STUDY

DIRECTORATE GENERAL INTERNAL POLICIES OF THE UNION

EUROPEAN PARLIAMENT

Policy Department C
Citizens' Rights and Constitutional Affairs

TOWARDS A EUROPEAN PNR SYSTEM?

QUESTIONS ON THE ADDED VALUE AND THE PROTECTION OF FUNDAMENTAL RIGHTS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

JANUARY 2009
PE 410.649

EN

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

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

TOWARDS A EUROPEAN PNR SYSTEM?

QUESTIONS ON THE ADDED VALUE AND THE PROTECTION OF FUNDAMENTAL RIGHTS

STUDY

Abstract:

In November 2007, the European Commission published a proposal on the use of Passenger Name Record (PNR) data for law enforcement purposes. This proposal is closely related to other instruments obliging air carriers to transmit passenger data to national authorities, including Directive 2004/82/EC and various agreements that were signed with third countries. The establishment of an 'EU PNR system' is presented as a tool in the fight against terrorism and organised crime, but will also be used to investigate other crimes and to prevent illegal immigration. The European PNR system raises both practical as legal concerns.

This study, taking into account the different comments of the organisations and institutions involved and the Resolution of the European Parliament of 20 November 2008, questions in the first place the efficiency and added value of the current proposal. To assess this question it takes into account existing measures on the large-scale collection and storage of personal information (the Schengen Information System, Visa Information System and the EU proposals for automatic border control). The EU and its member states are bound by EU, international, and national standards on human rights.

Therefore, the second part of this study describes the legal implications of an EU PNR system, focusing in particular on the right to data protection, the right to private life, the prohibition of discrimination and the issue of profiling.

Finally, part three includes some final remarks and recommendations.

PE 410.649

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

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

Author: **Evelien Brouwer, Utrecht University**

Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS)

Manuscript completed in **January 2009**

Copies can be obtained through:

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

Information on **DG IPOL publications**:

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

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

Brussels, European Parliament

TABLE OF CONTENTS

INTRODUCTION

In November 2007, the European Commission published a proposal for a Council framework decision on the use of passenger name record (PNR) data for law enforcement purposes (COM(2007) 654). The principal purpose of the draft framework decision is the establishment of a tool in the fight against terrorism and organised crime. Yet, considering the current discussions within the Council and its relation to other instruments in this field, it is to be expected that the data to be processed and stored within the so-called 'EU PNR system' will also be used to investigate other crimes and to prevent illegal immigration. For example, this proposal is closely related to Directive 2004/82/EC on the use of passenger data for the purposes of border control and preventing illegal immigration. Furthermore, it is important to take into account other instruments recently adopted within the EU that provide for the large-scale collection and storage of personal information (for example the Schengen Information System (SIS), Visa Information System (VIS) and the EU proposals for automatic border control. Also, the EU as well as different member states have signed bilateral agreements with third countries, such as the US, Australia and Canada, on the transfer of passenger data to the authorities of those countries.

While confirming that law enforcement authorities should obtain all the tools they need to adequately carry out their tasks, the European Parliament in its Resolution of 20 November 2008 underlined that the justification of the current proposals needs to be convincingly substantiated – not only because of the considerable impact of these instruments on the personal life of citizens, but also because of their consequences for air carriers. This study, taking into account the different comments of the organisations and institutions involved, describes both the practical and legal issues of the proposed EU PNR data system.

Part One describes the content of the Commission's proposal, but also deals with questions and issues raised on the basis of this proposal within the EU Council. To assess the practical meaning and consequences of this PNR proposal, Part One additionally considers existing measures directly related to the current proposal, including the aforementioned Directive 2004/82/EC, the EU–US PNR Agreement and other large-scale information systems within the EU.

Part Two analyses the legal implications of the proposed EU PNR system. Emphasising that the EU and its member states are bound by international, EU and national standards on human rights, this part focuses on the limitations imposed by data protection rights, the right to private life and the prohibition of discrimination. The following important data-protection principles are dealt with: the purpose limitation principle, data retention time limits, individual access and correction rights, and the tasks and powers of data protection authorities (at the EU and national levels).

Part Three includes some final remarks and recommendations.

PART ONE. THE DRAFT FRAMEWORK DECISION AND RELATED INSTRUMENTS AND LAW PROPOSALS

1. The transfer of API data – Directive 2004/82/EC

In April 2004, the Council adopted Directive 2004/82/EC on the obligation of air carriers to transmit passenger data to the border control authorities of the EU member states.[1] In contrast with the EU–US Agreement on PNR data, this Directive concerns the transfer of advanced passenger information (API) data, which is to be differentiated from passenger name records, to be dealt with below. API concerns data from the machine-readable zone of the passport, including name, date of birth, passport number and nationality. PNR data includes the data that are registered by the airline companies or travel agencies when a traveller makes a reservation, including the individual's name, seat number, travelling route, booking agent, etc. The most important difference between API and PNR data is that the information that can be extracted from PNR data mainly depends on the information the passenger submits him- or herself to the reservation system. Therefore, with respect to passport information, API data offers national officers more objective and permanently valid information, permitting the identification of individuals, whereas PNR data is more often used in profiling, offering national officers information on the background of the individual and his or her possible relations with other persons being sought.

