricky in an rapidly changing world where technologies permeate everyday life. As technology develops, the “reasonable expectation of privacy” develops along with it, generally to the detriment of privacy as technology itself tends to decrease privacy expectations. In the Kyllo case, the Supreme Court used the criterion of a device being “in general use” to determine whether or not it infringed privacy; however, as most technology applications tend to develop from limited, sectoral use to general, public use, the related privacy expectations at one point in time will become unreasonable. Hence, using ‘reasonable expectations of privacy’ to face developments in technology poses the risk of a slow but certain erosion of privacy.

Although privacy is only protected indirectly, it is worthy to note that in 1965, in the case *Griswold v. Connecticut* (318 U.S. 479, 1965), the Court stated that the

¹⁵ *Schmerber v. California*, 384 U.S. 757, 767, 1966.

¹⁶ The *Katz v. United States* (1967) case is important in relation to two questions: the relevance of the individual and the relations between the individual, the society and the private sector. The Court stressed the principle that the Fourth Amendment “protects people, not place” (Solove D.J. et al., 2006, pp. 34-35), thus focusing on the individual rather than the “sanctity of the home”. Justice Harlan, concurring in *Katz*, firstly defined the famous “reasonable expectations of privacy test” in order to provide a method to determine the individual’s right of privacy. The test is twofold: a person must “have exhibited an actual (subjective) expectation of privacy” and “the expectation [must] be one that society is prepared to recognize as ‘reasonable’” (Solove, D.J. et al, 2006, p.34).

¹⁷ The challenges raised by the twofold *Katz* determination of one individual’s right of privacy are clearly represented by this case, known as *Smith v. Maryland* (442 U.S. 735, 1979). It argued that the installation of a so-called “pen-register”, a mechanical device that records numbers dialled on a telephone, was not infringing the Fourth Amendment even if it was done without warrant. In fact, “all telephone users realize that they must “convey” phone numbers to the telephone company [...]. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial” *Smith v. Maryland*, quoted by Solove, D.J., et al., 2006, p. 234). Given the daily use of these electronic equipment, among others, for the prevention of law violations, the reasonable expectation of privacy of the petitioner could not be assumed to be one that society is prepared to recognise as reasonable. However, such reasoning, based on a supposed “risk-assumption” could become very problematic in contemporary societies strongly based, and dependent, on communication networks.

¹⁸ In the case *Kyllo v. United States* (533, U.S. 141, 2000), the Court decided that government’s use of thermal imaging equipment without a warrant is unlawful, because the technology is not in general public use. On those cases, the balance should be based on the question whether “the [Founding] Fathers enjoyed this level of security from government surveillance and harassment” (Ku, R., quoted in Solove, D.J., et al., 2006, p. 261).

individual has a constitutional right of privacy. Protection of personal data is not protected as such, and having in mind the Pen Register case and other cases it would be misleading to say that personal data is constitutionally protected as such without there being strong privacy aspects.

Finally, it is important to observe that federal constitutionalism is complemented and co-exists with state constitutionalism. The constitutional right of privacy is directly provided in some State Constitutions. Among them, the Californian constitutional right of privacy applies also to private parties.¹⁹ It has established an Office of Privacy Information and a new Data Security Law is pending, which would amend the breach notice law to require those subject to it, state agencies and persons or businesses doing business in California, when notifying individuals of a breach of their personal information, as defined, to also notify the Office of Privacy Protection. It would apply only in the case of notifications made by the “substitute” method, that is using mass media rather than individual notifications”.

2.2. US data protection legislation: A short history

Data protection may not be in the US constitution, but it is not absent in the US legal landscape. On the contrary. According to the historical analysis of authors such Solove, Rotenberg and Schwartz, one of the main drivers of legal discussion and legislation in the US is the relation with technological developments.²⁰ The growing capacities and diffusion of information technologies became the focus of a series of publications in the 1960s. Peter Blok refers to these publications as the “literature of alarm” (Blok, P., 2001, p. 3). One of the main issues raised is that automating computing risks distorting the relations between governmental organisations and citizens. Therefore, the main issue becomes the definition of guarantees of protection of data management. Within this socio-political context, the *Code of Fair Information Practices* of 1973 became a cornerstone of further legislation on data protection.²¹ It identified the following five ‘practices’ or principles:

1. There must be no personal data record keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.

¹⁹ Art. 1 Sec. 1 of the Californian Constitution states: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy”.

²⁰ The Warren and Brandeis article on “the right to privacy”, published in the Harvard Law Review in 1890 (reproduced in Solove, D.J., et al., 2006, pp. 12-22) has proved to be one of the most influential contributions to the development of a privacy legislation in the US. The article highlights the potential negative consequences of the diffusion of instantaneous photography and sensationalistic press. The article calls for the definition of a new right of privacy, the right to be let alone. Apart from the strong influence that this article still has in US juridical culture, it is worth to note that Warren and Brandeis did not define privacy as an absolute right, but they set up a list of different legitimate limitations to this right, mainly protecting the right of freedom of expression (Solove, D.J., et al., 2006, pp. 20-22).

²¹ The Code was proposed by the report of the United States Department of Health, Education, and Welfare (HEW)

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.²²

The main piece of ‘hard’ legislation covering data processing by government agencies was adopted the following year, in 1974. The Privacy Act covers the management of systems of record held by federal agencies and submits it to the application of fair information practices. It is partly based on the outputs of a four years work of the Senator Irvin, chairman of the Senate Committee on Constitutional Rights. The original law proposal included the set up of a Federal Privacy Board. Finally, this provision was dismissed as part of political bargain to allow both chambers to pass the act.

2.3. *The Privacy Act of 1974*

The Privacy Act of 1974 (5 U.S.C. § 552a, 1974) is the main legal framework protecting personal data held by the public sector in the United States. It protects record held by US government agencies and requires them to apply fair information practices.²³ From a first overview of the main provisions of Privacy Act, it appears that the Code of Fair Information Practices was strongly integrated in the wording. All the five principles find their place in the law. The transparency principle is translated in (e)(4): “Each agency that maintains a system of records shall [...] publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records [...]”. The access and correction principles shape the provisions of the section (d) on “access to records”. Data security is addressed in section on “agency requirements”, at (e)(5) and (10). Finally, the purpose limitation principle is enshrined in (e)(1), stating that each agency shall “maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President”.

Besides the translation of the Fair Information Practices, the Privacy Act identifies a specific class of sensitive data: “records describing how any individual exercises rights guaranteed by the First Amendment” (e)(7). Such records shall not be maintained unless strict and cogent rules. The Privacy Act provides for the establishment of Data Integrity Boards within agencies participating or conducting matching programs (u). Such Data Integrity Board has essentially review, approval and guidelines setting powers. It has no enforcement powers and is not structurally independent, consisting of “senior officials designated by the head of the agency” (u)(2).

Finally, sections (g) and (i) defines the procedures of legal redress available to individuals and of criminal penalties in case of certain categories of misconduct of government officers.

²² U.S. Department of Health, Education, and Welfare, Secretary’s Advisory Committee on Automated Personal Data Systems, Records, Computers, and Rights of Citizens, 1973, p. viii. Available at: <http://epic.org/privacy/hew1973report/>. See also: Solove D.J. et al., 2006, pp. 35-36.

²³ After a first section dedicated to the definition of the key terms, The Privacy Act’s provisions delineate (among other): the “conditions of disclosure” (§ 552a (b)); “accounting of certain disclosures” (c); “access to records” (d); “agency requirements” (e); “civil remedies” (g); “criminal penalties” (i); “general and specific exemptions” (j and k) and “data integrity boards” (u).

2.4. *Three main flaws of the Privacy Act from a transatlantic perspective*

Notwithstanding such remarkable translation of the fair information practices into the wording of the Privacy Act, a certain number of scholars, both European and North American, have raised substantial criticism (Blok, P., 2001, Bignami, F., 2007a & b). Given the scope of this study, it is worth to concentrate the analysis on some of the main flaws addressed to the Privacy Act, in particular those that could become (or already are) crucial issue in case of negotiation of a transatlantic agreement.²⁴ The first issue the definition of ‘system of records’ of the Privacy Act. The second main flaw concerns the redress system. The third issue focuses on some vague limitations to data management imposed by the Privacy Act.

I. A basic notion in the Privacy Act is “system of records”. *System of records* “means a group of any records under the control of any 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”.²⁵ One author comments that the present definition of “system of records”, coupled with the use of a data mining instrument, could lead to the exclusion of enormous database from the scope of the Privacy Act (Bignami, F., 2007a, pp. 634-635). The core of her reasoning is that a database of phone numbers not directly associated to names but retrieved by proxies such as country codes, risks to escape the definition of system of records. If the reasoning proves its validity, it could be easily extended to other types of data. The availability and spreading of data mining in law enforcement action could lead to the establishment of new databases out of the scope of the Privacy Act. Furthermore, such an interpretation of “system of records” could foster divergences in the interpretation of data collection and sharing.

In its negotiations with the US, the EU will have to be very carefully in its requirements and formulations. IP addresses and other personal data such as CCTV images may well be disregarded as personal data by US officials (see: Gellman, 2005).

II. The Privacy Act grants certain rights to the individual. *Individual* is “a citizen of the United States or an alien lawfully admitted for permanent residence”.²⁶ In its quite paradoxical simplicity, the issue of redress, especially the non-availability of civil remedies for non-US citizens, represents one of the main issues at stake in the follow up of the works of the High Level Contact Group. In fact, according to the definition of “individual” recalled above, EU citizens that are not permanent in the US are excluded from the scope of the Privacy Act. This provision in itself represents a major obstacle in transatlantic negotiations.²⁷ However, the provisions on civil remedies are, *per se*, framed in a way that strongly limits the possibility of legal redress. In order to

²⁴ In general, critics identify at least five sets of issues: the Privacy Act covers only a limited number of authorities (Blok, P., 2001); it provides few substantial limitations to the use of personal data (Blok, P., 2001 and EPIC, 2006); the passive attitude of the Office of Management and Budget (Blok, P., 2001); the inefficiencies and limitations of the redress system (Blok, P., 2001 and Bignami, F., 2007 & 2008) and the lack of the institutionalisation of a independent authority (Bignami, F., 2007 & 2008). We will come back to the latter below sub 2.6.

²⁵ See § 552a (a)(5) of the 1974 Privacy Act.

²⁶ See § 552a (a)(2) of the 1974 Privacy Act.

²⁷ In its opinion on the adequacy level of the protection offered by the Privacy Act, the Belgian Data Protection Commission underlined the same points (Commission de la Protection de la Vie Privée, 1998, pp. 2-5).

start a civil action against the agency, the behaviour of the agency must have had an adverse effect on the individual (g)(1)(D). Moreover, the court should determine that the “agency acted in a manner which was intentional or wilful” (g)(4). Such a complex framework, especially within a context marked by the lack of structural independent authorities, risks to limit *ex ante* the enforcement of legal redress. Moreover, the criteria of “adverse effect” could be difficult to prove in an environment marked by the use of invisible technologies of control (Bignami, F., 2007, p. 633).

The EU should not only address the issue of redress for non-US citizens. The limited scope of US redress (‘intentional adverse effect’) is equally troublesome. It disregards the basic European idea that data protection concern is not only about blocking and prosecuting illegitimate use of data, but also to channel legitimate use of data and to create redress for problems arising with this (De Hert, P. & Gutwirth, S., 2006).

III. The third set of issues concerns the limitations and the exemptions to data management imposed by the Privacy Act. Administrative interpretation of the provision allowing disclosure of data “for routine use”²⁸ is said to have weakened “significantly” the effectiveness of the law (EPIC, 2006, p. 1, Blok, P., 2001, pp. 22-23).

Although many data protection principles as recognized in EU law are present in American law, there is no solid basis in US law for core principles such as purpose limitation and data minimization. To protect these core principles should be a central element in EU negotiations.

2.5. Brief overview of other statutory laws

As stated before, the United States has no comprehensive legal framework covering the private sector. However, since the 1970s, the Congress has passed several laws covering different economic sector or regulating surveillance activities.

