COMMON MARKET LAW REVIEW

CONTENTS Vol. 46 No. 3 June 2009

Aims
The Common Market Law Review is designed to function as a medium for the understanding and implementation of Community Law within the Member States and elsewhere, and for the dissemination of legal thinking on Community Law matters. It thus aims to meet the needs of both the academic and the practitioner. For practical reasons, English is used as the language of communication.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Permission to use this content must be obtained from the copyright owner. Please apply to: Permissions Department, Wolters Kluwer Legal, 111 Eighth Avenue, 7th Floor, New York, NY 10011-5201, United States of America. E-mail: permissions@kluwerlaw.com.

Common Market Law Review is published bimonthly.
Subscription prices 2009 [Volume 46, 6 issues] including postage and handling:
EUR 682.00/USD 965.00/ GBP 502.00 (print)
This journal is also available online. Online and individual subscription prices are available upon request. Please contact our sales department for further information at +31(0)172 641562 or at sales@kluwerlaw.com.
Periodicals postage paid at Rahway, N.J. USPS no. 663–170.
U.S. Mailing Agent: Mercury Airfreight International Ltd., 365 Blair Road, Avenel, NJ 07001.
Published by Kluwer Law International, P.O. Box 316, 2400 AH Alphen aan den Rijn, The Netherlands

---

Printed on acid-free paper.

Common Market Law Review **46**: 885–919, 2009.
© 2009 *Kluwer Law International. Printed in the Netherlands.*

THE PNR AGREEMENT AND TRANSATLANTIC ANTI-TERRORISM CO-OPERATION: NO FIRM HUMAN RIGHTS FRAMEWORK ON EITHER SIDE OF THE ATLANTIC

VAGELIS PAPAKONSTANTINOU AND PAUL DE HERT*

1. Introduction

Seamless air commuting between the EU and the USA appears to constitute nowadays a much sought-after, but nevertheless still elusive cause. The level of cooperation between the two parties has had, and is still having, its best and worst days, burdened by a complex regulatory framework, encompassing several different fields, aggravating thereby the situation. The protection of individual privacy obviously constitutes one of those substantive difficulties which still needs to be resolved. Despite the fact that the notion of individual privacy is a highly esteemed and protected notion on both sides of the Atlantic, different approaches and institutions on the two sides, together with the, by now international, "war against terrorism" have frequently led to bitterness, if not mutual suspicion.

After some forty years of law-making history, the protection of individual privacy, although broadly acknowledged in principle both in the EU and the USA, remains more divergent than convergent between the two parties. The USA notoriously awards fewer institutional safeguards to individual privacy, considering it a matter of individual alertness and redress. Europe, on the other hand, has a long history of institutional privacy protection (notably through a Data Protection Directive[1] and national Data Protection Acts[2] establishing Data Protection Commissions), at least for private and part of public sector data processing.

* Vagelis Papakonstantinou is lecturer at the University of Patras, Partner in PKpartners Law Firm in Athens, Greece. Paul De Hert is professor at the Vrije Universiteit Brussels and associated professor at Tilburg University. This publication is partly the result of a project on law, technology, and shifting balances of power, funded by the Dutch Organization for Scientific Research (NWO). The authors wish to thank Christopher Docksey and Rocco Bellanova for careful review of drafts. All errors remain the authors' own.

1. Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. 1995, L 281/31, (hereinafter, the Data Protection Directive).

2. See, for instance, the German or French Data Protection Acts dating back to 1976 and 1978 respectively.

The relationship between the two parties has traditionally been conflictual and had previously been addressed by the so-called "Safe Harbor" arrangement, which tried to offer a path to escape the undesired restructive consequences of the Data Protection Directive, at least as far as broad commercial exchanges of personal data are concerned.[3]

However, cooperation while commuting over the Atlantic brought the two privacy protection systems once again into conflict. After 9/11, the request of American security authorities to have increased access to the personal data of passengers (PNR data) visiting the USA, inevitably led to yet another confrontation of the two systems, this time however on a more "sensitive" field than ever: rather than commercial exchanges, this time the processing of personal data by the police, customs and other security authorities is at stake, a processing that substantially threatens individual privacy.[4]

This confrontation, as will be demonstrated below, inevitably revealed the shortcomings of both privacy protection systems. In the USA, the lack of institutional safeguards creates suspicion. In Europe, the absence of a comprehensive regulatory framework in the so-called Third Pillar (security-related) processing, which was only amended in late 2008, unavoidably led to a piecemeal and circumstantial approach. In both cases the – internal and external – struggle of powers has led and will continue to lead to privacy regulating agreements, which nevertheless rarely originate from privacy concerns.

This contribution aims to set the PNR scene with regard to the protection of privacy when individuals travel from the EU to the USA, analysing at the same time the perspectives offered by the negotiations and conclusion of the (to date) three separate PNR agreements.

2. Passenger Name Records (PNR)

The term Passenger Name Record (PNR) denotes "the travel record for a person, as used by airline and travel agency databases".[5] Indeed, PNR data are the data required by an airline, in order for an airplane ticket to be bought; this information nowadays can include the passenger's full name, date of birth, home and work address, telephone number, e-mail address, passport details,

3. For a comprehensive list covering developments until the Safe Harbor arrangement was concluded, see the official European Commission Data Protection site at ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm (US – United States – Safe Harbor).

4. For a brief but accurate introduction to the international debate, see the European Data Protection Supervisor (EDPS) Letter to the incoming presidency: fundamental rights are not captives of security, 11 June 2007 (available in the official EDPS site).

5. See en.wikipedia.org/wiki/Passenger_Name_Record.

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. Its exact content will depend on the data provided by the data subject, as not all the fields are compulsory. Databases of PNR data are normally hosted centrally, within an international reservation system.[6]

PNR data obviously constitute "personal data" within the meaning of EU law. Regardless of the distinction between First (commercial) and Third (security) Pillar processing, PNR data undoubtedly fall under the category of "any information relating to an identified or identifiable natural person" (as defined in the Data Protection Directive)[7] or "any information relating to an identified or identifiable individual" (as defined in the 1981 Council of Europe Convention),[8] and hence fall within the scope of the EU data protection provisions.

In the past, passenger records used to include fewer fields. Airlines' data collection policies differed (and will probably continue to differ in the future, regardless of the PNR Agreements). However, nowadays, according at least to the recent PNR Agreements discussed in this paper, each PNR entry can include up to thirty-four (34) fields with personal information of the passenger. The significance of *per se* collecting so much data from every individual can hardly be overlooked, particularly when the data processing is not going to be restricted to its apparent purpose, which is simply allowing the airline company to provide a better service. Indeed, the PNR data transfers system leads to the creation of a database with comprehensive information on all basic individual data, such as residence and workplace, payment preferences, age, etc. Moreover, by collecting and correlating information like "special meal requirements" or "seating particularities" or even by "efficient" use (profiling) of the same individual's name, inferences may be made about such sensitive issues as the religion or health condition of the passengers.[9] In this sense, privacy concerns when it comes to PNR processing appear far from being unjustified.

6. Few airlines (either in the EU or 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, "What's in a Passenger Name Record", 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.

7. Art. 2 of the Data Protection Directive, cited *supra* note 1.

8. Art. 2(a) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, the 28 Jan. 1981.

9. In this context, at least according to First Pillar distinctions, such data would constitute "sensitive data", requiring thus additional safeguards to "common" data processing (see Art. 8 of the Data Protection Directive, cited *supra* note 1).

3. The EU legal framework

3.1. *First and Third Pillar processing within the EU*

The first point to be noted with regard to the PNR data issue from the European perspective refers to the fundamental, EU, distinction between processing of personal information within the First Pillar, as opposed to processing of personal data within the Third Pillar. Following the Pillar structure established by the Treaty of Maastricht,[10] processing of personal data under the First Pillar essentially includes all commercial processing, that is, processing normally performed by private parties in the course of their business. Processing of personal data under the Third Pillar refers to all processing performed by State law enforcement agencies (for instance, the police, customs agencies, judiciary processing) executing their powers and tasks (crime prevention and investigation, State security etc.).

Data protection in the First Pillar benefits from a comprehensive EU legal framework. Since 1995, the Data Protection Directive has been setting the regulatory basis for the EU system for individual privacy protection: a set of data protection principles, accompanied by the creation of independent national supervisory authorities in the Member States to warrant their implementation. The Data Protection Directive was subsequently accompanied by sector-specific measures that built upon its premises and expanded the level of protection afforded to individual privacy within the EU.[11] All Member States have by now harmonized their national legal systems with the above set of Directives, ensuring thus a uniform level of protection where only small differences can be found. What is therefore in place at the time being within the EU with regard to First Pillar processing is a comprehensive, uniform set of rules and regulations, with institutional support of more than a decade both at national (through the national Data Protection Authorities or Commissioners) and at EU level (notably through the European Commission,[12] the Article

10. At the time of writing this paper, the future of the Treaty of Lisbon, particularly after the result of the Irish referendum, remained unknown.