Following Directive 2004/82/EC, EU member states must oblige carriers to transmit at the request of the authorities responsible for border checks, by the end of check-in, information concerning the passengers they will carry (Article 3). The fact that the data must only be transmitted in response to a prior request is an important difference compared with the proposed PNR framework decision, which will include the systematic transmission of each flight entering or leaving from the territory of a member state. On the basis of Directive 2004/82/EC, when carriers fail to observe this obligation – by not transmitting the required data or by transmitting incomplete or false data – member states should take the necessary measures to impose sanctions, including a maximum fine of €5,000 and a minimum one of €3,000 (Article 4).

Shortly before the final adoption of the Directive, despite earlier agreements reached within the Council on a strict purpose limitation, two important extensions were included in the draft text after pressure on the part of the UK. First, in Article 6 of the Directive an exception was added to the general rule that the data transferred to border authorities must be deleted within 24 hours of their transmission: they may be stored for a longer period if the data are needed "for the purposes of exercising the statutory functions of the authorities responsible for the external border checks in accordance with national law and subject to the data protection provisions under Directive 95/46/EC". Second, Article 6 provides that member states may also use the passenger data for law enforcement purposes. Especially this latter amendment to the original proposal extends the purpose of the Directive significantly, raising the question of whether this goal of the Directive could still be based on its current legal foundation: Articles 62(2) (a) and 63(3)(b) of the EC Treaty. Furthermore, Article 6 and the explicit reference in Preamble 12 of this Directive to the purpose limitation principle of Article 6(1)(b) of Directive 95/46/EC seem to include a (twofold) contradiction.

[1] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004.

Either the sole purpose of Directive 2004/82/EC is to combat illegal immigration, in which case further use for law enforcement purposes will infringe the rule of purpose limitation in Directive 95/46/EC, or the API Directive clearly implies the use for law enforcement purposes, but then this use will fall outside the scope of Directive 95/46/EC, as is provided in Article 3 of this Directive.

The implementation date of this Directive exceeded 5 September 2006. Although the majority of the member states (except Denmark, Spain and Poland) adopted measures of implementation, in many countries the required data systems are not yet operational. In April 2008, the European Commission informed the UK House of Lords that there was no clear picture on whether the data are useful for the purposes for which they are collected.[2]

2. The draft framework decision on the use of PNR for law enforcement purposes

2.1 Commission proposal: COM(2007) 654

In addition to the existing Directive on the transfer of API data, in November 2007 the European Commission published a proposal for a Council framework decision on the use of PNR for law enforcement purposes.[3] As distinct from Directive 2004/82/EC, whose sole purpose is the fight against illegal immigration, the central purpose of this proposal is preventing and combating terrorist offences and organised crime. According to the European Commission's *Impact Assessment* study, PNR data can be useful in five ways for law enforcement purposes:

- running PNR data against alert systems to identify known terrorists and criminals;
- identifying (unsuspected) passengers connected to known terrorists or criminals (for example when they use the same address, credit card number or contact details);
- identifying "high risk passengers" by running PNR data against a combination of "characteristics and behavioural patterns";
- identifying "high-risk passengers" by running PNR data against risk intelligence relevant at a certain time; and
- providing intelligence on travel pattern associations after a terrorist offence has been committed.[4]

Where the first two goals include the identification of individual persons – namely terrorists or criminals or persons connected to them who are known at the time of the

[2] House of Lords, European Union Committee, *The EU/US Passenger Name record (PNR) Agreement*, London, 5 June 2007.

[3] European Commission, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654, Brussels, 6 November 2007; see also the Commission's *Accompanying document to the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes – Impact Assessment*, SEC(2007) 1453 of 6 November 2007, and its summary *Accompanying Document to the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, Commission Staff Working Document, SEC(2007) 1422, Brussels, 6 November 2007.

[4] See the European Commission's *Impact Assessment* study (SEC(2007) 1453), 2007 (*supra*), pp. 8–9.

searches – the third and fourth goals include the identification of high-risk passengers who are unknown at the time of running the PNR data by using profiles or intelligence available at that time. The fifth goal does not address the identification or search for individual passengers at all, but only aims at establishing new profiles or providing new information on "travel or behavioural patterns".