These laws could range from focusing on specific activities such as video rental (Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711, 1988), to approaching more transversal issue such as credit reporting (Fair and Accurate Credit Transactions Act, Pub. L. No. 108-159, 2003). It is also important to mention the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Pub. L. No. 104-191) that empower the Department of Health and Human Services with the authority to promulgate regulations on privacy of medical records; the Gramm-Leach-Bliley Act (GLBA) of 1999 (Pub. L. No. 106-102, 15 U.S.C. §§ 6801-6809) that obliges financial institutions to publish privacy notices and provide opt-out rights when they seek to disclose data to other companies; as well as the Children’s Online Privacy Protection Act of 1998 (Pub. L. No. 106-170, 15 U.S.C. §§ 6501-6569) restricting the use of information gathered from children under the age 13 by Internet web sites.

Among the laws regulating surveillance activities, it is worth to remind the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. §§ 1801-1811, 1978), amended by

²⁸ See § 552a (a)(7)) of the 1974 Privacy Act. *Routine use* “means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected”.

the USA-PATRIOT Act of 2001, as well as the Electronic Communication Privacy Act (18 U.S.C. §§ 2510-2522, 2701-2709, 1986). Both laws provide standards and procedures for the use of electronic surveillance, with the FISA focusing on gathering foreign intelligence. It is worth to remark that the recent amendments to FISA have weakened its protecting standards. The USA-PATRIOT Act modified the need of foreign intelligence gathering: from being the “primary purpose” to a “significant purpose” (EPIC, 2006, p. 7, Solove, D.J. et al., 2006, pp. 288-289). The potential relevance of such changes within a transatlantic perspective has been remarked also by senior EU officials involved in informal JHA meetings.²⁹

The Congress has also passed other laws that deal with privacy and data protection, but with the aim of foster government access to personal data.³⁰ Among them, one of the most significant is the USA-PATRIOT Act.³¹ Since its adoption, the USA-PATRIOT Act has raised harsh discussions and criticism (EPIC, 2006, p. 8, Solove, D.J. et al., 2006, pp. 298-300, Birnhack, M.D. and Elkin-Koren, N., 2003, pp. 30-31) ranging from the weakening of the privacy guarantees of other laws to the accusation of de-balancing the relation between the government and the individual. Among the main reforms introduced by the USA-PATRIOT Act there are: a new definition of domestic terrorism; delayed notice of search warrants; new definition of Pen Registers and Trap and Trace devices; sharing of foreign intelligence information.

A second significant law that deals with privacy and data protection is the Homeland Security Act (6 U.S.C. § 222, 2002). This Act consolidates and fuses 22 federal agencies into the Department of Homeland Security (DHS) and sets up of a Privacy Office within the same Department. The competencies and activities of this Privacy Office will be analysed in the next session.

Finally, it is important to recall another piece of US legislation that could play an important role in privacy protection. If, as stated, access to records and legal redress could be limited for EU citizens under the Privacy Act, the Freedom of Information Act (FOIA) (5 U.S.C. § 552, last amended in 2002)³² provides the possibility, for every person, to access records maintained by US public authorities. Such a right of access is not without limitations, especially when information deals with law enforcement activities (paragraphs (b)(7) and (c)(1)) and foreign intelligence and counter-intelligence (c)(3).³³

2.6. Overview of the main US supervisor authorities

As already stated in the brief historical overview, at the moment of the approval of the Privacy Act the idea of setting up an independent data protection authority was disregarded. The passive attitude of the Office of Management and Budget has been already mentioned, especially the lack of audits and controls on the base of plants

²⁹ Council of the European Union, *EU-US informal JHA senior level meeting (09-10 January 2008, Ljubljana)*, doc. 5172/08, Brussels, 18 January 2008, pp. 5-6.

³⁰ For a comprehensive list of laws passed since the beginning of the 1970s in the US, see Solove, D.J., et al., 2006, pp. 36-37. For further details on each legislation, refer to the relevant chapter of the same publication.

³¹ Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA-PATRIOT Act, Pub. L. No. 107-56, 2001).

³² Available at: <http://www.usdoj.gov/oip/foiastat.htm>

³³ It is interesting to note that a Dutch Member of the European Parliament, Sophie In't Veld, has decided to test the FOIA system by lodging a request of access to her data processed by the Automatic Targeting System.

(Blok, P., 2001, pp. 25-26). However, since 2001, a certain number of privacy offices have been set up, at different levels.

- The *Homeland Security Act of 2002*, discussed above, has established the DHS Privacy Office. The Secretary of the DHS has the responsibility to appoint a senior official as Chief Privacy Officer (DHS CPO). The responsibilities of this Chief Privacy Officer are to ensure that the use of technologies sustain and not erode privacy protections; to assure compliance of Privacy Act systems of record management to Privacy Act fair information practices; to evaluate legislation and regulation proposals; to conduct privacy impact assessment and to report to the Congress annually. Finally, according to the European Council documents and its own Annual Report to the Congress,³⁴ the Chief Privacy Officer has also assumed a consultative and participative role in the works of the EU-US High Level Contact Group.

- The President's Civil Liberties and Privacy Oversight Board has been established in 2004 by the *Intelligence Reform and Terrorism Prevention Act* (IRTPA, Pub. L. No. 108-458, 2004). The five members of the Board are appointed by the President, and the chair and vice-chair appointments are submitted to the Senate approval. Its purpose is to "provide an enhanced system of checks and balances to protect privacy and civil liberties"(IRTPA, (a)(2), quoted by Rotenberg, M., 2006, p. 44). The main responsibilities are to advise the President and other executive branch officials in order to ensure that respect of privacy and liberties are taken into account in the implementation of laws and regulations, as well as to review terrorism information sharing practices. Finally, a Civil Liberties Protection Officer has been established in the Office of the National Intelligence Director by the same Intelligence Reform and Terrorism Prevention Act. Its responsibilities are very similar to those of the DHS CPO (Rotenberg, M., 2006, pp. 48-49). The most relevant difference is that the Civil Liberties Protection Officer does not report to the Congress.

2.7. Two critical assessments: Privacy agencies and legal redress

I. In its article on "privacy oversight after 9-11", Rotenberg assesses the activities of the first years of work of the US privacy agencies (Rotenberg, M., 2006, pp. 19-30, 43-44, 52-55 and 58-60). His conclusions are generally negative, two agencies out of three have done nothing because of institutional problems or interpretation of their mandates. The most active agency has proved to be the DHS Privacy Office: "[t]hroughout public reporting, active outreach, the participation of an external advisory board, the development of a good framework for privacy evaluation, and the issuance of significant reports on the unlawful transfers of personal information of American citizens and the risks of RFID-enabled documents, the DHS Privacy Office suggests both the structural attributes and record of achievement that could make a successful agency-specific privacy office" (Rotenberg, M., 2006, p. 59).

However, if this finding demonstrates that privacy agencies can succeed in limiting executive choices, the fact that the chief privacy officer is political appointment could undermine the necessary oversight. Bignami therefore defines US privacy agencies as not structurally independent when compared to EU data protection authorities (Bignami, F., 2007b, p. 7). Moreover, US privacy agencies in general lack powers to investigate and sanction privacy violations.

³⁴ Department of Homeland Security Chief Privacy Officer, *Annual Report to Congress, July 2006-July 2007*, Washington, July 2007, p. 7.

II. This situation transforms the courts in the “sole guarantors of Privacy rights” (Bignami, F., 2008, p. 6). The lack of powers of US privacy agencies is also underlined by Gellman, who rejoins Bignami also on the role of courts and points at the practical obstacles to individual legal redress through them. In his study on video-surveillance law in the United States, Gellman concludes that: “[t]he courts may offer the only possibility of remedy for an individual whose privacy was invaded by video surveillance. However, pursuing cases in court is not always a practical remedy. Litigation can be expensive, plaintiffs can have great difficulty finding lawyers willing to take the cases, providing damages is difficult, and the prospects for relief are uncertain.” (Gellman, R., 2005, p.34)

The final Report of Wik-Consult/RAND Europe also highlights the effectiveness of US enforcement measures. In their study of comparison of privacy and trust policies in the area of electronic communications they report the lack of sufficient recourse to private redress. In particular, “the fact that it is typically the FTC that pursues cases on behalf of the consumer [...] and the limited ability in practice for consumers to pursue their own claims, support the view of some respondents that organisations may not be under sufficient pressure to maintain individual privacy.”(Wik-Consult/RAND Europe, 2007, p. 78)

PART TWO – NEW TECHNOLOGIES AND CASE-STUDIES

Given the aim of this study, paving the way to a parliamentary debate on the possible conclusion of a transatlantic agreement on data protection, it seems wise to analyse the most relevant challenges emerged in the last few years. In particular, it is important to consider data mining, one of the main technologies that have been introduced in the field of law enforcement and security, and the diffusion of measures aiming at accessing a growing number of data of different nature and different sources.

In the fields of security and law enforcement, the requests for data access are steadily multiplying. The personal data concerned are of different nature, from biographical to banking data, and they are accessed from different sources, directly from individual or from commercial databases.

Given the nature of present modernity, most of these measures have an international, and, especially, a transatlantic scope. Therefore, it is not surprising that they have been at the core of long and frequently harsh debates. Below, following our discussion of data mining, is provided an overview of the most relevant programs.

1. Data mining: A technology of analysis and the related issues of profiling and risk assessment

1.1. What is data mining?

Data mining is said to be one of the most relevant and important tools in the fight against terrorism and international crime. It is not an entirely new tool, and its growing use is not limited to the public sector. On the contrary, for several people it is the private sector that has firstly experienced this diffusion of data mining.³⁵

Data mining is generally described as an analytical instrument able to identify suspects, detect illegal activities and thus prevent threats. In the last decade, it has also become the focus of harsh discussions among experts, law enforcements officials, scholars and civil rights advocates. The decision of the US government to launch and fund data mining programs has also interested public attention and raised strong critics. Some of those critics have led to the cancellation of specific programs. It is therefore important to define what data mining is, describe some of the more relevant data mining programs and finally focus on concerns and responses to data mining. A shared definition of what data mining does not exists. Several experts and scholars adopt their own definition. Notwithstanding a certain number of definitions, the one provided by Ann Cavoukian seems to offer the best way to approach the issue. “Data mining is a set of automated techniques used to extract buried or previously unknown pieces of information from large databases. Successful data mining makes it possible to unearth patterns and relationships, and then use this “new” information to make proactive knowledge-driven business decision” (Cavoukian, A., 1998, p. 4).³⁶

³⁵ In its report on data mining, Cavoukian recall the six factors identified by IBM has crucial in the diffusion of data-mining in the private sector: “(1) A general recognition that there is untapped value in large databases; (2) A consolidation of database records tending toward a single customer view; (3) A consolidation of databases, including the concept of an information warehouse; (4) A reduction in the cost of data storage and processing, providing for the ability to collect and accumulate data; (5) Intense competition for a customer’s attention in an increasingly saturated marketplace; (6) The movement toward the de-massification of business practices”, Cavoukian, A., *Data Mining: Staking a Claim on Your Privacy*, Information and Privacy Commissioner/Ontario, 1998, p. 5.

³⁶ We note that this definition, dating back to 1998, focuses on the business use of data mining.

Therefore, data mining is based on a multiplicity of techniques and it relies on automating processing. It relies on large databases and can extract previously unknown information from data. Those information are offered under the form of patterns and relationships, and could be used, in a second moment, in the decision-making process. The added value of this simple definition is that it contains, *in nuce*, most of the elements of other more complex, and topic-oriented definitions.

Other elements can be added to this presentation. First of all, data mining does not adopt a verification approach but a discovery approach. A verification approach is based on the formulation of a hypothesis, for example the relation between two actions, that is later verified or rejected. The main limits of this approach are the creativity of the user and the linearity of the programs generally used (Seifert, J.W., 2007, p. 1). On the contrary, the discovery approach does not imply the formulation of an hypothesis and can “examine several multidimensional data relationships simultaneously, identifying those that are unique or frequently represented” (Seifert, J.W., 2007, p. 1)⁽³⁷⁾.

When data mining is applied to security and law enforcement fields, it is useful to identify two approaches: “subject based searches” and “pattern-based data mining” (Rubinstein, I, et al., 2008, p. 262). The first one simply accelerates the average process of information gathering on already suspected persons. It could be also considered a targeted use the discovery approach. Instead, the second approach is more advanced in relation to the recourse of all the data mining possibilities. Pattern-based data mining is based on the development of “a model of assumptions about the activities and underlying characteristics of culpable individuals or the indicators of terrorist plans” (Rubinstein, I, et al., 2008, p. 262).