11. For instance, Directive 97/66/EC of the European Parliament and of the Council of 15 Dec. 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, or Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

12. By now, DG Justice,which has succeeded DG Internal Market – a switch of authorities of accurate semantic value, see relevant Statewatch coverage available at www.statewatch.org/news/2005/jul/06eu-data-prot.htm.

29 Working Group,[13] and, of course, since January 2004, the European Data Protection Supervisor (EDPS)).[14]

Unfortunately, the situation is not the same when it comes to Third Pillar processing. Security-related processing is expressly excluded from the scope of the Data Protection Directive,[15] and until late 2008, when the data protection Framework Decision (DPFD) was finally released (see below), the field lacked an equivalent basic, standard-setting regulatory text. Actually, the standard-setting role was supposedly assumed by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data opened for signature back in 1981, as amended by a couple of Recommendations,[16] but the Convention admittedly was a too broad and partly outdated text. Despite the fact that security-related processing within Europe lacked until recently a common regulatory basis, specific sectors did go ahead alone: most notably the Schengen Agreement[17] but also the Europol[18] and Eurojust[19] Agreements all include detailed data protection rules and procedures in their respective texts (using admittedly as basic principles and procedures those introduced in the First Pillar Data Protection Directive). Until late 2008, therefore, what was actually in place within the EU with regard to Third Pillar processing was a series of sector-specific approaches accompanied by a Council of Europe Convention that only broadly regulated the field.

The two aforementioned sets of processing (First Pillar and Third Pillar) ought therefore not be confused: whereas First Pillar processing benefits from a well-regulated environment, an already long history and legislative tradition and productive institutions, all this well-developed system of data protection

13. Officially named the Working Party on the Protection of Individuals with regard to the processing of Personal Data, established by Art. 29 of the Data Protection Directive, cited *supra* note 1.

14. See edps.europa.eu/EDPSWEB /.

15. See Art. 3(2) of the Data Protection Directive, cited *supra* note 1.

16. For work within the Council of Europe on Convention 108, as it has been code-named, see www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/.

17. 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, signed 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, signed in 1990).

18. See The EUROPOL Convention (consolidated text) at www.europol.europa.eu/index.asp?page=legal.

19. See Council Decision of 28 Feb. 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA), O.J. 2002, L 63/l.

does not apply (at least directly)[20] to any Third Pillar processing of personal information.

The data protection shortcomings of the Third-Pillar processing of personal information have obviously not gone unnoticed within the EU. Standard-setting developments, however, (the introduction of an equivalent, that is, to the Data Protection Directive) took place long after all PNR Agreements were concluded. In particular, the Framework Decision "on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters"[21] (DPFD) was released in order to constitute the standard-setting text for all Third-Pillar processing only in late 2008. Back in 2007, when the PNR discussion took place, the DPFD was still only in the making, therefore no firm basis for security personal data processing existed.

There was an attempt to fill the gap through the Treaty of Prüm. In early 2007 the German Presidency managed to obtain support from the Member States for the incorporation at EU level, by means of a Council Decision,[22] of provisions of the Treaty of Prüm. The Treaty of Prüm began as an initiative between seven EU Member States that aimed at closer cooperation in crime-related processing; they therefore entered an "international police cooperation" Treaty on 27 May 2005 in Prüm[23] on enhancing cross-border cooperation,

20. The Data Protection Directive and the First Pillar mechanisms have nevertheless unavoidably become reference points for all European data protection and, thus, extremely influential for the Third Pillar, especially when the people responsible for applying them in the First Pillar are called upon to act in Third Pillar situations; therefore, an indirect but ever-present influence on Third Pillar processing should always be considered (see, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, COM(2005)475 final, 4 Oct. 2005, 4). Additionally, it should be noted that a number of Member States have used in their own jurisdictions First Pillar instruments (the data protection principles and the Data Protection Commissioners) to regulate their, internal, security processing as well.

21. Council Framework Decision 2008/977/JHA of 27 Nov. 2008, O.J. 2008, L 350/60.

22. Council Decision of 27 Feb. 2007, on the stepping up of cross-border cooperation, particularly in combating terrorism, and cross-border crime (available at: register.consilium.europa.eu/pdf/en/07/st06/st06566.en07.pdf). As per the relevant Press Release, "The Justice and Home Affairs Council reached agreement about a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, incorporating in the framework of the Union important provisions of the Prüm Treaty [which] have now become part of the legislative framework of the European Union and will be implemented in all Member States" (See "The Integration of the 'Prüm Treaty' into EU legislation", 12.06.2007, available at europa.eu/rapid/pressReleasesAction.do?reference=IP/07/803).

23. Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, "Treaty of Prüm", 27 May 2005. Available at register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf. See Bellanova, "'The Prüm Process': the way forward for EU police cooperation and data exchange?"

in particular in order to combat terrorism, cross-border crime, and illegal immigration and addressing specific processing (DNA profiles, fingerprints, vehicle registration). The Prüm Treaty contains data protection provisions, but they are related to the processing powers contained in the Treaty. They do not have a general scope.

In addition to the fact that there was no general regulatory framework back at the time the PNR Agreements were concluded, no case-specific text regulating PNR data processing exists within the EU today either. In other words, even if the processing of PNR data among European air carriers while travelling within the EU Member States falls under the scope of the Data Protection Directive, the eventual processing of the same data for law enforcement purposes lacks specific regulation. Although regulatory steps in this direction have been recently recorded,[24] the lack of such an intra-EU instrument deprived the EU of valuable experience and regulatory background when it negotiated PNR Agreements with the USA.

3.2. *The ECJ Ruling: PNR data processing is Third Pillar*

The second point to be noted with regard to the PNR data issue from the EU perspective refers to the fact that PNR data transfers to American authorities need to be considered as Third Pillar and not as First Pillar processing. This clarification was not obvious from the start. Regardless of the fact that PNR data are collected and processed by US authorities which evidently fall within the "security" field, the EU side chose initially to treat the PNR data transfers as First Pillar processing.

The situation was ultimately clarified by a European Court of Justice ruling.[25] According to that judgment: "while the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account … is, however, quite different in nature …, [concerning] not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes".[26] The ECJ further asserted that "it follows that the transfer of

in Guild and Geyer (Eds.), *Security vs. Justice? – Police and Judicial cooperation in the European Union* (Aldershot, Ashgate, 2008), pp. 203–221.

24. See *infra* note 80.

25. Joined Cases C-317/04 & C-318/04, *Parliament* v. *Council*, [2006] ECR I-4721 (hereinafter, the ECJ ruling).

26. Ibid., para 57.

PNR data … constitutes processing operations concerning public security and the activities of the State in areas of criminal law".[27]

The background and the practical implications of the ECJ ruling will be elaborated below; its general merits exceed the purposes of this analysis. For the time being, it is enough to note that PNR data transfers from air carriers to US authorities fall within the Third Pillar, a Pillar that, as already noted, lacks to date a comprehensive legal framework.

4. The US legal framework

4.1. *The regulatory framework*

Perhaps contrary to popular belief, individual privacy and personal data are protected in the USA, even if in a totally different way than in Europe. However, the American system is, arguably justifiably, a complicated system to European eyes, whereby protection for individual privacy is conferred not directly (by a single piece of legislation such as a Data Protection Act), but rather through a combination of Constitutional law, Supreme Court case law, federal legislation, sector-specific legislation, and, where applicable, State legislation, as well as, the theory of torts.

An essential first clarification, before a short analysis of the American system for the protection of privacy is attempted, while keeping PNR data processing in mind, refers to the fact that a general right to individual privacy *per se* (as is the case, for instance, with ECHR Art. 8) is nowhere guaranteed in the US legal system.[28] Instead, protection is conferred either explicitly for "specific privacy rights" or is inferred through other sources, for instance Supreme Court decisions (which, nevertheless, do not necessarily have the right to privacy at their core). In this context, according at least to recent OECD findings,

> "in the United States privacy protection in the private sector is partly treated as an aspect of consumer protection enforced by the Federal Trade Commission under long-standing powers which prohibit unfair and deceptive acts of practices in commerce. A parallel role is played by the Department of Justice for criminal proceedings. But in the common law legislative tradition the United States also has specific sectoral and subject-matter

27. Ibid., para 56.

28. Brenner, "Constitutional Rights and New Technologies in the United States" in Leenes, Koops and de Hert (Eds.), *Constitutional Rights and New Technologies* (Cambridge University Press, 2008), pp. 225–265; Bignami, "European versus American Liberty: A comparative privacy analysis of anti-terrorism data mining", 11 et seq., with further bibliography (available at www.astrid-online.it/Dossier--t1/BIGNAMI-EU-USPrivacy.pdf).

> legislation, for example in the financial services and health sectors, which provides for enforcement of privacy by other federal bodies as well. There is also privacy enforcement at a State level".[29]

Nevertheless, it should be made clear that the notion of privacy, as in particular made concrete and materialized by "data protection" in Europe (essentially, the basic data protection principles), remains largely unknown in the US legal system.