The reasons for submitting this proposal, as set out by the Commission in its Explanatory Memorandum, are a little ambiguous. On the one hand, the Commission refers to the fact that only a limited number of member states adopted legislation in this field, meaning "that the potential benefits of an EU wide scheme in preventing terrorism and organised crime are not fully realised".[5] This seems to indicate that the proposal is an autonomous initiative of the Commission to tackle threats to security in the EU within the general goals of creating a 'European area of freedom, security and justice'. This view is supported by the fact that at the time the Commission's proposal was presented, only the UK, France and Denmark had already enacted primary legislation for the capture and use of PNR data. On the other hand, the Commission emphasises the necessity of a harmonised approach: "[A] harmonised approach makes it possible to ensure EU wide exchange of the relevant information." This goal is recalled by the Commission when explaining the choice of instruments: "As the aim is approximating member states' legislation, other instruments than a Framework Decision are not appropriate."

The Commission's proposal provides for the duty of air carriers to transmit the data of their passengers of international flights to the member state on whose territory the flight is entering, departing or transiting. According to the proposal, the data must be made available 24 hours before the scheduled flight departure to so-called 'passenger information units' (PIUs) to be established in each member state. With the establishment of the PIUs, the Commission's proposal envisages the decentralised collection of PNR data, considering this a better policy option to protect data and to minimise costs for its setup and operation. The data may be retained for thirteen years: five years after their transfer to the PIU of the first member state on whose territory the international flight is entering, departing or transiting, and upon expiry of this period another period of eight years. During this second period, the data may be accessed, processed and used only with the approval of the competent authority and "only in exceptional circumstances in response to a specific and actual threat or risk related to the prevention or combat of terrorist offences and organised crime".

Article 8 of the Commission's proposal provided that passenger data could be transmitted to law enforcement authorities of third countries for the prevention, detention, investigation or prosecution of terrorist events or organised crime. As discussed below, this provision has been extended meaningfully during the Council negotiations.

2.2 Discussions within the EU Council

During the negotiations within the EU Council on the Commission's proposal, several issues have been raised for further discussion. These issues are summarised in the *Report on the thematic work carried out from July to November 2008* published by

[5] See the Explanatory Memorandum to the Commission's *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654, Brussels, 6 November 2007 p. 2 and p. 7.

the French presidency in November 2008.[6] An important question that has been dealt with in the Council is the functional and geographical scope of application of this proposed framework decision: whether it should be extended to other modes of transport and whether, in addition to international flights to and from the EU, all or some intra-Community flights should be covered. A second issue of discussion has been the widening of the purpose of the PNR framework decision to integrated border management, and aside from terrorist offences and organised crime, to other serious crime. Further discussion points have been the composition and specific tasks of the PIUs, including the applicable rules on data processing by the PIUs and the interconnection between the PNR database and the API database and other files on persons or objects sought or under alert with a view to determining the action to be taken (SIS).

In their meeting of 24 October 2008, the ministers of the JHA Council discussed additional characteristics of the future PNR system.[7] It was emphasised that the data to be forwarded to the public authorities would serve as input for analysing the terrorist and criminal threats, but would also be used in the context of individual inquiries. With regard to the transfer of PNR data on intra-Community flights, the Council noted that the cost/benefit ratio should be assessed before including these data in the system. Referring to the fact that some member states already collect these data at national discretion, the Council agreed to review this issue once the PNR system had been in operation for a few years. In its conclusions of October 2008, the Council gives an explicit suggestion of the possible extension of PNR data to other means of transport, stating that "PNR data are related to travel movements, *usually flights* and include passport data, name, address, telephone numbers, travel agent, credit card number, history of changes in the flight schedule, seat preferences and other information" (emphasis added).

During the Council discussions, the added value of PNR data for law enforcement purposes was described as follows:

> [T]he establishment of a PNR database offers both opportunities to analyze behavioral tendencies in criminal circles, on which basis the criminal risk on particular flights can be assessed, and opportunities to provide information for investigations by intelligence services, customs, police and the criminal justice system. It allows the proactive use of the information contained in it, with the aim of preventing crime and detecting crimes which have been committed or are being planned; also, thanks to the later use of data which have been stored, it may help to clear up unsolved crimes.[8]

This description clearly indicates the intended use of the PNR data for profiling purposes, in a proactive and repressive response to terrorism or security threats. It also indicates that the data may be used for the investigation of general crimes.

In the meeting of 27–28 November 2008, the JHA Council referred to the aforementioned presidency report on the thematic work, which according to the Council, would have resulted in "an increasingly clear vision of the practical scope and essential features of a possible European PNR system reconciling operational

---

[6] Note from the French presidency to the COREPER/Council, *Report on the thematic work carried out from July to November 2008*, Council Doc. 15319/1/08, Brussels, 20 November 2008.

[7] Council of the European Union, Conclusions of the 2899th meeting, Justice and Home Affairs, Luxembourg, 24 October 2008, Council Doc. 14667/08 (Presse 299), Brussels, 24 October 2008.