In an expert report of the Council of Europe data mining and profiling are clearly linked. According to the report, data mining is the second step out of the three that constitutes a process of abstract profiling (Consultative Committee, 2008, pp. 3-4).³⁸ The report rejoins the idea of the utility of a distinction between two possible uses: descriptive and predictive (Consultative Committee, 2008, p. 9). Descriptive methods are used to identify information already present but hidden in the mass of data, as could be the case of “subject based searches”. Predictive use aims to predict future behaviour on the base of the exploitation of a set of observed and documented facts. Pattern-based data mining seems closer to this second method.

1.2. Overview of US data mining programmes in the security field

Carnivore. This is a computer program made public by FBI in 2000. It can sift through digital packets in search of specific text strings. It can also target messages

³⁷ According to a report for the Congress of the Congressional Research Service (Seifert, J.W., 2007, p. 1), five parameters can be adopted in examining the data:

1. association (patterns where one event is linked to another);
2. sequence or path analysis (patterns where one event leads to another);
3. classification (identification of new patterns);
4. clustering (finding groups based on previously unknown facts) and
5. forecasting (discovering patterns from which one can make reasonable predictions regarding future activities).

³⁸ The three steps are: observation (data collection and data warehousing), data mining (establishment, within a certain limit of error, of correlation) and inference (infer new data on the category to which persons belong). The inference step is the one generally defined “profiling”.

sent from a defined computer or email address. It has two operative modes: “pen” or “full”. The full mode provides for the scan of the full content of messages, while in “pen” mode the program scans only “addressing” information. The program is designed in a way that allows human observation only for the information filtered (Etzioni, A., 2002, pp 274-275).

Total Information Awareness (TIA). It was a project developed by the Defence Advanced Research Projects Agency (DARPA): the aim was to detect terrorist by scanning large databases of personal information with the scope of detecting the information signature of terrorists (EPIC, 2006, p. 13). Following rising criticisms on the scope of the project, the name was modified in Terrorism Information Awareness (TIA). Finally, on 2003, the Congress decided to cut funding.

Multi-state Anti-Terrorism Information Exchange (MATRIX): this project was run by the State of Florida together with a private company, Seisint. According to Epic, MATRIX combined public and private records from multiple databases with data analysis tools and provided a wealth of personal information in near-real time to law enforcement agents in 13 participating states (EPIC, 2006, p. 13). All the States that were involved, but Florida, withdraw its participation on the base of privacy concerns. Federal funding was cut on April 2005 (Seifert, J.W., 2007, p. 15).

Computer Assisted Passenger Prescreening System II (CAPPS II). The program was going to replace the Computer Assisted Prescreening program launched in 1996 as pilot project to screen airlines’ passenger. CAPPS II was developed by the Transportation Security Administration (TSA) and aimed at screening the information on passengers provided at the purchase of the ticket. On the base of the screening, passengers were fit or in a “selectees” category, requiring further security screening, or in the normal category. Passengers’ information were also checked against lists of known terrorists. PNR records were supposed to feed the CAPPS II system, however, according to the first EU-US PNR agreement, EU PNR would have been used only after the conclusion of the experimental trial. Finally, the system was abandoned in 2004, when Delta Airlines refused to provide passenger information (EPIC, 2006, p.11 and Seifert, J.W., 2007, pp. 8-11). It has been replaced by the launch of the Secure Flight project.

Secure Flight. This program was also developed by the Transportation Security Administration as a passenger pre-screening program. The program requires the “submission of a limited amount of passengers reservation information by an aircraft operator to TSA for watch list matching purposes” (Rotenberg, M., 2007, p. 6) The project encountered difficulties in meeting data protection and privacy criteria, and its launch has been postponed to 2010 (EPIC, 2006, p. 13, Seifert, J.W., 2007, pp. 11-12 and Rotenberg, M., 2007, p. 6).

Automate Targeting System (ATS). This program has been originally developed by the Treasure Enforcement Communication System to assign cargos risk assessment scores. The Department of Homeland Security aims to deploy the ATS system to screen travellers entering the US by car, plane, ship and rail (Seifert, J.W., 2007, p. 17, Steinhardt, B., 2007, p. 1 with reference to a System of Records Notice posted in the Federal Register in November 2006). ATS collects information both directly and form other systems. It is not clear if at present ATS is used to profile human being or not. Steinhardt underlines that the contradictory statements of the US government on the use of such a system pose a serious problem of transparency (Steinhardt, B., 2007).

NSA database of telephone calls information. This program was launched by the National Security Agency (NSA) as a classified program in 2002, and kept secret for at least four years. It aimed at collecting, analysing and sharing telephone calls information. It is still not clear how the program has been managed (Seifert, J.W., 2007, pp. 18-20). Bignami reports that at the end of 2001, NSA approached the main US telecommunications providers and asked them to provide NSA “incidents” (addressing) data of all communications (Bignami, F., 2007, p. 614). This NSA program poses the same issue of transparency, and accountability, of the ATS system. It also raises questions on the collaboration between private sector and public security agencies. Finally, given the claimed use of “incidents” data, and retrieval by phone numbers, it highlights the flaws of the Privacy Act definition of “system of records” (Bignami, F., 2007, pp. 634-635).

1.3. Three concerns raised by data mining

The foregoing description of US data mining systems is coloured by problems and data protection criticisms of all kind. More generally one needs to observe that all data mining programs have raised numerous critics, especially in the United States. The questions raised by data mining range from the respect or collision with data protection principles, to accountability and oversight on governments, to the shape itself of present modernity.

I. First there a quite paradoxical relation between data mining and some data protection principles (Cavoukian, A., 1998, Solove, D.J., 2008, Bignami, F., 2007a). Indeed, a good data mining program cannot, in advance, delineate what the primary purpose will be (Cavoukian, A., 1998, p. 12). The “discovery model” upon which data mining is based, does not need an hypothesis, and without an hypothesis, establishing the specific purpose of data collection or data processing is a much more complex task. The antithesis to purposes and use limitation reaches its own peak when data mining programs are run on data initially collected for other, generally commercial, purposes. Therefore, the most part of the data mining programs in the field of law enforcement and security run as further processing: CAPPS II mined passengers’ travelling information, the NSA database is supposed to mine telephone calls’ information stored by communication providers for other purposes.

II. Another critical issue of data mining programs is the respect of the principles of transparency, data access and rectification. Data mining process are invisible, and it is hard, if not impossible, to track their use for data subjects. Moreover, some programs, such as the NSA telephone calls database (Bignami, F., 2007a, p. 609-611), have been developed in secrecy. Generally, there is a high level of confidentiality surrounding their working guidelines or even their current application, as it is the case with ATS (Steinhardt, B., 2007). The data subject hardly knows that her data are processed, and therefore cannot enforce its rights of access and rectification.

III. Furthermore, the impact of the secrecy aspect of data mining goes beyond the threat to data protection principles. It calls into question the accountability of governments and agencies, as well as the role of private sector. Such an issue is particularly relevant within an institutional context deprived of data protection authorities, or with privacy agencies lacking strong powers. Such a high level of secrecy, even on the outcomes in term of increased security, does not allow for the balancing of these measures against the principle of proportionality.

Notwithstanding these different layers of criticism, according to Rubinstein, Lee and Schwartz, there is an emerging “consensus view” concerning, at least, pattern-based

data mining: “the basic premise is that data mining has substantial potential to protect against terrorism. But policy experts also insist that technological and legal safeguards are needed” (Rubinstein, I., et al., 2008, p. 266).³⁹

1.4. European and US responses to data mining

A first European response to data mining and profiling has been recourse to more explicit data protection principles. The Europol Convention with its length articles on data protection principles a good example of this approach. Europol is allowed to gather extensive amounts of data and to subject it to modern intelligence tools at the price of more precise data protection duties that explain, for instance, why not Member States have no automatic access to all files kept by Europol. A second response came from the European Court of Human Rights. In a recent case, *Liberty v. United Kingdom*, the Court has examined an episode of mass-surveillance of telecommunication data.⁴⁰ In its judgment, the European Court of Human Rights states that a secret system of mass surveillance operated by the UK Minister of Defence between 1990 and 1997 is in breach of the right to privacy established in article 8 of the ECHR. In its conclusion:

“the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court’s case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants’ rights under Article 8 was not, therefore, “in accordance with the law” (§ 69, *Liberty v. United Kingdom*).

Such a judgement creates an important argument against the introduction, and the legality, of secret data mining programs in Europe. Human rights require, the Court holds, that profiling programs are partly made foreseeable through detailed regulations.

The legal protection against such kind of programs in the US appears far more limited. According to Cate, “most government data mining today occurs in a legal vacuum outside the scope of the Fourth Amendment and without a statutory or regulatory framework”.⁴¹ Cate describes the extraordinary volume and variety of personal data to which the government has routine access, directly and through industry. He also examines the absence of any meaningful limits on that access, due to the outdated and inadequate nature of statutory protections and the Supreme Court’s

³⁹ They also identify the seven principles that define the generally accepted framework for government data mining: 1) legal authorization; 2) access controls and authentication of users; 3) rule-based processing; 4) anonymization and selective revelation; 5) audit function; 6) addressing false positives and 7) accountability measures.

These principles appear to address several of the critics raised. They especially create a framework that should ensure accountability, oversight, transparency and minimization of privacy intrusion.

⁴⁰ European Court of Human Rights, Case of Liberty and others versus United Kingdom, Application no. 58243/00, Strasbourg, 1st July 2008. Available at: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=30&portal=hbkm&action=html&highlight=liberty&sessionid=14127824&skin=hudoc-en>

⁴¹ Cate, F.H., ‘Governing Data Mining: The Need for a Legal Framework’, *Harvard Civil Rights-Civil Liberties Law Review*, Vol. 43, 2008, p. 437.

view that the Fourth Amendment does not limit routine data collection, accessing data from third parties, or sharing data even if illegally gathered. Finally, he surveys the issues that this unregulated access poses for national security and personal privacy, advancing the proposal of a statutory framework based on the work of the numerous public and private commissions that have addressed the issue over the past five years.

2. The growing request of data: Biometrics

Both EU and US have launched, in the last 10 years, initiatives aiming at accessing and processing biometrics. Since 9-11, the reliance on biometrics seems to have grown exponentially. Biometric identifiers are generally supposed to be more reliable than former instruments and they permit an easier form of digitalisation. One of the main programs of biometrics collection is the *United States Visitor and Immigrant Status Indicator Technology* program (US-VISIT). This program was launched in 1996 with the aim of providing a tool to identify visa over stayers. The original purpose was immigration management. However, since the adoption of the USA-PATRIOT Act, it has been endorsed, and redirected to, anti-terrorism functions (Hobbing, P., 2007, p. 5). The US-VISIT requires visitors to the US to submit two biometric identifiers: fingerprints (initially two, actually raised to ten) and a digital photo, as well as a certain number of biographical data (EPIC, 2006, p.12). Biometric data are checked against twenty interfacing government databases, in order to control if the visitor is listed as a criminal or a terrorist. Until 2004, EU Member States participating to the Visa Waiver Program (VWP) were exempted from the scope of US-VISIT. Since then, EU citizens are required to submit their data to the US port of entry. The “in loco” submission is the main difference with the submission procedure of citizens of non-Visa Waiver Program countries, those are requested to submit data at the US consular office (EPIC, 2006, p. 12). The data retention period of data stored in the US-VISIT is established at 75 years. Data are accessible to a high number of US agencies: other DHS components and other law enforcement agencies at federal, state and local level. US-VISIT is generally compared to the EU developed Visa Information System (VIS). VIS will store biographical and biometrics data, digital photo and fingerprints, of visitors applying for a 3 months visa. However, several relevant differences should be underlined: VIS has been conceived and developed as an administrative tool and its main purpose is to support the common visa system. Access to VIS data would not be possible to law enforcement agencies on routine base. Data retention period will be limited to five years.

3. The growing request of data: Electronic System of Travel Authorization

3.1. The introduction of Electronic System for Travel Authorization

On 3 June 2008, the Department of Homeland Security announced the intention to start a new pre-travel authorization program for travellers from Visa Waiver Countries. ESTA’s stated purpose is to mitigate the VWP security risks by obliging VWP citizens to send their data prior to departure, and thus allowing CBP to check those data against several law enforcement databases. While the program has already started on a voluntary base on 1 August 2008, it will become compulsory on 12 January 2009.