At a top US level, the First, Fourth and Fifth Amendments, as interpreted by the Supreme Court over the last 200 years, have led to a case-specific approach to the protection of individual privacy.[30] The cases where individual privacy is indeed protected in the USA by means of the Constitution, as interpreted by the Supreme Court (given the lack of any direct mention of a generic right to privacy), could be brought down to very specific, real-life situations: according to the Fourth Amendment, a person's right against unreasonable searches of "one's papers", a person's right to privacy of his or her "mail", the use of "wiretapping" techniques or the use of tracking devices, the secrecy of communications, the inviolability of the home, and the inviolability of the body are either regulated or protected.[31] And, according to the First Amendment, the right to speak anonymously, the right to intimate association, to pseudonymous or anonymous association or speech are guaranteed,[32] while, "the Fifth Amendment privilege against self-incrimination plays a very modest role in protecting online privacy".[33]

The US Constitution, as interpreted by the Supreme Court, provides thus for a piecemeal, case-specific protection to individual privacy (which, to European eyes, would have to be broken down into a numbered list of privacy-threatening situations – if this task was at all possible in the modern world – in order to assess its effectiveness in any measurable way). Altogether, however, it has been held that "from the perspective of an American lawyer, anyway, the American system of constitutional rights appears to do a generally satisfactory job of protecting digital privacy", noting nevertheless that

29. OECD, Report on the Cross-Border Enforcement of Privacy Laws, 2006, 12 (available at www.oecd.org/sti/security-privacy).

30. In this context, even since 1989 it has been noted, probably not unjustifiably, that "Americans are sensitive to foreign ignorance of a long line of court cases protective of personal privacy", Flaherty, *Protecting privacy in Surveillance Societies* (University of North Carolina Press, 1989), p. 306.

31. See Brenner's listing, op. cit. *supra* note 28, pp. 5–18, and Privacy and Human Rights Report 2006 (PHR 2006) analysis on the USA, under www.privacyinternational.org/article.shtml?cmd[347]=x-347-559478.

32. See Brenner's listing, op. cit. *supra* note 28, p. 230 and PHR 2006, cited *supra* note 31.

33. Brenner, op. cit. *supra* note 28, p. 235. See also PHR 2006, cited *supra* note 31.

> "the most critical gap in constitutional privacy protections comes in the area of data privacy; more specifically, it exists in the area of third-party records. … the Supreme Court has held that citizens 'assume the risk' – assume the loss of privacy – whenever they share information with third-parties, such as financial institutions, Internet service providers, utility companies, etc. On the one hand, this is a faithful, literal application of the spatially-based conception of privacy that existed when the Fourth Amendment was adopted; on the other hand, however, it is completely inconsistent with the realities of the modern world".[34]

At a federal level – obviously of particular importance for PNR data processing – "three pillars of federal privacy law" may be identified:

> "the three core privacy authorities for U.S. Government use of personally identifiable information are: the U.S. Privacy Act of 1974, the Freedom of Information Act (FOIA) and the E-Government Act of 2002. These laws are supplemented with a framework of regulations, Executive Orders and other policies. Other U.S. laws such as the Federal Information Security Act (FISMA) provide for the security of sensitive information that includes protections for personally identifiable information. There are also a number of laws of general application, such as the Whistleblower Act and the Inspector Generals Act of 1978, that provide additional oversight and accountability".[35]

In general, however, it should be noted that neither the Privacy Act of 1974, nor any other regulatory text for the same purposes, holds the role of a "common regulatory basis", upon which at least all federal processing legislation ought to build. In the same context, no set of processing principles is uniformly (even at federal level) recognized as basic personal data processing principles (as is the case with the Data Protection Directive). Instead, each one of the above regulatory texts follows its own rules and priorities and establishes its own scheme of enforcement through different, mostly federal, agencies (see below, under 4.2.).

Probably of less importance for the purposes of this analysis are the various sector-specific regulations governing the processing of personal information, as they are mostly addressed to private sector processing (for instance, the Data Matching Program (Assistance and Tax) Act 1990, the Video Privacy Protection Act etc.).[36] The same applies to State legislation, due to its restricted scope.

34. Brenner, op. cit. *supra* note 28, p. 38.

35. See Kropf, "Networked and layered: U.S. privacy oversight and accountability", (2007) *World Data Protection Reporter*, 3.

36. For a complete list, see the PHR 2006 analysis, cited *supra* note 31.

4.2. *The oversight model*

The American system does not rely on establishing a single, independent authority for the supervision of all privacy-, or even data protection-, related issues in the country, as is the case in Europe. This absence of a central system for the protection of privacy, as is the case in European federal systems (see for instance, Germany), has been explained as a result of political compromise back in 1974.[37] In the meantime, as already noted, different sector-specific Acts have introduced different enforcement mechanisms, and awarded the respective duties to different (federal) agencies, validating thus even today an assessment made in the 1980s that "the US is a notable exception to the premise that locating the effective national agent for the implementation of data protection is an easy task".[38]

At any event, and at federal level (concerning thus only federal agencies' processing of personal data) the US oversight model ranges from strategic guidance, provided by the Office of Management and Budget (OMB), to internal federal agency Chief Privacy Officers (full-time posts established either by the agencies themselves, for instance, the Internal Revenue Service or the Postal Service, or by the Congress, for instance, the Department of Homeland Security (DHS)). The Department of Homeland Security Chief Privacy Officer's powers, being more relevant to PNR data processing, are to "1) assure that new technologies do not erode privacy; 2) assure that personal information in Privacy Act Systems of Records is handled in compliance with the FIPs [principles] as set out in the Privacy Act; 3) evaluate new legislation on personal information; 4) report to Congress; and 5) coordinate with the DHS Civil Rights and Civil Liberties Office".[39]

It appears that today all US federal agencies, following an OMB memorandum, have appointed internal Chief Privacy Officers. Their intra-agency powers, however, may differ substantially: while the Chief Privacy Officers of the DHS or the DOJ report to the Congress, and run internal agency controls, this does not seem to be true for all CPOs in the US federal privacy oversight scheme.

Because apparently no hierarchy among them exists, "OMB and the CPOs maintain their network through formal interactions such as the approval process for a Privacy Act System of Records Notice (SORN). CPOs also coordinate

37. The Privacy Act of 1974, although issued within a "Watergate" climate, created political concerns for creating "more bureaucracies" and, ultimately, the risk of a presidential (President Ford) veto led to the intermediate solution of awarding part of these duties to the US Office of Management and Budget, Flaherty, op. cit. *supra* note 30, p. 314.

38. Flaherty, op. cit. *supra* note 30, p. 315.

39. Kropf, op. cit. *supra* note 35, at 4, see also PHR 2006 analysis cited *supra* note 31.

through informal meetings and conversations to discuss on privacy issues of the day".[40] At the same time, in 2004 a Civil Liberties Protection Officer was established by Congress in the Office of the Director of National Intelligence through the Intelligence Reform and Prevention Act (IRTPA).

Both the CPOs and the Civil Liberties Protection Officer are responsible for introducing, approving and monitoring the application of their respective agencies' Privacy Impact Assessments (PIAs), the equivalent to a code of practice in European data protection schemes.[41] Accordingly, a PIA is an "analysis of how personally identifiable information is collected, stored, protected, shared and managed. The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system. PIAs are posted on a federal agency's website".[42]

As far as the purposes of this analysis are concerned, PNR data processing falls within the powers of the US Department of Homeland Security (DHS), in its capacity as supervising authority of the US Bureau of Border and Customs Protection (CBP). DHS has an internal Chief Privacy Officer, appointed through the process and equipped with the powers described above. This CPO's office will be essentially in charge of all US PNR data processing.[43] Because all PNR data will be maintained in CBP's APIS (Advance Passenger Information System), the relevant SORN (System of Records Notice[44]) and in particular its PIA,[45] incorporating the provisions of the Privacy Act and E-Government Act of 2002, are also of immediate relevance.

Finally, of some relevance might also prove the Privacy and Civil Liberties Oversight Board, also established by Congress in 2004 through the Intelligence Reform and Prevention Act (IRTPA), but answerable to the President, which among others is "specifically charged with reviewing the terrorism information sharing practices of executive branch departments and agencies to determine whether guidelines designed to appropriately protect privacy and

40. Kropf, op. cit. *supra* note 35, at 4.

41. On the role of codes of practice in European data protection see Art. 25 of the Data Protection Directive, cited *supra* note 1, and Papakonstantinou, *Self-regulation and the protection of privacy* (Nomos, 2002), pp. 91 et seq.

42. Kropf, op. cit. *supra* note 35, at 4.

43. Consequently, all European queries or requests as afforded by the Second PNR Agreement have to be filtered through it (see below under 6.3.).

44. As per DHS explanation, "a System of Records is 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 identifier assigned to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the Federal Register. This notice is generally referred to as a system of records notice (SORN)" (www.dhs.gov/xinfoshare/publications/gc_1185458955781.shtm).

45. Available, together with all updates, at www.dhs.gov/xinfoshare/publications/editorial_0511.shtm.

civil liberties are being followed"; the Board "provides advice and recommendations to the President and executive branch department and agency heads, as appropriate, and additionally makes an annual report to Congress".[46]

4.3. *Individual redress*

An important issue for the purposes of PNR data processing refers to the means of individual redress that the US privacy protection scheme affords to US and non-US citizens, particularly after these means have been extended to apply to European citizens as well, as will later be seen.[47] Attention will again be given only to US federal-level processing, but attention will also be given this time to the rights afforded to European citizens by the Data Protection Directive.