[8] See Council Doc. 15319/1/08, 20 November 2008, p. 7 (op. cit.).

effectiveness with respect for citizens' fundamental rights in general and personal data protection rights in particular".[9] The Council furthermore instructed the preparatory bodies within the Council to examine all outstanding legal and operational issues, and announced continued dialogue with the European Parliament, and in the member states with the national parliaments and economic operators. In the conclusions of both the October 2008 and November 2008 meetings, the Council notes that the PNR data to be forwarded prior to boarding is commercial information already collected by airlines for their own commercial purposes. This explicit note is meant to emphasise that transport organisations will not be required to collect extra information on their passengers.

2.3 Position of the European Parliament

In November 2008, the European Parliament (EP) adopted a critical Resolution on the Commission proposal for a Council framework decision on an EU PNR.[10] With this resolution, the EP decided to reserve its formal opinion on the framework decision once its concerns have been addressed. The resolution, prepared by Sophia in 't Veld and adopted by 512 votes in favour, 5 against and 19 abstentions, criticised in particular the lack of evidence that this instrument would be a legally justified and efficient tool in the fight against terrorism. Considering the communitarian principle of subsidiarity, the EP notes that the need for Community action has not been sufficiently demonstrated. Whereas the Commission claims that the aim of the measure is to harmonise national schemes, the EP points out that few member states have a system for the use of PNR data for law enforcement purposes. Therefore, according to the EP, rather than harmonising (non-existing) national systems, the Commission's proposal merely imposes a duty for member states to set up such a system. The EP adds that the Commission's proposal includes a decentralised scheme, meaning that the European added value is even less clear.

In its resolution, the EP expressed serious concerns about the protection of individuals' rights. According to the EP, since the proposed measures have a considerable impact on the personal life of Union citizens, their justification in terms of necessity, proportionality and usefulness in achieving their stated objectives needs to be convincingly substantiated. The EP therefore stressed that effective safeguards for privacy and legal protection must be put in place. More specifically, the EP proposed further clarification of the relationship between the use of PNR and other measures such as the API Directive, the Electronic System for Travel Authorisation, biometrics in passports, SIS, VIS and national border protection schemes. Furthermore, referring to the earlier European Court of Justice (ECJ) judgment on the legal basis of the EU–US PNR Agreement in *European Parliament v. Council*,[11] the EP urges the Commission to examine carefully which legal basis is appropriate for the proposals as well as the accompanying measures. Other points of important criticism by the EP concern the lack of a precise purpose limitation in the proposal, the use of profiling and further use of sensitive data, the retention periods and transfers of PNR

[9] Council of the European Union, Conclusions of the 2908th meeting, Justice and Home Affairs, Brussels, 27–28 November 2008, Council Doc. 16325/08 (Presse 344), Brussels, 27 November 2008.

[10] European Parliament, Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of PNR for law enforcement purposes, B6-0615/2008, 2008(a).

[11] Joined cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union and Commission of the European Communities*, 30 May 2006.

data to third countries. Finally, the EP emphasised the importance of a clear definition of the role and powers of the PIUs "in particular in terms of transparency and democratic accountability and in order to lay down appropriate data protection rules".

2.4 Comments of the Association of European Airlines

Air transport operators have carefully followed the negotiations on the framework decision, being aware that its implementation involves extra costs and efforts for their organisations.[12] Therefore, in the first place airline companies have advocated the greatest possible harmonisation of the obligations imposed on them to limit the cost and the burden of legal responsibilities. Also, the Association of European Airlines (AEA) has repeatedly underlined that airlines or private entities should not be systematically required to collect passenger data on behalf of governments for purposes not related to aviation.[13] As the AEA stated in its position paper of December 2007, the "security of citizens cannot be the responsibility of airlines: this should remain the exclusive task of national [a]uthorities". In its comments of 2007, the AEA also questioned the level of harmonisation in the Commission's proposal, considering that a framework decision would not be the appropriate legal instrument to guarantee the goals pursued by the Commission. According to the AEA, this did not seem to be the intention of the Commission, referring to the Explanatory Memorandum and stating that this instrument "leaves as much scope as possible to the national decision makers". The AEA stressed the preference of airlines for a central collection/filtering system at the EU level.[14] The AEA regrets the European Commission's choice of a decentralised system, whereby airlines would have to transmit data to national PIUs. According to the AEA, this could imply multiple transmission requirements and extra costs for the air carriers. The AEA also expressed its concern about the possible impact of the EU requirements on international relations. The AEA referred to the growing number of third countries asking for reciprocity and requested clarification on the management of relations with these third countries, advocating that these relations be dealt with at the EU level.