The program is addressed to citizens of VWP countries entering the US via air or sea carriers for a maximum period of 90 days. VWP citizens applying from a land border will still continue to use the paper-based form. According to the FAQ of the CBP, the citizens of States that have already signed a VWP Memorandum of Understanding are still excluded from the program, and will require to submit a visa procedure.⁴²

The ESTA application has to be submitted at least 72 hours before departure. The response to such application could be of three kinds: “Authorization Approved”, “Authorization Pending” and “Travel Not Authorized”. Once authorization is granted, it will remain valid for a maximum period of two years, or until expiration of the passport. Once passport expires, a new ESTA application should be submitted.

The ESTA approval will not grant a right of entry into the US territory, but only the right to embark on air or sea carriers.

At present, no cost is planned for ESTA application. It is possible that at a later stage a fee will be required. The submission of the application is done electronically, on a securitised web site. Also third parties, such as relatives or travel agents, would be permitted to enter a request. Data have to be submitted in English, as it was the rule on the paper-based format.

The data requested by ESTA are the same of those requested in the I-94W form, the paper-based form that is currently filled en-route and submitted at the port of entry. While after the official start of the programme the I-94W will be definitely substituted by ESTA, during the transition period, travellers that adhere voluntary to the program will also have to fill the en-route form. Those data include both biographical and travel information.⁴³ Some travel information, such as flight information and

⁴² The EU Member States that have already signed a VWP Memorandum of Understanding with the US are: Czech Republic, Estonia, Greece, Hungary, Latvia, Lithuania, Malta and Slovakia.

⁴³ The Privacy Impact Assessment on ESTA of the DHS Privacy Office lists the data required. They are:

- “Last name, First and Middle Names
- Unique ESTA identifier (provided by CBP)
- Email Address, if available
- Phone Number
- Date of Birth
- Country of Citizenship
- Sex
- Passport Expiration Date
- Passport Number and Issuance City, Country, and Date
- Destination Address, City, State
- Flight Information, if available
- City of Embarkation, if available
- Whether the individual has a communicable disease, physical or mental disorder, or is a drug abuser or addict?
- Whether the individual has been arrested or convicted for a moral turpitude crime, drugs, or has been sentenced for a period longer than five years?
- Whether the individual has engaged in espionage, sabotage, terrorism or Nazi activity between 1933 and 1945?
- Whether the individual is seeking work in the United States?
- Whether the individual has ever been denied a United States visa or entry into the United States or had a visa cancelled? (If yes, when and where?)
- Whether the individual has been excluded or deported, or attempted to obtain a visa or enter the United States by fraud or misrepresentation?
- Whether the individual has ever detained, retained, or withheld custody of a child from a United

destination addresses, as well as biographical information, such as contact data, could be updated after the first ESTA application. However, it is worth to note that ESTA information include also sensitive data such health information and criminal records, as well as data directly or indirectly linkable to third persons, as in the case of destination address.

ESTA information are checked against law enforcement databases, with the aim of assessing possible security risks.

Once the ESTA system will fully replace the paper-based form, the data retention period of ESTA application data will be of 75 years.⁴⁴ This is the same storing period to which paper applications are submitted (DHS CPO, 2008, p. 12).

ESTA application data will be available for data sharing with a wide range of agencies and actors. ESTA application data will be accessed by other DHS components on the base of “routine access”. Furthermore, information may be shared with a large spectrum of agencies.⁴⁵ Finally, data will be sent to air carriers technically able to manage these data.

According to the DHS CPO Privacy Impact Assessment, data subjects’ right of access will be granted, even to foreign nationals, under the Privacy Act. However, it will be submitted to Privacy Act limitations, including the possible non-disclosure of data that are shared with law enforcement agencies (DHS CPO, 2008, p. 19). Individuals can also seek administrative redress under the DHS Traveler Redress Program (TRIP).

3.2. *Three potential concerns raised by ESTA*

The Electronic System for Travel Authorization could seem just an innocuous move from a paper-based system to an electronic, more efficient and technologically updated tool of management. However, it has already encountered some resistance, notably in the EU, where the perception is that ESTA could represent a disguised visa. However, within the scope of this study, it is important to put the accent on other issues raised by the introduction of ESTA, and especially its potential impact on privacy, data protection and security management.

I. Even if it cannot be said that ESTA is in itself a data mining program, its functioning is based on the recourse to existing data mining program, in particular the Automatic Targeting System (ATS) and the Treasury Enforcement Communication System (TECS).⁴⁶ In fact, according to the DHS CPO Privacy Assessment, the delivery of the responses to VWP citizens will automatically result from the screening provided by the mentioned programs (DHS CPO, 2008, p. 5). This implies that

States citizen granted custody of the child?

- Whether the individual has ever asserted immunity from prosecution?” (DHS CPO, 2008, pp.4-5).

⁴⁴ During the transition period and the co-presence with paper-based form, the data will be stored for the same period of validity of the ESTA approval, plus one year plus other 12 years in archive, but still available for retrieval. After this 15 years period, they will be archived under stricter rules of access.

⁴⁵ In particular, ESTA data will be shared with consular offices of the Department of State, on the base of memorandum of understanding, as well as a “appropriate federal, state, local, tribal and 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, or where DHS believes information would assist enforcement of civil or criminal laws” (CBP, 2008).

⁴⁶ The fact that ESTA information will run on ATS seems to confirm that this program is already assessing risk scores to human being, or at least it is doing this since 1 August 2008.

European citizens' data will be, finally, automatically processed before a similar system is applied also to personal data of US citizens. It is worth to remember that even in the frame of the PNR agreements, use of EU citizens' data in the CAPPS II system was delayed. Secondly, it is still not clear how the decision of denying authorization will be taken, if solely on the base of automating processing or with the recourse to human double-checking.

II. ESTA stated purpose of mitigating VWP security risks appears to reinforce the idea that security management is shifting from a state-based perspective to a more individual-based focus. Furthermore, it clearly calls into question the role of the private sector, which continues to be increasingly integrated in the security system surrounding air travelling.

III. The idea that ESTA represents only a move towards a more technologically developed tool of data management could prove misleading. Even if the data are the same of the older, paper-based, form, the inherent possibilities of search, matching and transmission of electronically registered data call for a closer check of data protection guarantees. I-94W form could include sensitive data, and data sharing rules appear to be very flexible. In such cases, data protection safeguards cannot be based only on strong security criteria, but must better address all data protection principles.⁴⁷

3.3. *The proposed EU Electronic System of Travel Authorization*

On 13 February 2008, former Vice-President Frattini, Commissioner for Justice, Liberty and Security, unveiled the new "border package". Both communications aim at improving border management in the EU, especially through the development of new technological instruments. The proposal for a possible set up of an EU Electronic System of Travel Authorization is advanced in the Communication on Preparing the next steps in border management in the European Union.⁴⁸ ESTA is presented as one of three instruments able to improve EU border management. The other two instruments are the establishment of a bona fide traveller's register and the introduction of an entry/exit system.

The description of the future system is merely one paragraph, and it does not provide details on the exact structure, functioning, and features of a possible EU ESTA. According to what is stated in the Communication, ESTA will apply to third country nationals not subject to visa requirements. Potential travellers will be required to submit their data, biographical, passport and travel details, prior to their departure. Requests of authorization will be sent electronically and data could be used "for verifying that a person fulfils the entry conditions before travelling to the EU" (Commission, 2008, p. 9).

The Commission Communication does not state which data will be required, how much time before, if there will be any cost charged to the applicant and which specific rights will be granted on the base of authorization.⁴⁹ Notwithstanding the lack of

⁴⁷ When ESTA will be fully in use, US authorities will be able to access and retain, even for long period, a massive quantity of personal data on EU travellers. For air-travelling, the sum of those data with PNR data could argued to be excessive.

⁴⁸ Commission of the European Union, *Communication from the Commission of the European Union to the European Parliament, the Council, the European Economic and Social committee and the Committee of the Regions, Preparing the next steps in border management in the European Union*, doc. 6666/08, Brussels, 13.2.2008.

⁴⁹ Surely, those questions will be discussed by the feasibility study that the Commission is supposed to launch in 2008 (Commission, 2008, p. 9).

details, it is possible to advance some further hypotheses and some remarks on the possible adoption of this new tool. It could be interesting to note that the Commission Communication stresses that: “[s]ystems must comply with EU data protection rules including the requirements of necessity, proportionality, purpose limitation and quality of data. Particular care should be taken to ensure full compliance with the requirements of Article 16 and 17 of the Directive 95/4/EC on confidentiality and security [...] the study to be launched by the Commission on the possibility of an electronic travel authorisation will also consider the relevant data protection issues arising from such a system” (Commission, 2008, p. 9). Such a statement, in particular the reference to the Data Protection Directive, could imply a foreseen use under the first pillar legal base, therefore, not for security purposes. If this will be the case, the EU ESTA system would strongly differ from the one adopted at US level. However, the possible entry into force of the Treaty of Lisbon could change the present legal-base constraints.

The second remark concerns the timing of the communication. The EU has still not taken a common position on the US introduction of the ESTA regime. Such a public statement on the desire to implement a parallel system in the EU risks undermining any kind of negotiations with the US.

Finally, the Commission Communication seems to confirm the growing tendency towards an international dissemination of similar measures based on data access. This has been the case with PNR and seems to become the case with ESTA.

4. The growing request of data: Travel data

4.1. Overview of the three EU-US agreements and of the ECJ judgement

Passenger Name Records (PNR) contain data requested by an airline company when buying a ticket. Currently, this information can include the passenger’s full name, date of birth, home and work address, telephone number, e-mail address, passport details, credit card details or method of payment, the names and personal information of emergency contacts, as well as details of any special meal requirements or seating preferences or any other similar requests. Although its exact content will depend on the data provided by the data subject, as all the fields are not compulsory. Databases of PNR data are normally hosted centrally, within an international reservation system.⁵⁰

Since the end of 2001, processing of PNR data for security purposes has become a real transatlantic issue. On November 2001, the CBP started to ask, on the base of the 2001 Aviation and Transportation Security Act, international air carriers for access to their passengers’ data⁵¹. As the request seemed to contradict European airlines’ (data

⁵⁰ Few airlines (both in the EU and in the USA) host their own passenger databases; in fact, most ‘outsource’ the processing of their PNR data altogether to third (data processing) parties (for instance, EDS) that ultimately upload airlines’ PNR data to the so-called Global Distribution Systems (SABRE, Galileo, Amadeus, Worldspan), see Hasbrouck E, What’s in a Passenger Name Record, <http://hasbrouck.org/articles/PNR.html>. The issue of, even European, airlines having their data processed by American companies for PNR purposes is one of the least discussed aspects of the PNR scene.

⁵¹ See UK House of Lords – European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement* (HL Paper 108, 5 June 2007, The HL PNR Report), 1-4. More US projects on PNR processing after 9/11, both abandoned and eventually adopted, may be found at the PHR2006 analysis on the USA, under [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559478](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559478)

protection) obligations concerning the personal data they possessed, air carriers were faced with the dilemma of which law to break. Therefore, the European Commission decided to intervene, obtaining at first a provisional suspension of the entry into force of the measure. The following entry into force of the measure and the decisions of most airlines to comply with it finally pushed the Commission to negotiate with the USA an EU-wide solution.

Since then, three agreements have been negotiated. The First Agreement was signed on 28 May 2004 in Washington. Given the decision to select as legal base the first pillar, and thus with the obligation to respect the Data Protection Directive, it was preceded by the issuing of the Decision “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”.⁵²

A couple of months after the First PNR Agreement was concluded, on July 2004, the EP filed two actions in front of the European Court of Justice, each one aimed at the Council’s and Commission’s Decisions, upon which the First PNR Agreement was based. The Court reached its decision two years later, on May 30, 2006⁵³. It did not go into the substance of the EP’s claims, because it found that the First PNR Agreement did not pertain to commercial communications but rather to security matters, hence the legal basis of the First PNR Agreement could not be the Data Protection Directive (that only applies on First Pillar processing), therefore the First PNR Agreement had to be annulled. The Court subsequently set a deadline (September 30, 2006) for a new PNR Agreement to be entered.⁵⁴

Negotiations for conclusion of the Second PNR Agreement indeed began on July 2006 but this time by the Council, because the ECJ Decision prohibited the Directive’s application on PNR data processing. The outcome of the negotiations was a new Interim PNR Agreement that finally entered into force on October 2006. The texts of the 2004 and 2006 agreements were almost identical, the main difference being the choice of the legal base and the relative consequences of a weakening of the position of the Parliament.