As far as individual access is concerned, it is noted that "the FOIA [Freedom of Information Act] provides any person, regardless of citizenship or location, an administrative process to seek access to information about them". The same is true for the Privacy Act of 1974, which "requires agencies to have an administrative process to allow U.S. citizens or lawful permanent residents to seek access … to records about them, subject to certain exemptions". Nevertheless, access to personal data records does not necessarily lead to a right of amendment as well: the Privacy Act of 1974 does not grant rights of amendment to non-US citizens. Assistance for European citizens will therefore have to be sought elsewhere, either in the so-called DHS Traveller Redress Inquiry Program (TRIP) – which seems to allow any individual to seek redress for the records maintained by DHS components responsible for transportation and border security – or perhaps in the "department-wide policy to afford privacy protection for the non-US persons in DHS systems of records", issued by the DHS CPO. Even with the best will in the world, however, (and unlimited legal resources) finding the relevant legal basis in the above scheme will evidently be a lot less than straightforward.[48]

If the above rights are indeed exercised by non-US citizens with regard to the processing of their PNR data and replies by the competent federal US agencies are not deemed satisfactory, access to the US justice scheme appears the only solution. Using the same "three-pillar federal privacy law system", it appears that only

46. Kropf, op. cit. *supra* note 35, at 4. The Bush Administration, however, allowed it to fall into disuse, by failing to appoint members.

47. Under the Second (2007) PNR Agreement (see below under 6.2.).

48. It should, nevertheless, be noted that all DHS Traveller Redress Inquiry Program (TRIP) forms have been placed online and are thus readily available to all passengers (at www.dhs.gov/xtrvlsec/programs/gc_1169826536380.shtm). For the respective 2007 PIA see www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhstrip.pdf.

> "two of the three pillars provide for legal redress. The Privacy Act provides for four separate and distinct civil causes of action – two of which are injunctive (amendment and access) and two of which provide for monetary damages (accuracy lawsuits and lawsuits for other damages). The limitation, however, is that only U.S. persons legal permanent residents are granted standing in the courts to pursue claims under the Privacy Act. Non-U.S. persons may seek amendment of their records through administrative programs established outside the procedures afforded by the Privacy Act like the DHS Traveler Redress and Inquiry Program, however".[49]

Under the FOIA, on the other hand, "any person may challenge an agency's response to his or her FOIA request in federal court. Access to the court system is permitted regardless of citizenship or resident status".[50]

4.4. *Comparison and compatibility with the European system*

An assessment of the US model for protecting individual privacy lies well beyond the purposes of this analysis. Although the "adequacy" criterion of European Data Protection, as will be discussed below (under 5.1.) indeed makes some form of assessment imperative, such a task would be objectively impossible, because of the huge number of variants that it would include: the two systems differ conceptually, and the gap between them is impossible to bridge. In fact, setting aside such metaphysical assertions as "US privacy protects individual liberty, while in Europe the value protected is dignity",[51] it could be held that we are essentially trying to compare two different things: in the US the talk is only of "privacy", whereas in Europe the talk is of "data protection" as a subset of "privacy". While both systems evidently acknowledge and protect "privacy", it is equally evident that the "right to data protection", as a separate and distinctive right to the right of privacy, remains totally unknown to the US legal system.

5. The First (and the Interim) PNR Agreement(s)

5.1. *Background*

Before 9/11, PNR data were only used for what their name implies: information to make an air travel reservation. They were not systematically collected

49. Kropf, op. cit. *supra* note 35, at 6.
50. Ibid.
51. A distinction suggested by Whitman in "The Two Western Cultures of Privacy: Dignity Versus Liberty", 113 *Yale Law Journal* (2004), 1151.

(reservations could before 9/11 allegedly be made with the person's initials), and generally attracted no great attention. After 9/11, however, in the belief that the processing of PNR data could contribute to keep terrorists out of its country, the US Bureau of Border and Customs Protection (CBP) started asking international air carriers for access to their passenger data, which also had to increase in accuracy and quantity.[52]

As the request seemed to contradict European airlines' (data protection) obligations concerning the personal data they possessed, air carriers were faced with the dilemma which law to break. After coordination with the Commission, which published a Statement, they decided to comply with the US request, thus creating a situation which the PNR Agreement(s) tried to "legalize" and which may only be explained through a brief elaboration of the notorious "adequacy" criterion in European data protection.

5.2. *The "adequacy" criterion*

The "adequacy" criterion constitutes typical regulatory "gunboat diplomacy", by no means invented in the EU: for instance, the USA has implemented it itself, in the case of the Semiconductor Chip Protection Act 1984 – it is however the EU that applied this criterion in the data protection field in its relationships with third countries. And, this criterion effectively applies under both First and Third Pillar processing.

As far as First Pillar (commercial) processing of personal data is concerned, according to the Data Protection Directive:

> "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection" (Art. 25(1)).

This means that, when it comes to First Pillar processing, in principle no personal information is allowed to travel outside the EU if the country it is transmitted to does not guarantee an "adequate" level of protection.[53]

52. The CBP implemented in fact the Aviation and Transportation Security Act 2001. See UK House of Lords, European Union Committee, The EU/US Passenger Name Record (PNR) Agreement (HL Paper 108, 5 June 2007), 1–4. More US projects on PNR processing after 9/11, both abandoned and eventually adopted, may be found at the PHR 2006 analysis, cited *supra* note 31.

53. Unless any of the derogations foreseen in Art. 26 of the Data Protection Directive apply.

With regard to Third Pillar (security) processing, the same wording is employed in the Council of Europe Convention, or rather, in one of its Additional Protocols,[54] as well: "Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer" (Art. 2(1)). Consequently, even after the ECJ's decision placed PNR data processing under the Third Pillar regime, the "adequacy" criterion is still valid, even if the procedure that accompanies its implementation no longer needs to comply with the Data Protection Directive.[55]

The question whether general data protection in the USA is "adequate" according to EU standards remains today largely unanswered. Under the First Pillar, long and painstaking negotiations led to a complex scheme configured around the Safe Harbor Principles, which affirm the "adequateness" of certain processing, in order not to suffocate international commerce.[56] Under the Third Pillar, it is only since 2007 that work on the adequacy of the US law enforcement systems has been carried out within the EU-US High Level Contact Group.[57]

It was in this (complex) environment that the CBP started asking European airlines for access to their passengers' personal data (PNR data), threatening that otherwise they would not be allowed to land on US soil. As already seen, European airlines were effectively faced with the dilemma, which law to break: by transferring personal data of their passengers to America they would be breaking European data protection law (because the adequacy of American processing had not been assessed), but by not doing so they would lose the whole American market.

The First PNR Agreement, as it will be immediately demonstrated, was the EU reply to the above dilemma, allowing in effect European airlines to continue operating in the American market. It was nevertheless based on First

54. 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. At any event, the Protocol has not received sufficient signatures to bring it into force; it also remains questionable whether the Council of Europe norms can be equated automatically with the Third Pillar.

55. More precisely, with the requirements of Art. 25 of the Data Protection Directive, cited *supra* note 1. The "adequacy" criterion has survived the DPFD process (see its Art. 13), it therefore remains relevant within security processing of personal data.

56. See the official Commission webpages on "the adequacy of the protection of personal data in third countries", at ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

57. See Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, Council of the European Union, 9831/28.05.2008, and also de Hert and Gonzalez Fuster, Memorandum to House of Lords PNR Report, cited *supra* note 52, 61 et seq.

Pillar processes and, as a result of that, was in effect annulled by the ECJ (see below, 5.3.); this led to the Interim PNR Agreement (5.4. and 5.5.) and, ultimately, to the Second (2007) PNR Agreement (section 6) in effect today.

5.3. *The First (2004) PNR Agreement*

Going back to November 2001, when European airlines were first faced with the dilemma of which law to break, as explained above, the European Commission decided to intervene. It first informed the United States authorities, in June 2002, that their request to access PNR data could come into conflict with Community and Member State legislation on data protection, and thus helped introduce an immediate brake on CBP requests. CBP, for its part, "postponed the entry into force of the new provisions but, ultimately, refused to waive the right to impose penalties on airlines failing to comply with the legislation on electronic access to PNR data after 5 March 2003. Since then, a number of large airlines in the European Union have granted the United States authorities access to their PNR data".[58] The Commission ultimately allowed air carriers to transmit their PNR data to the CBP only when provisional undertakings and a commitment to negotiate a full international agreement were secured.

The Commission thus entered negotiations with the USA (CBP and its supervising authority, the Department of Homeland Security – DHS) in order to resolve the PNR matter centrally, for all Member States. As already noted, as legal basis for the Commission's intervention served its own assumption that PNR processing constituted commercial processing (thus falling under First Pillar rules, authorizing its direct intervention). It therefore entered negotiations with the USA in 2003. From the American perspective the new instrument was intended to build upon the Aviation and Transportation Security Act of 2001.