Dealing with the provision on sanctions against airlines not transmitting data or transmitting incomplete or erroneous data, the AEA emphasises that the PNR only contains data "that are actually provided by the passenger", and therefore PNR data will almost always be incomplete even in terms of API data. According to the AEA, airlines have no possibility to check the accuracy of data provided by the passenger voluntarily and thus they cannot be held liable for incorrect data.

2.5 Position of the European Data Protection Supervisor

In his opinion of December 2007 on the draft proposal for the framework decision, Peter Hustinx, the European Data Protection Supervisor (EDPS), puts this proposal in the context of other measures dealing with the transmission of PNR data, including

---

[12] Council Doc. 15319/1/08, 20 November 2008, p. 3 (op. cit.).

[13] Association of European Airlines (AEA), *Comments on the European Commission Proposal to the Council of the European Union for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, AEA, Brussels, 5 December 2007 and *Policy Paper on transfer of airline passenger data to governments*, AEA, Brussels, April 2008 (retrieved from www.aea.be).

[14] See the AEA's *Policy Paper on transfer of airline passenger data to governments*, April 2008 (*supra*).

the aforementioned Directive 2004/82/EC as well as the EU agreements with third countries, including the US, Canada, Australia and South Korea.[15] The EDPS emphasises that the current proposal for the transmission of PNR data for law enforcement purposes is a further step in a movement towards "a routine collection of data of individuals who are in principle not suspected of any crime". In his comments, the EDPS concentrates on four main issues:

- the legitimacy of the intended proposal, including its purpose, necessity and proportionality assessed against the criteria of Article 8 of the EU Charter on Fundamental Rights;
- the data protection regime applicable to the proposed data processing operations;
- the quality of the recipients of data at the national level, including the quality of the PIUs, intermediaries and competent authorities designated to perform risk assessment and analysis of passenger data; and
- the conditions of transfer of data to third countries.

Concerning the first question of legitimacy, including the criterion of necessity of the proposed measure, the EDPS notes that in the *Impact Assessment* study when referring to other national PNR systems put in place, the Commission fails to give precise facts and figures relating to those systems. The EDPS criticises the mere reference to the reporting of "numerous arrests" with regard to "various crimes" in the UK system and observes that no details are given about the US programme, except that "the EU has been able to assess the value of PNR data and to realize its potential for law enforcement purposes". The EDPS goes on to point out that not only is there a lack of precise information on concrete results in the proposal itself, but also that reports published by other agencies, such as the US Government Accountability Office, do not confirm at this stage the efficiency of the measures (points 27–28). Considering the criterion of proportionality, the EDPS recalls other large-scale systems monitoring the movement of individuals within or at the borders of the EU, whether in operation (the SIS) or about to be implemented such as the VIS. According to the EDPS, the way in which they can already contribute to in-depth and comprehensive analysis should be subjected to "in-depth and comprehensive analysis, before deciding to establish a new form of systematic scanning of all persons leaving or entering the EU by plane" (point 34). Therefore, as to the legitimacy of the proposal, the EDPS concludes clear and undeniable elements of justification are missing and that the necessity and proportionality tests have not been fulfilled.

As to the matter of the applicable data protection regime, the EDPS questions whether a third-pillar instrument creates legal obligations on a routine basis for law enforcement purposes upon private or public sector actors falling outside the framework of law enforcement cooperation. With this conclusion, the EDPS seems to draw from the conclusions of the ECJ in the aforementioned judgment in *European Parliament v. Council*; however, according to the EDPS the case of this judgment

[15] European Data Protection Supervisor, Opinion on the draft proposal for a Council Framework Decision on the use of Passenger Name Records (PNR) data for law enforcement purposes, EDPS, Brussels, 20 December 2007.

would have been different to the present EU PNR proposal.[16] Moreover, the EDPS points out that the relationship between the current PNR proposal and the Framework Decision on the protection of personal data for the third pillar remains unclear. This lack of clarity, according to the EDPS, may result in a lack of legal certainty about the applicable data protection regime, for example in relation to which provision on purpose limitation would apply, noting that the Data Protection Framework Decision allows processing for wider purposes compared with the PNR proposal and Directive 95/46/EC. Also, the EDPS argues that the different regimes that would apply at the national level would have a major impact primarily on the exercise of the rights of the data subjects, especially concerning the rights of access and rectification of data. The data subject risks being confronted not only by different competent entities (the airline companies, the PIUs and the law enforcement authorities) but also by different recipients of the data: the data may be transmitted to the PIU of the flight departure or arrival country and possibly also to the PIUs of other member states on a case-by-case basis.

On the third issue, the EDPS concludes that the draft PNR framework decision does not provide any specifications about the quality of the recipients of personal data collected by airlines, nor about the intermediaries or PIUs. As to the latter organisations, the EDPS underlines that while the proposal entrusts PIUs with very sensitive processing of information, it does not give any detail concerning their quality or the conditions in which they must exercise this competence. Additionally, the EDPS notes that the enforcement of an EU PNR system will be rendered difficult considering that law enforcement authorities have diverse competences depending on the national laws of the member states, including or not intelligence, tax, immigration or police functions.