The Interim Agreement included also a sunset clause, which obliged the main actors, DHS, Commission and Council Presidency, to maintain the negotiations open in order to conclude a new agreement. Quite surprisingly, negotiations were concluded within the time limits, and on July 2007 a Third Agreement was signed. Difficulties while negotiating the 2007 PNR Agreement from the American perspective were evidently based on the fact that the American side had secured extensive PNR data processing powers under the First and Interim PNR Agreements. The European side, on the other hand, was found in a more complex situation. Given the American request of ever-more data processing powers and its airlines wish to operate in the American market, it also had to bear in mind the Parliament sensitivities⁽⁵⁵⁾, that felt it was again left out of the negotiation process and pressed for a restrictive data protection approach. Perhaps even worse, the European side while negotiating with the USA essentially had no text of reference: the Data Protection Directive being not applicable, and no other standard-setting Third Pillar legislation existing. Finally, the Commission

⁵² Commission Decision 2004/535/EC

⁵³ Joined Cases C-317/04 and C-318/04, 30.05.2006.

⁵⁴ Par. 74, ECJ Decision.

⁵⁵ See, for example, OUT-Law News, European Commission Broke Rules over passenger Data Parliament told, 28 March 2007, at <http://www.out-law.com/page-7912>

announced a relevant initiative only after the Second PNR Agreement was concluded.⁵⁶

4.2. Main features of the 2007 PNR agreement

The Second PNR Agreement is, in fact, composed of three distinct documents: "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"⁵⁷. It is however the exact legal relationship among these three documents, if any, that indeed raises questions.

As far as the Agreement itself is concerned, it expressly constitutes an international agreement, according to Articles 24 and 38 of the Treaty of the European Union. It is, nevertheless, the legal nature of the following "*letter exchange*" that leaves unanswered issues. The, somewhat unique, methodology of the Council to conclude international agreements whose substantial clauses are set in accompanying letters, appears to have been particularly popular during the Summer of 2007: both the SWIFT and the PNR cases were dealt with by the Council and the German Presidency with, essentially, the same legal scheme: in an explicit effort to avoid the standard international agreement format the "creative" solution of "letter exchange" was devised, whereby in both cases letters would be exchanged between the two parties but effectively no single legal text (in the form of an international agreement) would be concluded⁽⁵⁸⁾. At any event, the choice to conclude an international Agreement whose substantial clauses in their entirety are included in "letter exchanges" remains a questionable choice from a European data protection perspective.

As far as its substance is concerned, the Agreement itself is a rather brief text of "structural" drafting. The 2007 PNR Agreement follows thus the rule-making methodology of its predecessors: a broad text incorporated into an agreement is complemented by more "technical" annexes (in the past, the Undertakings, now, the "DHS Letter"), whose "relationship" however to the main text has always been left ambiguous.

The definition of PNR data under the 2007 PNR Agreement is included, as it is the case with all other substantial terms, in the DHS Letter. PNR data now include nineteen (19) fields, ranging from name and date to "available frequent flier and benefit information (i.e., free tickets, upgrades, etc)", or all available contact and payment/billing information⁽⁵⁹⁾. Sensitive personal information (as per the Data Protection Directive's definition) are filtered out, but may be accessed "for an exceptional case" (defined as "where the life of a data subject or of others could be

⁵⁶ A process that began only in late 2007 – early 2008 with an unforeseeable, at least at the time of this paper, outcome (see however a first draft of the Commission's proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes under <http://www.statewatch.org/news/2007/oct/eu-com-pnr-proposal.pdf>, as well as, the relevant EDPS Opinion on the Proposal, issued on December 20, 2007 (available at the official EDPS site).

⁵⁷ Parliamentary Debates, Monday, July 9, 2007, Strasbourg (under <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20070709+ITEM-018+DOC+XML+V0//EN>).

⁵⁸ See EDRI, EDRI, Final Agreements between EU and USA on PNR and SWIFT, at <http://www.edri.org/book/print/1231>.

⁵⁹ See Chapter III, U.S. Letter to EU.

imperilled or seriously impaired”, a far from adequate definition of what ought to mean an emergency).

The purpose of PNR data processing by American authorities is again set in the DHS Letter, in its Chapter I: “DHS uses EU PNR strictly for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law. DHS will advise the EU regarding the passage of any US legislation which materially affects the statements made in this letter”. As it has been clearly stated, combating terrorism is not the only reason why European PNR data may be processed by American authorities; rather than that, a relaxed purpose description covering “*other serious crimes*” is preferred. Attention should also be given to the right withheld by DHS to “*advise*” the EU whenever American legislation affects the DHS Letter; rendering thus its term and undertakings, if any, of temporary term, and reinforcing concerns on its legal nature expressed above (under 1). Further sharing of European PNR data within American administration is possible but restrained (and obviously remains the sole responsibility of the DHS) under Chapter II of the DHS Letter, but European PNR data may be transferred by the DHS to third countries “after consideration of the recipient's intended use(s) and ability to protect the information”.

European PNR data shall be held in American systems for a period of altogether fifteen years: “DHS retains EU PNR data in an active analytical database for seven years, after which time the data will be moved to dormant, non-operational status. Data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk” (Chapter VII, DHS Letter)⁶⁰. This represents an extension of the retention term, from three and a half years under the First and the Interim Agreement. It is worth to note that deletion even after fifteen years remains uncertain: “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”⁶¹. Evidently, DHS is committed to delete the PNR data (if at all) from its own databases; nowhere in its Letter it undertakes to monitor deletion from other “domestic” databases it has already transmitted the data during their fifteen-year retention. Finally, the Second PNR Agreement, in line with its predecessors, provides for its periodic review: “DHS and the EU, will periodically review the implementation of this Agreement, the DHS letter, and US and EU PNR policies and practices with a view to mutually assuring the effective operation and privacy protection of their systems” (Art. 4).

It is finally important to note that the EU side triumphed the extension of redress rights for EU citizens. However, the type of redress procedures available to EU citizens is of administrative and not legal nature.

⁶⁰ The same term was used to clear data collected since the First PNR Agreement, an acute problem for American authorities at the time the Second PNR Agreement was concluded, because under the First and the Interim PNR Agreement it had to delete them already (see below under V.3.2).

⁶¹ See Chapter VII, U.S. Letter to the EU.

4.3. The EU PNR Framework Decision: Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes⁶²

At the same time the last EU-US PNR agreement was concluded, in June 2007, former Vice-President and Commissioner for Justice Liberty and Security declared his intention to present a proposal for a framework decision establishing a EU PNR system⁽⁶³⁾. The framework decision proposal was presented few months later, on 6 November 2007, as part of a package of anti-terrorism measures.⁶⁴

Since the first commission draft, the proposal has already raised several issues, ranging from the choice of the legal instrument to the time-schedule of the proposal, from the scope to the data protection regime. Discussions are still going on within the Multidisciplinary group on organised crime (MDG) and several questions have not yet been settled⁽⁶⁵⁾. Given the relevance of such a proposal, and the European and international impact of such a system in case of approval, it seems important to sketch an outline of its main provisions and then discuss some of the main issues raised.

4.4. Content of the EU PNR proposal

The following presentation is based on the last public version of the EU-PNR framework decision, document no. 7656/3/08 REV3, released on 19 June 2008.

The objectives of the proposal (art. 1) are making available by air carriers the PNR data of passengers to Member States, for the processing and exchanging the data by competent authorities. The main purposes are the prevention, investigation and prosecution of terrorism offences and serious crime (organised crime in the previous versions). The scope of the proposal is, at present, limited to cover international flights, therefore excluding intra-EU flights and other modes of transports. The purpose seems to exclude the use of PNR data for immigration management. However, all those point are still under discussion in the MDG, with some Member States asking for a major flexibility and the possibility to process data for other purposes or/and related to other modes of transports, notably sea carriers and trains.

Article 3 of the proposal establishes the Passenger Information Unit (PIU), which is supposed to become the national public authority responsible “for the prevention, detection, investigation or prosecution of terrorist offences and serious crime”. The PIU will be charged of two key tasks: collecting the PNR from air carriers (art.3(2)) and processing the data in order to carry out a risk assessment of the persons, identifying who will requires further examination by competent authorities. The purposes of analysis and risk assessment is four-fold: identify persons who are, or may be, involved or associated to terrorist and serious crime offences; create and

⁶² Council of the European Union, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, doc. 7656/3/08 REV3, Brussels, 19 June 2008.

⁶³ Mr. Frattini declaration is quoted by Statewatch on 15 July 2007: www.statewatch.org/news/2007/jul/03eu-pnr.htm

⁶⁴ Together with the EU PNR proposal, were tabled measures dealing with the criminalization of terrorist training, recruitment and public provocation to commit terrorist offences, the prevention of the use of explosives by terrorists, Commission of the European Communities, *Fight Against Terrorism: stepping up Europe’s capabilities to protect citizens against the threat of terrorism*, IP/07/1649, Brussels, 6 November 2007.

⁶⁵ The EU PNR proposal had been preceded by a Commission inquiry among Member States, private stakeholders and data protection authorities, with the scope of tailoring the proposal on the most shared policy option. Officially, the vast majority of Member States supported the initiative, and some of them advanced their will to extend the scope to other modes of transport in the mid-run.

update risk indicators for the assessment; provide intelligence on travel patterns and other trends; to be used in criminal investigations and prosecutions.

Even if the Committee set up by the same proposal will identify recommendations for common general criteria, criteria and guarantees concerning risk assessment will be provided under national law.

Two kinds of information can be exchanged among PIUs: analytical information flowing from PNR data as well as PNR data itself. The scope of these exchanges varies on the type of data: ad hoc and motivated for analytical information, *ad hoc* and/or routine (“regular basis”, art. 7(2)) for raw PNR data.

Air carriers will be obliged to make available PNR data at two different moments: 24 hours before the departure and immediately after flight closure. Nevertheless, in specific and exceptional cases, PIU can request access to data even prior to the 24 hour standard (art. 5(3)). Data shall be, compulsory, transmitted according to a “push” method, that is to say by sending data to PIUs, when air carriers databases are established in a Member States. When this is not the case and they do not have a “push” technical architecture, data should be made accessible to PIUs by the “pull” method, thus providing PIUs the capability to directly extract the data from the databases.

PNR data covered by the proposal of Framework Decision are 19, covering biographical, contact and travel data. They are the same categories of data covered by the EU-US agreement, as well as the EU-Australia agreement. As in the other two cases, among the categories is present the “general remarks” field. This is an open field, where travel agents could enter sensitive data. The proposal excludes formally this kind of information, however it is still not clear if and how it could be possible to filter this field.

Chapter III, articles 11 and 12, establishes the *ad hoc* frame of data protection. Such a frame aims to respond to the main principles of transparency and documentation; information for data subjects; protection of sensitive data; rights of access, rectification, erasure and compensation, judicial remedies, confidentiality and security of the process. It also establishes an oversight system provided by national, “completely” independent authorities, responsible for the application of national provisions pursuing from the framework decision. Such authorities should be endorsed of investigative and intervention powers, as well as the capacity of engaging in legal proceedings. They shall hear the claims lodged by any person, and thus including foreigners.

This frame applies only to data accessed, processed and exchanged by PIUs. National laws, in line with the present scope of the Data Protection Framework Decision that does not include “national” processing, will cover the handling of PNR data by law enforcement authorities.

The data retention period of PNR data amounts to a total of thirteen years, but it is split in two phases. Data will be initially kept in a database for a period of five years, starting from the transfer to the initial PIU. This first phase will be followed by a second period of eight years, where PNR will be stored in an “inactive” database, where access is submitted to stricter rules and for exceptional circumstances. After this period, PNR data shall be deleted.