One can only speculate why First Pillar processes were chosen altogether by the Commission. The comprehensive data protection background for First Pillar processing, particularly when contrasted to its then practically non-existent Third Pillar equivalent, could be one reason for the Commission's decision. Another could pertain to its urge to intervene before Member States started entering bilateral PNR Agreements with the USA; potentially, different intensities of enforcement could lead to a disruption of the internal market. After all, its position could appear understandable from a legal perspective, because one could very well perceive PNR data processing as processing between private parties due to the fact that airlines are transmitting the data.

58. Para 33, ECJ ruling, cited *supra* note 25.

Negotiations went on for most of 2003. Evidently, the most difficult problem to overcome related to the "adequacy" criterion. Because the "adequacy" of the suggested American processing of PNR data on European citizens had not yet been assessed, the Commission attempted to resolve this problem as follows: it suggested to the Council and the Parliament that, first, it would issue a Decision incorporating an assessment of the American (CBP) processing in relation to the provisions of the Directive ("Adequacy Finding"), and that, second, it would enter an international agreement, in order to deal with problems that would not be addressed by this Adequacy Finding – that is, the PNR Agreement. An international agreement was thought necessary, in order to deal with the problems of extraterritoriality ("pull" system) and legal obligation, as well as bindingness, non-discrimination and reciprocity. With regard to the proper legal basis, Article 95 was used for the PNR Agreement, because it was the same legal basis as for the Data Protection Directive, Article 25 of which was the basis for the Adequacy Finding.

On 23 February 2004, the Council authorized the Commission to negotiate such an agreement with the USA, and issued a series of negotiating guidelines. Accordingly, on 17 March 2004, the Commission made its final proposal to the Council, in order for the latter to issue a Decision "on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection".

The First PNR Agreement was signed on 28 May 2004 in Washington; prior to that, the Commission issued its 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",[59] and the Council its own Decision "on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection"[60] respectively. The CBP, for its part, formally adopted the Undertakings.

A couple of months after the First PNR Agreement was concluded, on 27 July 2004, the European Parliament, for its own reasons, filed two actions before the European Court of Justice, aimed at the Council's and Commission's Decisions respectively, upon which the First PNR Agreement was based. The legal grounds of the Parliament's actions need not be analysed here, also because they were never dealt with in detail by the ECJ; it is therefore sufficient to note that the Parliament claimed, among other things, that

59. Commission Decision 2004/535/EC of 14 May 2004, O.J. 2004, L 235/11-22.
60. Council Decision 2004/496/EC of 17 May 2004, O.J. 2004, L 183/83.

adoption of the decision on adequacy was *ultra vires*, that the legal basis for the Decision approving the conclusion of the agreement was not appropriate, and that fundamental rights had been infringed. Additionally, the then newly established European Data Protection Supervisor intervened in support of the Parliament in both cases.[61]

The Court reached its decision two years later, on 30 May 2006.[62] It did not go into the substance of the Parliament's claims, because it found, as has already been noted above (see section 3.2.), 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 (which only applies to First Pillar processing). The Court thus annulled the Council decision on adequacy, upon which the PNR Agreement was concluded, in effect asking for the First PNR Agreement to be also annulled.[63] The Court subsequently set a deadline (30 Sept. 2006) for a new PNR Agreement to be entered.[64]

The practical results of the ECJ ruling were, first, that the First PNR Agreement between the EU and the USA needed immediate substitution, and, second, that the Second PNR Agreement would need to follow "Third Pillar" processes (which, practically, exclude the Commission from negotiations and entrust this task to the Presidency and the Council).

The First PNR Agreement's provisions need not be analysed here,[65] not only because the ECJ in effect annulled it, but also because they were actually repeated in the Interim PNR Agreement, which will be elaborated on in the next section.

5.4. *The 2006 Interim PNR Agreement: Negotiations*

Negotiations for conclusion of the Second PNR Agreement indeed began on July 2006, but this time by the Council, because the ECJ ruling prohibited the Directive's application to PNR data processing. In this context, according to Article 24 TEU, this time the Council authorized "the Presidency, assisted as appropriate by the Commission" (rather than only the Commission as was the

61. The EDPS did not, however, support the *ultra vires* claim, see the official EDPS site at www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/47.

62. *Parliament* v. *Council* (ECJ ruling), cited *supra* note 25.

63. Paras. 71–74, ECJ ruling, cited *supra* note 25. See also annotation by Gilmore and Rijpma, 44 CML Rev. (2007), 1081–1099.

64. Para 74, ECJ ruling, cited *supra* note 25.

65. Nevertheless, a review of its implementation was indeed performed, as provided for in its Undertakings (clause 44) in Sept. 2005. The Report of the Privacy Office of DHS, establishing that "CBP has achieved compliance with the representations made in the Undertakings" may be found under www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_rpt_09-2005.pdf.

case with the First PNR Agreement) to "open negotiations for an Agreement with the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security".[66] However, given the tight deadline and the tense feelings that the Court's decision raised within Europe, its conclusion by September 2006 seemed unrealistic. Rather than that, an Interim PNR Agreement was suggested, that would remain in effect until the end of 31 July 2007, when the Second PNR Agreement would, presumably, have been concluded.

In accordance with "Third Pillar" processes (which, nevertheless, even then did not remain unquestioned by the Parliament), negotiations between the USA and the (Finnish) Presidency, "assisted by the Commission", were completed on 6 October 2006. On 11 October 2006, the Council adopted a decision "authorizing the Presidency to sign an Interim Agreement with the United States on the continued use of PNR data";[67] the Interim PNR Agreement was finally entered into on 18 October 2006.

The assessment of the lawfulness of the legal basis invoked by the Council in order to enter negotiations with the USA directly (together with the Presidency and "assisted by the Commission", as opposed to allowing each Member State to enter bilateral agreements with the USA), and to adopt, by means of a Decision, the Interim PNR Agreement exceeds the scope of this analysis; here it is enough to note that the Parliament, whose older actions had led to initiating these developments, remained largely dissatisfied.[68]

As far as its legal basis was concerned, the Interim PNR Agreement stated that "in view of the Undertakings issued on 11 May 2004 by DHS, Bureau of Customs and Border Protection, the United States can be considered as ensuring an adequate level of protection for PNR data transferred from the European Union concerning passenger flights to or from the United States".[69] Consequently, the Undertakings upon which the First PNR Agreement relied were considered, for the Interim Agreement's purposes, still valid, ensuring thus an "adequate" level of protection.

What we therefore had, in effect, was a bilateral international agreement (its implementation in the national law of each EU Member State ought to have followed) between the USA and the EU for PNR data transfers. The Interim

66. Preamble, Council Decision on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security, 13226/06.

67. Ibid.

68. See, for instance, European Parliament, "Balancing security and data protection for air travel and judicial cooperation", available at www.europarl.europa.eu/news/expert/background_page/019-10233-247-09-37-902-20060901BKG10232-04-09-2006-2006-false/default_en.htm.

69. Para 4, Interim PNR Agreement.

PNR Agreement expressly referred to the older Undertakings by DHS (as incorporated in the First PNR Agreement), which therefore also remained in effect; nevertheless the Interim PNR Agreement was also amended by a Side Agreement, as will be immediately demonstrated, which brought some effects which were disputed to say the least.

5.5. *The 2006 Interim PNR Agreement: Its provisions*

The Interim PNR Agreement contained essentially the same provisions as its predecessor of 2004; it is nevertheless its reading in combination with a Side Letter by the DHS (which was officially annexed to the Council's Decision adopting the Interim PNR Agreement, and was referred to in its text) which had raised substantial concerns on its actual effectiveness in protecting individual privacy.

At the Interim PNR Agreement's core lay, as was the case with its predecessor, the basic assumption that "in reliance upon DHS's continued implementation of the … Undertakings as interpreted in the light of subsequent events, the European Union shall ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America process PNR data contained in their reservation systems as required by DHS".[70] In addition, DHS had the right to "electronically access the PNR data from air carriers' reservation systems located within the territory of the Member States of the EU until there is a satisfactory system in place allowing for transmission of such data by the air carriers".[71]

Therefore, according to the Interim PNR Agreement, the DHS had, first, the right to instruct European airlines which PNR data to collect and, second, had access to them. Naturally, all this on condition that DHS continued to adhere to the Undertakings of 2004.

The Undertakings essentially included provisions of a substantial nature, regulating the details of DHS' processing; their implementation was central for fulfilment of the adequacy criterion. For instance, it is in the text of the Undertakings that the exact fields of PNR data the DHS could access were listed (34 fields altogether). The purposes of DHS processing were also set out in those Undertakings ("preventing and combating terrorism and related crimes, other serious crimes, including organized crime, that are transnational in nature, and flight from warrants or custody for the crimes described above"[72]). The treatment of "sensitive" data, the time period for which PNR data may be stored in

70. Ibid., para 1.
71. Ibid., para 2.
72. Para (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, 41543.

DHS' databases, DHS' systems' security, or even "notice, access and opportunities for redress for PNR data subjects" were equally issues regulated in the Undertakings of 2004.

Under the First and the Interim PNR Agreements (at least, until the Side Letter discussed below appeared) European PNR data would remain in American systems for a period of up to three and a half (3.5) years, which could be extended to seven (7) years altogether, after which period all data had to be deleted.