Finally, dealing with the conditions of transfer to third countries, the EDPS highlights various serious gaps in the Commission's proposal. These include for example the lack of rules concerning the quality of consent of member states for forwarding data from one third country to another, the concurring rules on the transfer of data to third countries in the Data Protection Framework Decision, the question of reciprocity (the fact that other third countries will ask the EU for PNR data for flights from the EU to their territory) and the impact of the EU PNR proposal on existing agreements with third countries.

Raising other substantial issues and emphasising again the "unprecedented impact of the proposal in terms of fundamental rights", the EDPS finally advises against adopting this proposal under the present treaty framework, and instead waiting for the new legal structure foreseen by the Lisbon Treaty. This would safeguard a co-decision procedure and strengthen the legal grounds for the proposed measures.

2.6 Opinion of the EU Agency for Fundamental Rights

Rather unexpectedly, the EU Agency for Fundamental Rights (FRA) was invited by the French presidency in September 2008 to give its opinion on the proposed framework decision. In response to this invitation, the FRA published an extensive and critical opinion in October 2008. Where the FRA focuses on three fundamental

[16] The EDPS notes that the EU–US PNR Agreement concerns data transfer to the US Bureau of Customs and Border Protection in a "systematic fashion", whereas the proposed EU PNR system would create "obligations on a routine basis", yet does not clarify the precise difference.

rights – the right to private life, the right to data protection and the prohibition of non-discrimination – the general conclusions of the FRA about the legitimacy and proportionality of the proposed EU PNR system are comparable to those of the EDPS. In its opinion, the FRA gives an extensive analysis of the jurisprudence of the European Court of Human Rights (ECtHR) dealing with Article 8 of the European Convention on Human Rights (ECHR), protecting the right to private life and data processing by national authorities. Based on this jurisprudence, the FRA concludes that defined and precisely specified data-processing operations to be undertaken by authorities constitute an essential guarantee against arbitrariness in the imposition of restrictive measures. Such protection is even more important as regards secret surveillance measures, owing to the heightened risk of arbitrariness in such circumstances.[17] In its conclusions, the FRA finds that the proposal lacks these essential guarantees, containing open-ended and imprecise formulations, failing to give sufficient evidence that the collection and use of PNR data for law enforcement purposes is necessary and adds value to the fight against terrorism and organised crime.

The FRA recommends, before adopting the new EU PNR system, an evaluation of existing measures, including the VIS, SIS and the API Directive, with a view to determining why these measures do not suffice to provide the additional intelligence required. The FRA is particularly concerned about the consequences of the EU PNR system and its use for profiling and the right to non-discrimination as protected in various instruments by which EU member states are bound, including Article 21 of the EU Charter of Fundamental Rights. With regard to this practice of profiling based on passenger data, the FRA stressed that reports published on earlier measures of profiling (in e.g. Germany and the UK) do not confirm the efficiency of profiling on grounds based on or associated with ethnicity, national origin or religion. Rather, the FRA points out that available evidence suggests that these profiling practices, as a means of countering terrorism and organised crime, are unsuitable, ineffective and thus disproportional.

The FRA thus concludes that profiling based on stereotypical generalisations about ethnic, national or religious groups should be explicitly banned. The FRA also recommends – should the proposal be adopted – the close monitoring of who becomes targeted by the proposed risk assessment to ensure compatibility with the prohibition of discrimination.

3. Relation to other EU information systems

Within the EU, many instruments have recently been developed on the use of large-scale databases and the exchange of personal data.[18] The use of these instruments will be closely related to the use of passenger PNR data. Important in this respect are the proposals of the European Commission for a European border management strategy.[19]

[17] See the cases *Klass and others v. Federal Republic of Germany*, 6 September 1978, Application No. 5029/71, *Rotaru v. Romania*, 4 May 2000, Application No. 28341/95, and *Segerstedt-Wiberg and others v. Sweden*, 6 June 2006, Application No. 62332/00.

[18] For an overview, see Florian Geyer, *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CHALLENGE Research Paper No. 9, CEPS, Brussels.

[19] See the European Commission's Communication on Examining the Creation of a European Border Surveillance System (EUROSUR), COM(2008) 68, Brussels, 13 February 2008(a) and the Communication on Preparing the next steps in border management in the European Union, COM(2008) 69, Brussels, 13 February 2008(b).