Article 8 of the proposal defines the rules that apply to transfer of PNR data and related analytical data to law enforcement authorities of third countries. Five conditions must be satisfied. The use purpose of data transferred should be restricted

of prevention, detection, investigation or prosecution of terrorism offences and serious crime, and the receiving authorities should be responsible of those tasks or the of their execution. The third condition applies to data already obtained by another Member State: in those cases of on-ward transfer, the prior consent of the originating Member State should be obtained.

Finally, two conditions are at the charge of the third country: it must ensure an adequate level of protection “of the intended processing” (art. 8(1)(d)) and shall not transfer the data to another third country without the express consent of the Member State.

4.5. Two considerations on the proposed EU-PNR system

Since its presentation, the proposal has already raised several questions. In order to remain within the scope of this study, and bringing added value, it seems important to focus on two main themes: data protection and proportionality.

I. The decision to develop *ad hoc* data protection provisions within the EU PNR Framework Decision seems to confirm the idea, and the political will, to build a sector-based system of data protection. If the proposal will be adopted, it will contribute with another piece to the present, complex, puzzle. Moreover, such *ad hoc* framework shows all the difficulties of this approach because will cover not the data *per se*. Provisions on data protection will cover only the exchange and the processing of data operated by a specific type of actor: the Passenger Information Unit. Therefore, in the simplest case, the same PNR will be covered by at least two different set of rules, the Framework Decision and national law, not to mention data protection rules that apply to air carriers and booking services. In case of exchange of PNR data, also the national rules of other Member States will apply. Such a complex picture contributes to underline the possible shortcoming of not extending the scope of the Data Protection Framework Decision to national processing.

In case of exchange with a third country, PNR data will be submitted to the receiving country standards. In fact, article 8 of the proposal only bounds the authorities of a third country to use the PNR data from a purpose point of view, and prior consent is sought only for onward transfer. Also concerning data protection and relations with third countries, a crucial provision is the request of an “adequate level” of protection. However, such adequacy criterion is limited to the degree of protection of a specific type of processing, and does not cover the entire data protection system of the third country. It is not clear who will be charged of the responsibility to assess such adequate level, and how to investigate and avoid further processing. On the other hand, it is very probable that countries have PNR agreements with the EU, such as US, Canada and Australia, will be automatically recognised adequate by virtue of the same agreements.

The *ad hoc* data protection frame of the framework decision seems reassuring on the fact that profiling will not be based on sensitive data: “no risk assessment criterion shall be based on a person’s race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual orientation” (art. 3(3)). However, there is no prohibition on the processing of these data *per se*, if the processing is not “solely” based on persons’ sensitive data.

II. The second consideration is that the EU-PNR system would introduce a data mining program, based not only on comparison with established lists, but on risk assessments and pattern recognition. This would be a major step in the development

of European measures of security and should require a clear assessment of its added value in terms of security and privacy impact. At present time, this would be difficult to check, given the lack of public documentation on the outcomes. It is important to remind that, according to the Slovenian Presidency notes, some Member States favour a proposal that set up limitations understood as minimum standards, “which would allow them to give a wider scope to their domestic legislation than will be required under EU law”.⁶⁶ In particular, the limitations that are under discussion are: modes of transport, geographical scope and purpose limitation. All these limitations directly influence the balancing of proportionality, and the very nature of the measure.

5. The growing request of data: Banking data

5.1. Access to banking data: SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a Belgian based cooperative that provides a worldwide service of financial messaging. SWIFT stores messages for 124 days in their two databases, one in Belgium and the other, the mirror, in the US. Notwithstanding its crucial role in the international financial system, SWIFT became even more famous by the end of June 2006.

After 9-11, the United States Department of the Treasury (UST), issues numerous subpoenas requiring access to messages stored in SWIFT’s US database. SWIFT negotiated, privately, with the UST a certain level of guarantees and accepted to comply with UST subpoenas. Both the issuing of subpoena and the effective availability of SWIFT data to the UST remained secret until the end of June 2006, when press coverage revealed the transmission of data.

The European Commission, the Belgian government and the data protection authority reacted, in order to assess if SWIFT had broken EU law, in particular the Data Protection Directive. The European Parliament expressed its concern in a resolution, on 6 July 2006⁽⁶⁷⁾ and disapproved the conduction of secret operations on US territory that could affect the privacy of EU citizens.

Finally, the opinion of the Belgian DPA highlighted the responsibilities of SWIFT of not complying with EU and Belgian law on data protection, and defined SWIFT as a data controller (according to art. 2, Directive 95) and not a merely processor. The article 29 Working Party opinion confirmed such a view, stating 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”⁽⁶⁸⁾.

What happened next is very interesting for the aim of this study. At the beginning of 2007, the German Presidency decided to negotiate with the US not only the new PNR agreement, but also a new agreement establishing a legal framework for UST access

⁶⁶ Council of the European Union, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, doc. 7656/3/08 REV3, Brussels, 19 June 2008, p. 2.

⁶⁷ European Parliament resolution on the interception of bank transfer data from SWIFT system by the US secret services (P6_TA-PROV(2006)0317).

⁶⁸ Article 29 Data Protection Working Party, *Opinion 10/2006 on the processing of personal data by Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, doc. 01935/06/EN WP128, Brussels, 22 November 2006, p. 26.

to SWIFT data. The 22 June 2007, merely one year after the revelation of the “SWIFT affaire”, the Commission and the Council, concluded an exchange of letters, representations, with United States Department of the Treasury⁶⁹). In its first letter, the UST describes the aims, the scope and the fundamental principles underlying its Terrorism Finance Tracking Program. The UST clarifies also the legal base of the subpoena instrument and specifies data protection guarantees applied to the processing of data received by SWIFT. Even if it tries to address all the data protection principles and European concerns, the guarantees appear to focus more on access control and computer system security than on data subjects’ rights. EU answer letter defines the new position of SWIFT and of its client financial institutions as “in compliance with their respective legal responsibilities under European data protection law” as soon as they will provide information to their clients that personal data will be transmitted in the US and, regarding SWIFT, will respect Safe Harbour principles.⁷⁰

SWIFT had decided to sign up to join the Safe Harbour agreement in April 2007 (González-Fuster, G., et al., 2008, p. 197).

The “SWIFT affaire” reaffirms the increased collaboration, more or less voluntary, of private sector and law enforcement agencies. It raises again the questions of purpose and use limitation, proportionality and transparency. Access to SWIFT has proved to be “extraordinarily valuable in combating global terrorism and its financing” (Council, 2007, p. 8), but no figures are joined to this UST statement.

The lack of transparency appears particularly worrying and does not contribute to ease the transatlantic dialogue, neither to the possibility of data subjects to enforce their rights.

Finally, the SWIFT exchange of letters seems to confirm the piece-meal approach to data protection in the field of law enforcement, security and transatlantic relations (De Hert, P., De Shutter, B., 2008, pp. 331-333).

5.2. Three considerations on PNR and SWIFT

The PNR and SWIFT agreements have raised, and continue to raise, several questions and concerns. Remaining within the scope of this study, it seems worth to focus on three issues that could, and should, affect any future work on further transatlantic agreement.

I. The first issue relates to the very purpose of the PNR processing. The purpose sought in processing “transatlantic” PNR is “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 the crimes described above”⁽⁷¹⁾. As stated before, an even wider purpose is currently part of the discussions on the EU-PNR proposal, with countries requiring the flexibility to process PNR for immigration purposes.

Claims on the effectiveness of the PNR processing have failed, until present, to publicly prove the validity of such a tool. Without an impact assessment on the effectiveness of such massive processing of personal data, it would be difficult, if not

⁶⁹ Council of the European Union, *Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes – “SWIFT”*, doc. 10741/2/07 REV2, Brussels, 29 June 2007.

⁷⁰ *Idem*, p. 2 of the Annex.

⁷¹ Par. (3), Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection, 2004, published in the US Federal Register Vol. 69, No 131, p. 41543.

impossible to assess the principle of proportionality. When looking at publicly available success rates of similar measures, such as the UK pilot project Semaphore, the cases mostly cover law enforcement purposes rather than anti-terrorism purposes⁽⁷²⁾.

The quantification of data on success rate of security measures could become a precious tool in assessing their proportionality and their limits. It can also offer an important indicator on how to develop more efficient instrument with a reduced impact on liberties.

II. The second issue concerns the legal status of the current EU-US agreement, especially concerning the Exchange of Letters. Apart from more juridical problems that have been addressed in other scientific articles⁽⁷³⁾, it highlights the US tendency, and a certain EU compliancy, to avoid the conclusion of clear international agreements. In fact, a similar instrument has been chosen also to fix the “SWIFT affaire”, and according to the finding of the High Level Contact Group, the US are not reluctant to follow the same line also in the future.

Therefore, in case of the negotiation of a data protection transatlantic agreement, it should be important to understand the relations between the new instrument and existing instruments.

III. The third issue has been raised by the ECJ judgement. The pillar structure of the EU has already been discussed as a major obstacle to a more uniform approach to data protection in the EU. The pillar structure also makes international negotiations more difficult.

It is important to fully involve the Parliament in the negotiations, and to include existing data protection authorities such as the EDPS or a representation of the Art.29 Working Party.

⁷² Letter from Ms Meg Hillier MP Parliamentary Under Secretary of State to Vice President Franco Frattini, European Commission, Annex to the House of Lords – European Union Committee, *The Passenger Name Record (PNR) Framework Decision – Report with Evidence*, London, 11 June 2008, pp. 7-8 annex.

⁷³ Papakonstantinou, V. and De Hert, P., “The PNR Agreement, European data protection and transatlantic anti-terrorism co-operation. No firm human rights framework on either side of the Atlantic?”, forthcoming.

Part Three – The work of the High Level Contact Group on Data Protection and the move towards a Transatlantic Data Protection Agreement

On 28 June 2008, the New York Times published an article stating that US and EU are close to conclude an agreement on transatlantic flow of personal data.⁷⁴ It focused on the content of an “internal report” jointly drafted by both sides’ negotiators, aiming at finding common principles of data protection and thus ensuring a smooth flow of information among parties. The New York Times article referred also to the recent difficulties in data sharing cooperation and to the main issues still under discussion, notably the possibility of allowing non-US citizens to pursue legal redress. Finally, it took into consideration the two available alternatives, their consequences and their institutional supporters, as well as the position of non-state actors, such as civil liberties groups and private companies.

The New York Times article had a great echo within the EU, and it has been quoted, discussed and even translated by several European newspapers.⁷⁵ The “internal report” discussed resulted to be the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection. According to the accompanying Presidency note, the document was supposed to be submitted at the EU-US Summit of 12 June 2008.⁷⁶ In fact, the declaration of this Summit refers to the report and seems to build on it, stating a common preference for the conclusion of “a binding international agreement that addresses all the issues identified in the High Level Contact Group report”.⁷⁷

Given the high relevance of such report, even within the limits of the few public available documents, it seems worth to focus on its content and some of the potential challenges raised. Therefore, the next sessions of this chapter will explore the context and the goal of the works of the High Level Contact Group, the principles agreed and the pending questions identified.

1. The context and the goal of the works of the High Level Contact Group

According to the Draft Final Report, the informal High Level Contact Group was established by decision of the EU-US JLS Ministerial Troika on 6 November 2006.

⁷⁴ Savage, C., “U.S. and Europe Near Agreement on Private Data”, *New York Times*, 28 June 2008. The article is also available online at: <http://www.nytimes.com/2008/06/28/washington/28privacy.html>

⁷⁵ See amongst others: Goldirova, R., “EU and US near deal on confidential data sharing”, *EU Observer*, 30 June 2008, available at: <http://euobserver.com/9/26416>; De Rituerto, R.M., “La UE y EE UU se acercan a un pacto sobre datos privados”, *El País*, 29 junio 2008, available at: http://www.elpais.com/articulo/internacional/UE/EE/UU/acercan/pacto/datos/privados/elpepiint/20080629elpepiint_7/Tes; Savage, C., “Usa e Ue pronti all'accordo viaggiatori senza privacy”, *Repubblica*, 29 giugno 2008, available at: <http://www.repubblica.it/2007/12/sezioni/esteri/usa-database-biometrico/iaccordo-usa-ue-voli/iaccordo-usa-ue-voli.html>; Traynor, I., “New pact would give EU citizens' data to US”, *The Guardian*, 30 June 2008, available at: <http://www.guardian.co.uk/world/2008/jun/30/eu.privacy>.