Among the few differences between the Interim PNR Agreement and its 2004 predecessor was, perhaps most importantly, the expansion of the catalogue of American agencies that could process PNR data: as per the Interim PNR Agreement it was not only the DHS, and in particular the CBP, but also "CBS, US Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it", excluding nevertheless explicitly certain "components of DHS".[73] Another point that had raised criticism concerned the fact that the Interim PNR Agreement allowed DHS to change the standards of processing, if US laws change to this end.[74]

Altogether the Interim PNR Agreement was, as its name suggested, neither a text substantially different from its predecessor nor one that could cause more problems to individual privacy than the previous regulatory framework already did, although the few differencess outlined above are not neutral.

Nevertheless, the situation was practically reversed by a Side Letter to the Interim Agreement of the DHS – this Side Letter being, confusingly, annexed to the Council's Decision on the adoption of the Interim PNR Agreement. The Side Letter was "intended to set forth [US] understanding with regard to the interpretation of a number of provisions of the PNR Undertakings issued on May 11, 2004 by the DHS"; in practice, however, it amended the Undertakings of 2004, upon which the Interim PNR Agreement was based. These amendments were indeed far from unimportant. In brief, European PNR data were suggested to be openly shared among any American agency that undertook some "counter-terrorism function" or even had public health concerns; the DHS could decide on its own which PNR data it required to be transmitted (regardless whether "pushed" or "pulled") for an indicative period of 72 hours before the respective flight; the limitation to only accessing 34 out of some 60 PNR data fields became indicative; PNR data would be stored for periods longer than 3.5 years since collection, and all this with no control whatsoever, because at least for as long as the Interim PNR Agreement remained in effect, no implementation review would be performed.

73. See Preamble, Interim PNR Agreement.

74. See para (1), Interim PNR Agreement, and House of Lords PNR Report, cited *supra* note 52, 60.

Given the reversing effect of the Side Letter to the PNR data status, it came as no surprise that the European Parliament and privacy advocates fiercely attacked the final wording of the Interim PNR Agreement and requested amendments and clarifications from the Council;[75] nevertheless, the timely (and unexpected) release of the Second PNR Agreement turned everyone's focus to the new provisions, which indeed differed substantially from their predecessors.

6. The Second (2007) PNR Agreement

6.1. *Background*

Negotiations between American and EU officials – this time, from the European perspective, as Third Pillar processes, including the Finnish and German Presidencies "assisted by the Commission" – went on for the second half of 2006 and the first half of 2007. Contrary to the general expectation that they would be impossible to conclude until expiration of the Interim PNR Agreement (at the end of July 2007), and thus that the term of the Interim Agreement would be extended for a couple of years more, an unprecedented German push during the last months of its Presidency (which in a swift, uniform move bound the PNR issue together with the *SWIFT* case and resolution[76]), led to conclusion of a text on 29 June 2007.[77] The text however still had to be ratified by all EU 27 national parliaments.[78]

Difficulties while negotiating the Second PNR Agreement from the American perspective were evidently based on the fact that the American side had

75. See EDRI's, "Enditorial, Are Transatlantic data protected?", 28 March 2007, under www.edri.org/edrigram/number5.6/transatlantic-data-protected.

76. The *SWIFT* case was resolved by the German Presidency practically in parallel with the PNR data issue (negotiations run at the same time, between the same participants) in June 28, 2007 (see, EDRI, "Final Agreements between EU and USA on PNR and SWIFT", at www.edri.org/book/print/1231).

77. Council Decision 2007/551/CFSP/JHA of 23 July 2007 (O.J. 2007, L 204/16–25) on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) available at eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:01:EN:HTML.

78. A process still not concluded at the time of finalizing this paper, which was nevertheless undermined by bilateral agreements between certain Member States and the USA (see below, under 6.7.). It should be noted, however, that the Agreement provided for provisional application, as per Art. 24(5) TEU, and therefore entered into force immediately not needing to wait for national procedures to be completed.

secured extensive PNR data processing powers under the First and Interim PNR Agreements (particularly under the Side Letter, see above), which it saw no reason to forego because of intra-European complexities (namely, the ECJ ruling, which imposed a new agreement). The European side, on the other hand, was found in a more complex situation. While there was the American request of ever more data-processing powers and the airlines' wish to operate in the American market, the European side also had to bear in mind the sensitivities of the European Parliament,[79] which, although under Third Pillar processes (Art. 24 TEU) did not participate in the negotiations, pressed for a strong data protection line (it should not be forgotten that it was the Parliament's reaction that triggered the ECJ ruling and started the whole process in the first place). Perhaps even more gravely, however, while negotiating with the USA, the European side essentially had no text of reference: the Data Protection Directive (with its definitions, principles and mechanisms) was judged by the ECJ not applicable, and no other standard-setting Third Pillar legislation existed, because the Data protection Framework decision (DPFD), which ought to have held this role, was still at the time only in the course of the law-making process. The European side also had no (formal) institutional assistance from the numerous EU data protection agencies, because all of them (the Art. 29 Working Party, the EDPS, or even national Data Protection Commissioners) fall under the First Pillar. To make things even worse, no EU PNR Agreement existed that would have preceded the US text (and have limited its scope); rather than that, the Commission announced a relevant initiative only after the Second PNR Agreement was concluded.[80]

It is under these circumstances that the Second PNR Agreement was released, an almost impossible task that was accomplished partly due to German persistence. In the following, however, we examine whether such persistence ultimately benefited or harmed the data protection purposes.

6.2. *Legal basis of the Second PNR Agreement*

The Second PNR Agreement is, in fact, composed of three distinct documents: in the careful wording of Franco Frattini, then Commissioner in charge, when addressing the Parliament, "the agreement is divided into three parts. First, an

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

80. A process that begun 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 www.statewatch.org/news/2007/oct/eu-com-pnr-proposal.pdf, as well as, the relevant EDPS Opinion on the Proposal, issued on Dec. 20, 2007 (available at the official EDPS site).

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".[81] It is however the exact legal relationship among these three documents, if any, that indeed raises questions (as will be elaborated below).

As far as the Agreement itself is concerned, it expressly constitutes an international agreement, according to Articles 24 and 38 of the Treaty on European Union. Its subject-matter (PNR data processing), following the ECJ ruling, falls under Titles V and VI of the TEU, and therefore the Council authorized the Presidency, "assisted as appropriate" by the Commission, to open negotiations with the USA for the conclusion of the Second PNR Agreement, which was eventually concluded by the Council itself.

The "*letter exchange*" part of the Second PNR Agreement attracted much criticism. The choice to conclude international agreements whose substantial clauses are set in accompanying letters, at least from the European point of view, threatened to further diminish the level of protection afforded by the previous PNR Agreements.[82] Whatever the background explanation for such law-making, the fact remains that, as far as PNR data are concerned, the Second PNR Agreement expressly begins by stating that "On the basis of the assurances in DHS's letter explaining its safeguarding of PNR (the DHS letter), the European Union will ensure that air carriers operating passenger flights in foreign air transportation to or from, the United States of America will make available PNR data contained in their reservation systems as required by DHS".[83] The wording here is particularly vague, evidently on purpose. Technically, the so-called DHS letter is not annexed or affixed in any strict way to the Second PNR Agreement: it is not "the" DHS letter, it could very well be "any" DHS letter addressed to the EU. In other words, the DHS will probably not feel compelled to adhere to this same "letter" throughout the term of the Second PNR Agreement.

Attention should also be given to the "assurances" provided by DHS, rather than "obligations" or "warranties" or any other term evidencing a mandatory context. Obviously, the DHS "assures" but does not "warrant" or "undertake"

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

82. See EDRI, cited *supra* note 76.

83. Art. 1, 2007 PNR Agreement.

to safeguard European PNR data. The qualitative difference is clear for everyone to see.

The subsequent "exchange of letters" further complicates matters. Why did the EU feel compelled to send a letter accepting "the DHS letter"? Given the wording of the Second PNR Agreement, the EU is already aware of the content of the "DHS letter" and it is on its exact premises that the Agreement itself is concluded. Why then introduce a "letter exchange" process, whereby the DHS addresses a letter to the EU, and the EU accepts it by replying back in writing as "ensuring an adequate level of data protection"? And why did those who drafted the Second PNR Agreement feel the need to draft its Article 6, whereby "DHS is deemed to ensure an adequate level of protection for PNR data transferred from the European Union", evidently regardless of its "letter", and in addition to what EU is replying in its own letter? No matter how innocent and well-intended such a "letter exchange" might appear, one cannot help but think that it introduces in practice an amendment process, whereby the DHS will be addressing "DHS letters" to the EU, and the EU will be assessing and responding to them accordingly.[84]

At any event, the choice of concluding an international Agreement whose substantial clauses in their entirety are included in "letter exchanges" remains a questionable choice from the European perspective when it comes to data protection purposes. As it will later be seen (below, under 6.4.) questions have immediately, and probably justifiably, been raised by the Parliament and privacy advocates as to the usefulness, and indeed lawfulness, of such a legal scheme.