The Commission's 'border package' of February 2008, including the proposal of an entry/exit system, allows the electronic recording of the dates of entry and exit of third-country nationals into and out of the Schengen area. This entry/exit system would enable national authorities to identify overstayers and to "take the appropriate measures".[20] Another proposal of the Commission includes the introduction of automated gates for "Bona Fide or Registered Travellers" enabling "the automated verification of travellers' identity without the intervention of border guards".[21] A machine will read the biometric data contained in the travel documents or stored in a system or database and compare them against the biometrics of the traveller, "accelerating border checks by creating automated separate lanes replacing the traditional control booths". Persons will be granted "registered traveller" status after appropriate screening on the basis of common vetting criteria, including a reliable travel history (no previous overstays; data to this effect can be retrieved from the entry/exit system), proof of sufficient means of subsistence and holding a biometric passport.

As mentioned above, in the discussions on the EU PNR data system, different options are to be discussed with regard to the interconnection with 'SIS-type files'. At present, the SIS is one of the most important databases used for border control and law enforcement purposes in the EU.[22] In January 2008, the SIS included nearly 23 million records on objects and persons.[23] Since its launch in 1995, the majority of personal data held in the SIS concerns third-country nationals to be refused entry on the basis of Article 96 SC.[24] The decision to report a third-country national in the SIS is primarily based on a national decision that this person is considered a threat to public order, public security or national security. Second, the decision can stem from a determination made through immigration law regarding the deportation, refusal of entry or removal of this person. The consequence of this decision to report an individual in the SIS is that the person in principle will be refused entry to every other Schengen state (which entails more than 27 Schengen states, including the non-EU member states Norway, Iceland and Switzerland). On the basis of an SIS alert, a third-country national can also be denied a visa or a residence permit, or even expelled or detained.

In a presidency note of October 2008 on the PNR framework decision, the following options are proposed: to interconnect SIS-type files with PNR data on all passengers on the flights selected; to do so only for those passengers deemed positive upon profiling; to assign interconnection to PIUs; or to assign interconnection to competent authorities.[25] The use of databases such as the SIS and the future SIS II,[26] including its

[20] See the European Commission's (2008a) Communication COM(2008) 69, p. 8 (*supra*).

[21] Ibid., p. 6.

[22] For more details on the SIS and the development of SIS II, see Evelien Brouwer, *Digital Borders and Real Rights: Effective remedies for third-country nationals in the Schengen Information System*. Leiden/Boston: Martinus Nijhoff Publishers, 2008.

[23] Council of the European Union, SIS Database Statistics, Note, Council Doc. 5441/08, Brussels, 30 January 2008.

[24] On 1 January 2008, of the 859,300 records on persons held in the SIS, 696,419 (82%) were third-country nationals reported for the purpose of refusal of entrance – see SIS Database Statistics, Council Doc. 5441/08, 30 January 2008 (*supra*).

[25] See the Note from the French presidency to the COREPER/Council (Council Doc. 14592/08) of 21 October 2008 (op. cit.).

use by consular staff in third countries for the issuing of visas, raises important issues concerning the responsibility and accountability of member states when running passenger data against this database. The SIS is based on the principle of mutual trust and the mutual enforcement of national administrative decisions. This means that Schengen states can invoke one another's decisions to legitimise their own acts on the basis of SIS information, including refusal at the borders, the rejection of visa applications or even expulsions. In this regard, it is important to recall the proposal to include so-called 'troublemakers' in the SIS.[27] The purpose of this proposal is to share information on persons "whom certain facts give reason to believe that they will commit significant criminal offences". The proposal gives no definition of "significant criminal crime" other than that this should fall within a category higher than that of petty crime likely to disturb public peace and have a considerable effect on the public's sense of security. With the shared information, persons, including EU citizens, could be barred from certain events by a refusal of entry to the territory of the EU member state concerned.

4. EU–US Agreement on the transfer of passenger data

The history of the current regulation of the transfer of passenger data to the US is well known and has been described elsewhere more elaborately.[28] Still, because of its relationship to the current EU proposals, it is important to deal briefly with the general background and experiences of the EU–US cooperation here as well. Based on the Aviation and Transportation Security Act of 19 November 2001 and the Enhanced Border Security and Visa Reform Act of 14 May 2002, European air carriers were obliged to transfer data to the US Bureau of Customs and Border Protection (CBP) from 1 January 2003. Because they feared these data transfers would infringe the standards of Directive 95/46/EC, and they risked being fined by EU data protection authorities, they consulted the European Commission. The Commission started negotiations with the US authorities, meanwhile advising the EU data protection authorities not to impose fines on air carriers transmitting data to the US authorities. The negotiations between the US and the Commission resulted in an interim agreement in February 2003. On the grounds of Article 25 of EC Directive 95/46, the Commission adopted a so-called 'adequacy decision' expressing that the US would ensure an adequate level of data protection, allowing the transfer of data from EC member states to the US.[29] This adequacy decision enabled the Council of

[26] Such use would be made on the basis of Regulation No. 1987/2006 on the establishment, operation and use of the second generation Schengen Information System, OJ L 381/4, 28.12.2006 and with regard to its use for police and judicial cooperation in criminal matters on the basis of European Council, Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information (SIS), OJ L 205, 7.8.2007.