⁷⁶ However, at present it is still public available only the draft version of the HLCG Final Report, which brings the date of 28 May 2008, and was rendered public on 24 June, two days before the New York Times article.

⁷⁷ Council of the European Union, *2008 EU-US Summit Declaration*, doc. 10562/08 (Presse 168), Brdo 10 June 2008, p. 10.

The European Parliament was informed of the establishment of such group at the LIBE meeting of 19 December 2006.⁷⁸

The goal is twofold: to enhance transatlantic cooperation in data and information sharing while ensuring data protection and privacy rights.⁷⁹ The identification of common principles, “acceptable as minimum standards when processing personal data for law enforcement purposes”,⁸⁰ has been identified as the best solution to achieve such a twin goal.

The composition of the High Level Contact Group is based on senior officials coming from both EU and US institutions: the Commission, the Council Presidency, the US Departments of Justice, Homeland Security and State. According to the available documentation, no Member of the EP has participated to the works of the High Level Contact Group,⁸¹ neither officials of the EDPS or of national data protection authorities. No data are available on the direct involvement of US Senate or Congress representatives. It is worthy to note that the Privacy Office mentions, in its Annual Report to the Congress 2007, its role of resource and participant in the High Level Contact Group discussions.⁸²

Since its formation in November 2006, the High Level Contact Group has met at least 4 times, alternatively in the US and in Europe: on 26 February 2007 in Washington, on 4/5 April 2007 in Berlin, on 2 November 2007 again in Washington, on 12/13 March 2008 in Brdo. The High Level Contact Group has been progressively charged not only of finding common ground on data protection and privacy principles, but also to advance policy options.

2. The common principles

The Draft Final Report of the High Level Contact Group lists 12 common principles of data protection and privacy for law enforcement purposes.⁸³ These principles are:

1. Purpose Specification/Purpose Limitation;
2. Integrity/Data Quality;
3. Relevant and Necessary/Proportionality;
4. Information Security;
5. Special Categories of Personal Information (sensitive data);
6. Accountability;
7. Independent and Effective Oversight;
8. Individual Access and Rectification;
9. Transparency and Notice;
10. Redress;

⁷⁸ Council of the European Union, *EU-US High Level Contact Group on Data Protection and Exchange of information – Future proceedings*, doc. 6780/08, Brussels, 22 February 2008, p. 3.

⁷⁹ “The goal of the HLCG was to explore ways that would enable the EU and the US to work more closely and efficiently together in the exchange of law enforcement information while ensuring that the protection of personal data and privacy are guaranteed”, doc. 9831/08, p. 2.

⁸⁰ doc. 9831/08, p. 3.

⁸¹ However, a February 2008 note of the Slovenian Presidency underlines the fact that “certain Parliament Members have occasionally asked to be informed of the progress of works in the HLCG”.

⁸² Department of Homeland Security – Chief Privacy Officer, *Privacy Office Annual Report to the Congress*, Washington, June 2007, p. 46.

⁸³ doc. 9831/08, p. 4 and pp.11-14.

11. Automated Individual Decisions;
12. Restrictions on Onward Transfers to Third Countries.

According to the Annex to the Draft Final Report, a common language has been developed for those principles. However, the High Level Contact Group itself introduces some remarks to such common language. The first series of specifications concerns principles no. 7 and 9. In fact, Independent and Effective Oversight has to be understood as the accomplishment of the desired effect rather than a parallel implementation of the same principle. Transparency and Notice has to be understood as “the information that should be made available to data subjects”, and national laws will determine the modalities of information and their limitations. However, the most important remark of the High Level Contact Group concerns the redress principle. Even if both sides share the idea that data subjects must have an effective remedy of any redress procedures, there are strong differences in the two legal systems concerning access to legal remedies. As discussed before, the Privacy Act definition of individual excludes non US-citizens or aliens without a permanent residence permit.

The issue of redress seems quite crucial: on one side, and especially the European one, it could undermine the credibility of a transatlantic agreement. On the other side, it pushes for the adoption of new legislation on the US side.

3. Five pending questions, High Level Contact Group policy options and previous position of the European Parliament

The High Level Contact Group has also identified other five pending issues that, even if pertinent to transatlantic relations and recent negotiations’ experience, are not addressed in the mentioned common principles.⁸⁴ For those issues no common language has been found, and the High Level Contact Group recommends including them in the next negotiation package.

Those issues are:

1. Consistency in private entities’ obligations during data transfers;
2. Equivalent and reciprocal application of privacy and personal data protection law;
3. Preventing undue impact on relations with third countries;
4. Specific agreements regulating information exchange and privacy and personal data protection;
5. Issues related to the institutional framework of the EU and US.

Finally, the High Level Contact Group advances two main policy options in order to transfer such exploratory works into effective outputs: the conclusion of a binding international agreement or the choice for non-binding instruments, including “soft law” and political declaration. The first option, the binding agreement, is agreed to be the best solution. It offers the best answer to the twofold goal of the HCLG, and in general of transatlantic negotiations on data protection, providing legal security and data protection and thus paving the way to an ever increasing exchange of data and information. Given the impossibility to cover under a single agreement the protection of all kinds of data, such as a mutually trusted framework would facilitate any other

⁸⁴ doc. 9831/08, p. 7 and p. 14.

“future agreements relating to the exchange of specific law enforcement information that might arise between the EU and the US”.⁸⁵

However, this policy option presents several problems for the US, especially in the case that further legislation should be required, as for extension of redress rights to EU citizens and the relative amendment of the Privacy Act. On that base, such an international agreement risks to exit the executive Presidential competencies and necessitates the approval of the US Senate.⁸⁶ Obviously, the recourse to soft law would offer less legal certainty and security.

Even if the European Parliament has not directly participated to the High Level Contact Group, it appears to have already expressed a preference for the conclusion of an international agreement. In its resolution on the fight against terrorism, the Parliament “reaffirms the importance of cooperation with third countries in the prevention of and the fight against terrorism, and observes that the US is an essential partner in this field; considers that a common legal framework for police and judicial cooperation, with special emphasis on the protection of fundamental rights, especially of personal data, should be defined between the EU and the US, via an international agreement, ensuring appropriate democratic and parliamentary scrutiny at national and EU level”.⁸⁷ The preference for an international agreement, yet expressed some months before the conclusion of the works of the High Level Contact Group, seems to find further support in the last report of the EU Counter-Terrorism Coordinator. In its report to the Council on the Implementation of the EU Counter-Terrorism strategy, he states that “it would seem that a legally binding EU-US agreement (to be negotiated on the basis of the Lisbon Treaty) would offer the best guarantees in terms of both data protection and a sustained intensification of exchange of law enforcement data”.⁸⁸

⁸⁵ doc. 9831/08, p. 8.

⁸⁶ doc. 9831/08, p. 9.

⁸⁷ European Parliament, *European Parliament resolution of 12 December 2007 on the fight against terrorism*, doc. P6_TA(2007)0612, Strasbourg, 12 December 2007.

⁸⁸ Council of the European Union, *Implementation of the EU Counter-Terrorism Strategy – Priorities for further action*, doc. 9417/08, Brussels, 19 May 2008.

PART FOUR –FINAL CONSIDERATIONS

1. EU and US: Partners with common principles but different attitudes?

-The Constitutional protection of rights is organised differently within the EU and the US. The right to privacy in the US is recognised as a constitutional right, as the Court has highlighted in the case *Griswold v. Connecticut*. However, the scope and weight of such a protection do not seem to meet European standards. When it comes to personal data protection, there is no recognition as a constitutional right in the US, and the scope and weight of data protection do not seem to meet European standards.

On the other side, the EU is moving towards solid constitutional recognition of a right to privacy and a right to have personal data protected, including the right to be assisted by independent data protection supervisory authorities.

It is also important to recall that data protection in the US is organised at the level of federal and state law. Different States offer different levels of protection, including cases in which the laws and instruments of data protection seem particularly forceful, as for California.

- A possible image of the US-EU systems seems to be the chiasm: omnibus legislation in the EU with regards to private sector but piece meal approach in the third pillar; piece meal approach in the private sector in the US but a sort of omnibus legislation, the Privacy Act, covering government processing of records. This image is still valid although new legislative developments are of a nature to blur the picture. This is particularly true on the EU side, where there is a move towards a more omnibus framework in Justice and Home Affairs, with the prospective adoption of the Data Protection Framework Decision. While the Framework Decision risks not addressing all the problems, the European Parliament amendments appear to fix the main flaws and strengthen its provisions.

- The Privacy Act of 1974 remains the main legal framework protecting personal data held by the public sector in the United States. Its very existence, compared to the lack of an EU wide comparable legal instrument, together with the wording of the Fourth Amendment, has pushed several commentators to claim that the main focus and concern of US privacy legislation is the control of government data management and has pushed others to consider this Act as the best scheme protecting the “liberty” of its citizens. This study has highlighted several shortcomings in the 1974 regulation (and this independently from the shortcomings resulting from the piece-meal, sector-based data protection legislation covering the private sector). Three differences appear particularly relevant from a European point of view.

1. The Privacy Act does not protect individuals that are neither US citizens nor permanent residents. Such a lack of protection represents one of the main concerns for any transatlantic negotiation.
2. The lack of structurally independent data protection supervisory authorities in the US, represents, certainly from a European perspective, a weakness of the system especially in time of rapid technological development.

3. Finally, the lack of a solid legal basis for the principle of minimization in US law represents a third important shortcoming in US data protection in the context of increasing dissemination of personal data in everyday life.

-Several North-American scholars have highlighted the problems generated by the lack of structurally independent authorities, including those set up in the area of JHA such as the DHS Privacy Office and the President's Civil Liberties and Privacy Oversight Board. US privacy agencies lack powers to investigate and sanction privacy violations. Equally there is no indication that the system of legal redress before the court functions in a satisfactory manner. It is therefore useful to stress that the need for a supervisory authority has been internationally recognised, not only in text from the EU and the Council of Europe, but also by the United Nations in principle eight of the Guidelines for the Regulation of Computerised Personal Data Files, adopted by resolution 45/95 of the General Assembly on 14 December 1990. The need for data protection authorities as a principle is rarely questioned,⁸⁹ and a less than well-performing privacy office on behalf of the US therefore seems to be non-negotiable.

2. Lessons learned from case-studies analysis

On the base of the analysis of the cases-study, it seems possible to highlight some specific features of the most recent security measures. Among others, these appear as particularly important:

1. Security measures are increasingly based on the involvement of the private sector (PNR, SWIFT);
2. They rely on the development of "invisible" practices of analysis and surveillance, such as risk assessment, profiling and comparison (ESTA, PNR, SWIFT);
3. Even if it cannot be said that ESTA is in itself a data mining program, its functioning is based on the recourse to existing data mining programs.
4. There is a quite paradoxical relation between data mining and data protection principles, but granted that data mining programs respect the requirement of legality and are based on accessible regulations that give the subject an indication about the purpose and characteristics of the data mining program, there does not seem to be a principled objection against pattern-based data mining provided that technological and legal safeguards are foreseen.
5. Different countries, and thus different legal systems, promote and adopt similar or parallel security measures based on data access (PNR, ESTA).
6. These features offer an occasion to underline the peculiarities and importance of new challenges in privacy and data protection. Within such context, it is hard to maintain a clear distinction between data protection in the private sector and in the public sector. Data collected for one purpose could become, *per se*, data process-able for other purposes and in a different field. This raises important questions on purpose limitation and data minimisation. It also highlights the crucial importance of legal instruments able to both blocking illegitimate use of data and channelling the legitimate use of powers.

⁸⁹ For a defence of their relevance, see: Flaherty, David H. (1989), *Protecting Privacy In Surveillance Societies*, Chapel Hill: University of North Carolina Press

3. Which possible way forward?

With respect to the possible conclusion of a transatlantic binding agreement on data protection, the European Parliament (EP) should support and participate directly to the negotiations of a binding agreement. The EP must also obtain to be advised by the EDPS or the Art.29 Working Party, as it is happening in the US, where the Chief Privacy Officer has been already integrated to the High Level Contact Group.

The aim of the negotiations should be to ensure redress rights to European citizens, and the possibility of being represented by their Data Protection Authority. Such a possibility could significantly address the negative effects of self-help procedures: financial and time constraints as well as the generally limited knowledge of a foreign legal system.