6.3. *Provisions of the Second PNR Agreement and the DHS letter*

As far as substance is concerned, the Agreement itself is a rather brief text of "structural" drafting: as already seen, its Paragraph 1 sets the scene: "on the basis of the assurances in DHS's letter …, the European Union will ensure that air carriers … to or from, the USA will make available PNR data contained in their reservation systems as required by DHS". The Second PNR Agreement thus follows the rule-making methodology of its predecessors, whereby 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 (see,

84. One explanation for such "letter exchange" could be that the USA expected, on the basis of its assurances, an EU assurance of adequacy, that would also serve to bind national data protection authorities (some of which under their respective national law have powers over international transfers that do not distinguish between the First and Third Pillars in the same way as EU law).

for instance, the Side Letter in the Interim PNR Agreement above, under 5.5.).

The definition of PNR data under the Second PNR Agreement is included, as 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.[85] Sensitive personal information (as per the 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 imperiled 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 U.S. legislation which materially affects the statements made in this letter".

As clearly stated, combating terrorism is not the only reason 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 retained by DHS to "advise" the EU whenever American legislation affects the DHS Letter; rendering thus its term and undertakings, if any, of temporary nature, and reinforcing concerns on its legal nature expressed above (section 6.2.). 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 will be held in American systems for a period of altogether fifteen (15) 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

85. See Ch. III, U.S. Letter to EU.

> Secretary of Homeland Security and only in response to an identifiable case, threat, or risk" (Ch. VII, DHS Letter).[86]

This extension of the retention term (from three and a half years under the First and the Interim Agreement) will be discussed below (under 6.5.), here it is enough 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".[87] Evidently, DHS commits to delete the PNR data (if at all) from its own databases; nowhere in its Letter does it undertake to monitor deletion from other "domestic" databases to which it has already transmitted the data during their fifteen-year retention.

A lot of attention, justifiable also on international jurisdiction grounds, has been given to whether a "push" or a "pull" system would be established for the technical transmission of data. Europeans (and the EDPS) pressed for a "push" system, whereby PNR data will be transmitted by airlines to the DHS (rather than the DHS accessing them from their system, a "pull" system) and the Americans conceded; "DHS will immediately transition to a push system for the transmission of data by such air carriers no later than January 1, 2008 for all such air carriers that have implemented such a system that complies with DHS's technical requirements" (Para 2 of the Agreement).

Of greater importance is the extension of rights awarded by American legislation to European citizens as regards processing of their PNR data by American authorities, triumphed over by the European side.[88] To this end, Chapter IV of the DHS Letter (not the Agreement) sets out the following:

> "Access and Redress: DHS has made a policy decision to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens. … Furthermore, PNR furnished by or on behalf of an individual shall be disclosed to the individual in accordance with the U. S. Privacy Act and the U. S. Freedom of Information Act (FOIA)".

86. 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 above).

87. See Ch. VII, U.S. Letter to the EU.

88. Frattini to Parliament "Protection given under the United States Privacy Act will be extended through administrative procedures to non-US citizens, in particular with regard to redress and correction, and, therefore, EU citizens will be entitled to protection under that Act. That was not the case under the previous agreement" (see www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20070709+ITEMS+DOC+XML+V0//EN).

The above passages have somehow been interpreted by Europeans as granting them additional rights under the US Privacy Act of 1974. Nevertheless, we feel the need to examine exactly what the Americans have offered. Attention should be given to the exact wording of the DHS Letter: it refers to "administrative Privacy Act protections", not all protections. Referring to the "three-pillar federal privacy law system" (above, section 4), we note that the Privacy Act of 1974 altogether grants: (a) access rights to American citizens or lawful permanent residents, (b) amendment rights only to American citizens, (c) four separate and distinct civil causes of action in American courts, two of which are injunctive (amendment and access) and two of which provide for monetary damages only to American citizens and American permanent residents. Of those three elements, it is believed that only (a) and (b) constitute "administrative protections" and have thus indeed been extended to European citizens. Recourse to American courts according to the Privacy Act of 1974 appears not to be granted to European citizens in cases where they believe that DHS processing has breached their rights. A point also to be noted is that, until the Second PNR Agreement was concluded, the American side maintained that rights to access and amendment already existed, through "other administrative routes" (see above section 4). It therefore seems that Europeans are triumphant over the simplification of already existing procedures, rather than the granting of new rights.[89]

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 U.S. and EU PNR policies and practices with a view to mutually assuring the effective operation and privacy protection of their systems" (Art. 4).

6.4. *Data protection concerns regarding the amount of data disclosed*

If examined from a data protection perspective, (that is, in the light of the then in effect Data Protection Directive, or even the DPFD which came long after it, regardless of the latter's limitations in its scope) the Second PNR Agreement obviously does not stand a chance; it clearly and consistently steers away from all European basic data protection principles (for instance, independent monitoring, effective means of redress, the finality principle, transmission of personal data to third-countries only when the "adequacy" criterion is met, etc.).[90]

89. Even these rights were however diminished unilaterally by the USA immediately after entering the Second PNR Agreement (see *infra*, under 6.7).

90. See, above all, the European Parliament's Resolution of 12 July 2007, where among others, it is stated that: "the new PNR agreement fails to meet the second objective, as it is

If, however, placed under its proper international environment (terrorism threats all over the world, and war waging still in Iraq and Afghanistan) and given the First and Interim PNR Agreements, which inevitably constituted its points of reference, the Second PNR Agreement could perhaps stand an assessment. It is therefore in this light that its gravest shortcomings from a data protection perspective will be examined below, with the purpose of ultimately establishing whether rushing into a new text in perhaps the best possible way under the circumstances (the Second PNR Agreement) constituted a better strategy than extending the term of an admittedly bad one (the Interim PNR Agreement) until improved circumstances, at least from a European point of view, permitted its revision.

As already noted, PNR data under the Second PNR Agreement include nineteen (19) fields, rather than thirty-four (34), as was the case with its predecessors. From this point of view the decrease can only indicate an improvement of the level of privacy protection afforded to EU citizens. Nevertheless, close observation of the previous thirty-four fields and the current nineteen reveals otherwise: the reduction constitutes rather a rationalization than an actual decrease in the quantity of data held. Indeed in previous PNR Agreements common personal details such as "address", "billing address", "telephone numbers", constituted separate fields, whereas under the Second PNR Agreement such fields are all hosted under an "all available contact information" field.[91] The same, for instance, is the case with the older two fields on "travel agency" and "travel agent" which under the Second PNR Agreement have been consolidated under a single "travel agency/travel agent" field.[92] Therefore, the reduction in the absolute number of fields held by American authorities under the Second PNR Agreement is superficial, constituting a rationalization and consolidation of previous fields rather than an actual decrease in the number of items of personal information about European citizens held by American authorities.[93]

As far as the quality of the PNR data collected under the Second PNR Agreement is concerned, although at first they may appear inconspicuous, if properly correlated they could reveal sensitive information. For instance, "OSI,

substantively flawed in terms of legal certainty, data protection and legal redress for EU citizens, in particular as a result of open and vague definitions and multiple possibilities for exceptions" (also available at www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0347+0+DOC+XML+V0//EN&language=EN).

91. See fields No. 6, 8 and 9 of the Undertakings for the First and Interim PNR Agreements and field No. 7 of the Second PNR Agreement respectively.

92. See fields No. 12 and 13 of the Undertakings for the First and Interim PNR Agreement and field No. 10 of the Second PNR Agreement respectively.

93. In the European Parliament's words, it: "Takes note of the reduction in data fields from 34 to 19, but points out that the reduction is largely cosmetic due to the merging and renaming of data fields instead of actual deletions" (Resolution of 12 July 2007, cited *supra* note 90).

SSI and SSR information" refer to such passenger details as special meals request, which could ultimately point to religious beliefs. The same is after all true when the name of an individual is "properly" processed (profiled). DHS could support that all these data, because they are not "included in the above types of EU PNR data" but they are rather inferred by its own software, do not formally fall under the "sensitive data" provisions of the Second PNR Agreement (or, rather, the DHS Letter) and thus do not benefit from the "exceptional case" filter; ultimately, sensitive personal data of European citizens will be free for processing by the DHS.

6.5. *Data protection concerns regarding the PNR data retention period*

Whereas under the First and the Interim PNR Agreement personal data of EU citizens would have been held in American databases for a period of altogether 11.5 years (3.5 years immediately accessible and another 8 years "dormant"), under the Second PNR Agreement this period has been increased to 15 years (8 + 7 years respectively). Such an increase obviously poses an increased threat to individual privacy.

Even the original term of three and a half years was deemed excessive, and a concession to the American side during negotiations, based on the fact that such was the term originally intended for the First PNR Agreement.[94] The European point of view on this matter has been that

> "data must be retained for the period of time that is necessary for the purposes for which the data are collected. If, for example, identification of travellers posing a threat is the purpose, there would not be sufficient ground for retaining the data for longer than the retention period established under Directive 2004/82/EC. That Directive states that data should be deleted 24 hours after arrival. The retention of personal data of unsuspected individuals for possible future use for the given purposes has a substantial impact on human rights and would therefore need strong justification".[95]

A point also to be noted, which might explain American insistence on a data retention term extension, is that negotiations for the Second PNR Agreement took place while reaching the initial 3.5 years time limit: the First PNR Agreement was entered on May 2004, and during the Spring of 2007 Americans

94. See a common EU approach to the use of Passenger Name Record (PNR) data for law enforcement purposes – Art. 29 Working Party (available at ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2007_31_01_common_eu_approach_use_pnr_data_for_law_enforcement.pdf), 8.