Not only the EP need to be fully involved in the conclusion of an agreement on data exchange between the EU and the US and follow up the works of the High Level Contact Group, but it would be important also to invite the US Congress and Senate to participate as well. This could become particularly important in case legislation changes should be needed on the US side, especially to extend the protection of the Privacy Act in order to include EU citizens.

If there will be a binding agreement, the issue of adequacy could be put aside. Therefore, it will remain the need for maintaining clear instruments of canalisation of legitimate power and of blockage of illegitimate use.

In the follow-up of the High Level Contact Group works, it seems important to avoid the conclusion of a non-binding instrument. On the contrary, given its relevance within the US system, EU negotiations need to address the scope of notions such as “personal data” and the need to incorporate principles such as data minimization, as well as the flaws for non-US citizens in obtaining legal redress.

On the short term, it seems important to obtain access to the documentation produced in the framework of the High Level Contact Group works, especially studies and reports, in order to be able to build on what has already been done. It is crucial that the agreement addresses the new challenges posed by new security measures, in order to a forceful frame of reference for the coming years.

REFERENCES

LEGISLATION – EUROPE

- Article 29 Data Protection Working Party, *Opinion 10/2006 on the processing of personal data by Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, doc. 01935/06/EN WP128, Brussels, 22 November 2006.
- Charter of Fundamental Rights of the European Union, OJ C364, 18.12.2000, pp. 1-18.
- Commission of the European Communities, *Fight Against Terrorism: stepping up Europe's capabilities to protect citizens against the threat of terrorism*, IP/07/1649, Brussels, 6 November 2007.
- Commission of the European Union, *Communication from the Commission of the European Union to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Preparing the next steps in border management in the European Union*, doc. 6666/08, Brussels, 13.2.2008.
- , *Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States-Bureau of Customs and Border Protection*, OJ L235, 06.07.2004, pp. 11-22.
- Commission de la Protection de la Vie Privée, *Examen du caractère adéquat ou non du niveau de protection offert par le "Privacy Act" américain de 1974, conformément à l'article 25 de la directive 95/46/EC*, Avis N° 34/98, 14 décembre 1998.
- Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950.
- Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, Strasbourg, 8 November 2001.
- , *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS no. 108, Strasbourg, 18 January 1981.
- Council of the European Union, *2008 EU-US Summit Declaration*, doc. 10562/08 (Presse 168), Brdo 10 June 2008.
- , *Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, doc. 9260/08, Brussels, 24 June 2008.
- , *Implementation of the EU Counter-Terrorism Strategy – Priorities for further action*, doc. 9417/08, Brussels, 19 May 2008.
- , *EU-US High Level Contact Group on Data Protection and Exchange of information – Future proceedings*, doc. 6780/08, Brussels, 22 February 2008.
- , *EU-US informal JHA senior level meeting (09-10 January 2008, Ljubljana)*, doc. 5172/08, Brussels, 18 January 2008.
- , *Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes – "SWIFT"*, doc. 10741/2/07 REV2, Brussels, 29 June 2007.
- , *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, doc. 7656/3/08 REV3, Brussels, 19 June 2008.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31–50.
- 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 L 201, 31.7.2002, pp. 37–47.

- European Court of Human Rights, Case of Liberty and others versus United Kingdom, Application no. 58243/00, Strasbourg, 1st July 2008.
- European Court of Justice, European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04), Joined cases C-317/04 and C-318/04. European Court reports 2006 Page I-04721.
- European Parliament, *European Parliament resolution of 12 December 2007 on the fight against terrorism*, doc. P6_TA(2007)0612, Strasbourg, 12 December 2007.
- , *European Parliament resolution on the interception of bank transfer data from SWIFT system by the US secret services*, doc. P6_TA-PROV(2006)0317.
- European Parliament – LIBE Committee, Report on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [16069/2007 - C6-0010/2008 - 2005/0202(CNS)].
- European Data Protection Supervisor – EDPS, *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 (COM (2005) 475 final)*, OJ C 47, 25.02.2006, pp. 27-47.
- , *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*, OJ C91, 26.04.2007, pp. 9-14.
- , *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*, OJ C139, 23.06.2007, pp. 1-10.

LEGISLATION – UNITED STATES

- Appropriate Tools Required To Intercept and Obstruct Terrorism Act (USA-PATRIOT Act) Pub. L. No. 107-56, 2001.
- Bill of Rights, 1789.
- Children’s Online Privacy Protection Act, Pub. L. No. 106-170, 15 U.S.C. §§ 6501-6569, 1998.
- Electronic Communication Privacy Act, 18 U.S.C. §§ 2510-2522, 2701-2709, 1986.
- Fair and Accurate Credit Transactions Act, Pub. L. No. 108-159, 2003.
- Foreign Intelligence Surveillance Act (FISA) 50 U.S.C. §§ 1801-1811, 1978.
- Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 15 U.S.C. §§ 6801-6809, 1999.
- Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 1996.
- Homeland Security Act, 6 U.S.C. § 222, 2002.
- Intelligence Reform and Terrorism Prevention Act (IRTPA), Pub. L. No. 108-458, 2004.
- Privacy Act, 5 U.S.C. § 552a, 1974.
- Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711, 1988.

Case-law

- Griswold v. Connecticut*, 318 U.S. 479, 1965.
- Katz v. United States*, 389 U.S. 347, 1967.
- Kyllo v. United States*, 533, U.S. 141, 2000.
- Schmerber v. California*, 384 U.S. 757, 767, 1966.
- Smith v. Maryland*, 442 U.S. 735, 1979.

BIBLIOGRAPHY

- Bignami, F., 'European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data mining', *Boston College Law Review*, Vol. 48, 2007a, pp. 609-698.
- , *The U.S. Privacy Act in Comparative Perspective*, Contribution to the European Parliament Public Seminar 'PNR/SWIFT/Safa Harbour: Are Transatlantic Data Protected?', 26 March 2007b. Available at: http://www.europarl.europa.eu/hearings/20070326/libe/bignami_en.pdf
- Birnhack, M.D., 'The EU Data Protection Directive: An Engine of a Global Regime', *Computer Law & Security Report*, Vol. 24, No. 6, 2008.
- Birnhack, M.D. and Elkin-Koren, N., 'The Invisible Handshake: The Reemergence of the State in the Digital Environment', *Virginia Journal of Law and Technology*, Vol. 8, 2003, pp. 2-44.
- Blok, P., 'Protection des données aux Etats-Unis', Chapitre 1, Title IV in De Hert, P. (Ed.), *Manuel sur la vie privée et la protection des données*, Brussels, Ed. Politéia, feuillets mobiles, mise à jour No. 7 (2001), pp. 3-40
- Cate, F.H., 'Governing Data Mining: The Need for a Legal Framework', *Harvard Civil Rights-Civil Liberties Law Review*, Vol. 43, 2008, pp. 435-489.
- Cavoukian, A., *Data Mining: Staking a Claim on Your Privacy*, Information and Privacy Commissioner, Ontario, 1998.
- Consultative Committee of the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data, *Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee (T-PD)*, Strasbourg, 13-14 March 2008.
- De Hert P. and Gutwirth, S., 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, pp. 61-104
- De Hert, P., De Shutter, B., 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and SWIFT', in Martenczuk, B. & van Thiel, S. (Eds.), *Justice, Liberty and Security: New Challenges for EU External Relations*, VUB Press, Brussels, 2008.
- De Hert, P., Papakonstantinou, V. and Riehle, C., 'Data protection in the third pillar: cautious pessimism', in Mike, M. (Ed.), *Crime, rights and the EU: the future of police and judicial cooperation*, Justice, London, 2008.
- Department of Homeland Security – Chief Privacy Officer, *Annual Report to Congress, July 2006- July 2007*, Washington, July 2007.
- , *2007 Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties*, Washington, July 6, 2007.
- Electronic Privacy Information Center – EPIC, *Privacy and Human Rights, An International Survey of Privacy Laws and Developments*, USA, 2006.
- Etzioni, A., 'Implications of Select New Technologies for Individual Rights and Public Safety', *Harvard Journal of Law & Technology*, Vol. 15, No. 2, 2002, pp. 258-290.
- Gellman, R., 'A General Survey of Video Surveillance Law in the United States', in Nouwt, S. et al. (Eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, 2005.
- Gonzalez-Fuster, G., De Hert, P. and Gutwirth, S., 'SWIFT and the vulnerability of transatlantic data transfers', *International Review of Law, Computers & Technology*, Vol.22, No. 1-2, 2008.
- Guild, E., Carrera, S. and Geyer F., 'The Commission New Border Package, does it take us one step closer to a 'cyber-fortress Europe'?', *CEPS Policy brief*, No. 154, March 2008.
- Hobbing, P., *A comparison of the now agreed VIS package and the US-VISIT system*, Policy Department C – Citizens Rights and Constitutional Affairs, Briefing Paper, July 2007.

House of Lords – European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, London, 5 June 2007

—, *The Passenger Name Record (PNR) Framework Decision – Report with Evidence*, London, 11 June 2008.

Kightlinger, M.F., ‘Twilight of the Idols? EU Internet Privacy and the Post-Enlightenment Paradigm’, *Columbia Journal of European Law*, Vol. 14, No. 1, 2007, pp. 1-62.

Rotenberg, M., *Recent Privacy Developments in the United States, Particularly with Respect to Travelers Using Air Transportation*, Contribution to the European Parliament Public Seminar ‘PNR/SWIFT/Safa Harbour: Are Transatlantic Data Protected?’, 26 March 2007. Available at: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/rotenberg_/rotenberg_en.pdf

—, ‘The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11’, *Social Science Research Network*, September 2006, pp. 1-60.

Rubinstein, I.S., Lee, R.D. and Schwartz, P.M., ‘Data Mining and Internet Profiling: emerging Regulatory and Technological Approaches’, *The University of Chicago Law Review*, Vol. 75, 2008, pp. 261-285.

Seifert, J.W., *Data Mining and Homeland Security: An Overview*, Congressional Research Service, January 2007.

Steinhardt, B., *The Automated Targeting system (ATS)-A Violation of American Law, The EU-US PNR Agreement and Basic Human Rights*, March 21, 2007. Available at: <http://www.criticalthinking.org/resources/news/2007-statewatch.cfm>

Solove, D.J., ‘Data Mining and the Security-Liberty Debate’, *The University of Chicago Law Review*, Vol. 75, 2008, pp. 343-362.

Solove, D.J., Rotenberg, M. and Schwartz, P.M., *Information Privacy Law*, 2nd edition, Aspen, New York, 2006.

Wik-Consult/RAND Europe/CLIP/CRID/GLOCOM, *Comparison of Privacy and Trust Policies in the Area of Electronic Communications – Final Report*, Bad Honef, 20 July 2007.

Whitman, J.Q., ‘The Two Western Cultures of Privacy: Dignity versus Liberty’, *The Yale Law Journal*, Vol. 113, 2004, pp. 1153-1221.

Zarsky, T.Z., ‘“Mine Your Own Business!” Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion’, *Yale Journal of Law & Technology*, 2002-2003, pp. 1-56.

PRESS ARTICLES

De Rituerto, R.M., “La UE y EE UU se acercan a un pacto sobre datos privados”, *El Pais*, 29 junio 2008. Available at:

http://www.elpais.com/articulo/internacional/UE/EE/UU/acercan/pacto/datos/privados/elpeint/20080629elpepiint_7/Tes

Goldirova, R., “EU and US near deal on confidential data sharing”, *EU Observer*, 30 June 2008, available at: <http://euobserver.com/9/26416>

Savage, C., “U.S. and Europe Near Agreement on Private Data”, *New York Times*, 28 June 2008. Available at: <http://www.nytimes.com/2008/06/28/washington/28privacy.html>

—, “Usa e Ue pronti all'accordo viaggiatori senza privacy”, *Repubblica*, 29 giugno 2008. Available at: <http://www.repubblica.it/2007/12/sezioni/esteri/usa-database-biometrico/iaccordo-usa-ue-voli/iaccordo-usa-ue-voli.html>

Traynor, I., “New pact would give EU citizens' data to US”, *The Guardian*, 30 June 2008. Available at: <http://www.guardian.co.uk/world/2008/jun/30/eu.privacy>