95. Ibid.

faced the possibility of being forced to delete all European PNR data from their systems once the initial 3.5 period was completed.[96] The term-extension secured under the Second PNR Agreement must have been a relief for Americans, solving one of their immediate problems, while also securing that they would not face it again in the immediate future.

At any event, and regardless of the background that led to it, the extension of the data retention period for European PNR data constituted a defeat for European data protection, particularly given the fact that the American side never guaranteed that even after such term expires it would make sure that all PNR data would be erased from all other, American, data processing systems to which they will have been transmitted in the meantime (see above, under 6.3.).

6.6. *Human rights concerns about the effect of PNR data processing*

The contribution of PNR data processing *per se* to the international combat against terrorism is widely disputed. Obviously, once "terrorists" are aware that a PNR data processing system is in place they will take measures against it, practically leaving only unsuspecting passengers' data on American (or even European) security databases. However, despite widespread scepticism regarding PNR data processing as an effective anti-terrorist tool, no security or other agency anywhere in the world has ever presented any evidence (statistical or other) to their defence. In effect, security agencies press for ever more comprehensive PNR data processing (see also 6.7 below), asking the public to simply take their word as to their effectiveness on account of "national security".[97]

The Second PNR Agreement does not appear to offer any assistance in this area. First, it was concluded again without any evidence that its predecessors (the First and the Interim PNR Agreements) did a good job protecting us from terrorism.[98] On the other hand, its provisions on its periodic evaluation only pertain to "mutually assuring the effective operation and privacy protection of their systems" (Art. 4), taking thus the continued existence of these "systems" for granted.

At the same time, the EU itself has started moving towards implementing its own PNR processing system. Evidently, its approach is not the same as the one

96. See the Data Retention section in the Interim PNR Agreement.

97. See Commissioner Jonathan Faull's response to a relevant question in a public seminar held by the European Parliament LIBE Committee on 26 March 2007 (minutes available at www.edri.org/edrigram/number5.6/transatlantic-data-protected).

98. See In't Veld or Schaar in European Parliament LIBE Committee Seminar (previous note), as well as House of Lords PNR Report, cited *supra* note 52, at 20–22.

imposed upon it by the American side while drafting the PNR Agreements, but rather originates from more traditional European data protection concepts.[99] Regardless of any good intentions, however, the fact remains that any PNR data processing system by definition infringes the finality (data protection) principle, because it uses personal information collected for making a flight reservation for other (security-related) purposes. Such a serious infringement of the fundamental (European) right to data protection may only take place, if at all, if the result such processing achieves outweighs the infringement it causes, in other words, only if PNR data processing is so effective and indispensable in fighting terrorism that its mass infringements of individual rights are assessed of secondary importance.[100] No such case was ever proven (or even attempted to be proven) up until today. Nevertheless, the Second PNR Agreement and the intra-EU initiatives are evidence that PNR processing systems are here to stay, regardless of their compatibility with basic data protection law or their effectiveness in fighting terrorism in practice.

6.7. *Latest developments undermining the Second PNR Agreement engagements*

Despite the privacy shortcomings of the Second PNR Agreement, the American side appears to have undertaken a consistent policy immediately after its coming into effect to undermine it even further. The first step in this direction was made as early as one month after its signature: in August 2007 the Department of Homeland Security published its "notice of a revised and updated system of records pursuant to the Privacy Act of 1974 for the Arrival and Departure Information System (ADIS)". In this proposed rulemaking, DHS proposes to exempt this system of records (a new "arrival and departure system" intended to authorize people to travel only after PNR and API data has been checked and cleared by US agency watchlists[101]) from one or more provisions of the Privacy Act because of "criminal, civil, and administrative enforcement requirements".[102] In its view, the DHS has attempted, in its own words, "to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens. Consistent with U.S. law, DHS also maintains a system accessible by individuals, regardless of their

99. See *supra* note 80.

100. See also House of Lords PNR Report, cited *supra* note 52, at 5.

101. See relevant Statewatch entry at www.statewatch.org/news/2007/sep/04eu-usa-pnr-exemptions.htm.

102. Federal Register: Aug. 22, 2007 (Volume 72, No. 162), see also the relevant Statewatch announcement at www.statewatch.org/news/2007/aug/usa-adis-privacy-act-exemptions.pdf.

nationality or country of residence, for providing redress to persons seeking information about or correction of PNR".[103] However, it has also been held that the above exemption of this "revised and updated system of records" by the DHS actually "seem(s) to be meant to counterbalance 'the set backs' for the US government in the EU-US PNR agreement signed in June";[104] the timing of the DHS amendment of the US Privacy Act, only a month after the Second PNR Agreement was entered, seems to support such claims.[105]

In parallel to reinforcing its position domestically, the USA has entered an aggressive plan to undermine the Second PNR Agreement from within. Only a few months after the Second PNR Agreement was entered (and before it was ratified by all Member States) the Americans used their visa-waiver policies to lure bilateral (PNR) agreements out of those EU Member States whose citizens still need a visa to enter the USA. Most notably, the Czech Republic entered such a bilateral agreement that granted far greater "liberties" to American processing of its citizens' personal data.[106] The EU Commissioner in office at the time failed to address the problem and create a unified European stand, and effectively other Member States were left alone to enter bilateral negotiations with the US, without any EU assistance. It therefore seems that the Second PNR Agreement will effectively be valid only for a handful of EU Member States after all.

The Council for its part has been busy concluding PNR Agreements with third countries, namely Canada[107] and Australia.[108] Although at their core lies again the transmission of European PNR data to third countries, it appears that data protection considerations held a more central role in comparison to their

103. Ibid.

104. See EDRI, "US gains new advantages in the EU-USA PNR agreement", Newsletter No. 5.17, 12 Sept. 2007.

105. The DHS at the same time also amended the APIS system, where PNR data are maintained, because "DHS needs these exemptions in order to protect information relating to law enforcement investigations from disclosure to subjects of investigations and others who could interfere with investigatory and law enforcement activities. Specifically, the exemptions are required to: Preclude subjects of investigations from frustrating the investigative process;" etc. (Notice of Proposed Rulemaking for Privacy Act Exemptions Aug. 23, 2007, 72 FR 48346, available at www.dhs.gov/xinfoshare/publications/gc_1185458955781.shtm).

106. See EUBusiness.com, "EU Nations Set to Negotiate Individual US Visa Deals", 28 Feb. 2008, at www.eubusiness.com/news-eu/1204192026.71, and The Guardian, "Bush Orders Clampdown on Flights to US", 11 Feb. 2008, at www.guardian.co.uk/world/2008/feb/11/usa. theairlineindustry, ("the Americans could 'get' a gung-ho frontrunner" to sign up to the new regime and then use that agreement 'as a rod to beat the other Member States with'. The frontrunner appears to be the Czech Republic").

107. See Council Decision of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data, 2006/230/EC.

108. Available at www.statewatch.org/news/2008/jun/eu-australia-pnr-agreement-2008.pdf.

US equivalent; in this context even the European Parliament regretted that "EU negotiations with the US took no account of Directive 2004/82 nor of EU PNR agreements with Australia and Canada, that ensure higher standards of protection of personal data".[109]

7. Conclusion – towards a (predictable?) future

Time (indeed, the immediate future) has already proven that the Second PNR Agreement constituted an unnecessary concession, at least from the European point of view. As soon as the Agreement was entered into, American actions towards amending perceived "shortcomings" in domestic legislation and undermining European cohesion as to its implementation clearly point to an, in effect, null and void text.

In the meantime the EU is preparing its own PNR Agreement, in the form of a Framework Decision, whereas the DPFD has come into effect, setting the common principles for all EU security-related personal data processing. In addition, structural changes, in particular the latest version of the Treaty (whose future however remains unknown) transferring substantial powers to the, pro-privacy, Parliament, are also expected to gravely affect the field of security data processing.

All the above point indeed to the inevitable need for a Third PNR Agreement with the USA in the foreseeable future. This, new Agreement, will, as far as the European perspective is concerned, have a firm institutional basis (the DPFD and the EU PNR Agreement) and an emphasis on privacy protection (because of the Parliament's inevitable intervention). In this light, it appears that concluding the Second PNR Agreement at the time and in the form it was done, even if with the best of intentions and even if with the best possible outcome given the circumstances prevailing at the time, was a strategic mistake; a much preferable option would have been to wait, by extending the term of the Interim PNR Agreement for a couple of years, until the conditions were mature for the adoption of a totally new approach to transatlantic cooperation when it comes to personal data processing.

109. See Joint Motion for a Resolution to the European Parliament on the PNR Agreement with the United States, available at www.alde.eu/fileadmin/files/plenary_session/2007/july/2007-LIBE_-0048-01-EN.pdf.