[27] For earlier discussions on this proposal, see Council of the European Union, 2514th Council meeting of the Justice and Home Affairs Council, Luxembourg, 5–6 June 2003 (Council Doc. 9808/03, Presse 150). It was set on the agenda again in 2008 on 14 March (Council of the European Union, Note on Troublemakers, Council Doc. 7544/08, Brussels, 14 March 2008) and again on 23 December (Council of the European Union, Council Doc. 17608/08).

[28] See for example Paul de Hert and Rocco Bellanova, *Data Protection from a Transatlantic Perspective: The EU and US move towards an International Data Protection Agreement?*, Study for CEPS on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, September 2008.

[29] Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Border Customs Protection, OJ L 235, 6.7.2004.

the European Union to adopt the Agreement of 17 May 2004 between the EU and the US. The European Parliament 'successfully' sought the annulment of this agreement before the ECJ.[30] Its key complaint was that the provisions and powers granted in the EU–US Agreement would be too wide and constitute an interference with the individual's right of data protection; however, this was not the reason the ECJ annulled both the EU–US Agreement and the Commission's adequacy decision in its judgment of May 2006. The annulment was based on the ground that these instruments could not have their legal basis in the EU transport policy (first pillar), as the purpose of the EU–US Agreement was the enhancement of security and the fight against terrorism. Therefore, according to Article 3 of EC Directive 95/46 the Agreement and the adequacy decision also fell outside the scope of this Directive. Nevertheless, it is important to note that the ECJ started its judgment by referring to the provisions of the ECHR and in particular the right to private life as protected in Article 8 ECHR. Even if one were to conclude on the basis of this judgment that the transfer of passenger data to the US is not bound by the data protection provisions of Directive 95/46/EC, with the reference to Article 8 ECHR, it is clear the ECJ recognises that this right and the standards as developed by the ECtHR deriving from Article 8 ECHR apply. In its earlier judgment in the *Österreichischer Rundfunk* case, the ECJ confirmed the close connection between Directive 95/46/EC and Article 8 ECHR.[31] In this latter judgment, the ECJ also held that the applicability of the EC Directive must be interpreted broadly and not be limited to data processing directly linked to the freedom of movement as protected in the EC Treaty.

After having concluded an interim agreement in October 2006, the EU and the US Department of Homeland Security (DHS) signed a final agreement on the use of PNR in July 2007 and exchanged "Letters" including further details and commitments with regard to the use of PNR. In reaction to the ongoing discussions and the consequences for the protection of individual rights, the new EU–US Agreement was said to include some improvements compared with the text of 2004. For example, instead of the 34 kinds of data to be forwarded on the basis of the 2004 Agreement, the 2007 Agreement was said to include "only 19 elements of PNR data". It is apparent, however, that this reduction to 19 elements occurred through the merging of different categories, and in fact the Agreement obliges carriers to transfer the same kinds of data to the US authorities. A particular problem is the transfer and further use of sensitive data, including data revealing racial or ethnic origin, political opinions, religion, trade union membership and data concerning the health or sex life of the individual. To provide further guarantees on the use of these data, the text of the Letter annexed to the 2007 Agreement only provides that the CBP will use so-called 'code filters', which will delete all sensitive terms and codes mutually identified by the EU and the US. The Standard of Conduct providing guidance to CBP employees states that employees will not act or fail to act on an official matter in a manner that "improperly takes into consideration an individual's race, colour, age, sexual orientation, religion, sex, national origin, or disability". At this point, it is sufficient to

[30] Joined cases C-317/04 and C-318/04, 30 May 2006 (op. cit.). A negative effect of the 'successful complaint' before the ECJ was that the European Parliament set itself and the Commission even further aside with regard to the proceedings on the third-pillar agreement.

[31] Joined cases C-456/00, C-138/01 and C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others*, ECR I-4989, §§ 71-83.

note that "improperly" does not meet the criteria being applied on the basis of the non-discrimination principle that applies within EU law.[32]

Another problem raised during the discussions on the new EU–US Agreement was the fact that the US Privacy Act only applies to US citizens or to aliens lawfully admitted for permanent residence in the US. This meant that non-US citizens whose data are transferred to the US could not address the lawfulness or accuracy of the use or collection of these data within the US. This lack of legal protection was said to be resolved in the 2007 Agreement on the basis of a 'policy decision' by the US DHS to extend the administrative Privacy Act protections providing redress to data subjects seeking information about or correction of their PNR data to non-US citizens. Yet, the Privacy Act has not been amended for this purpose, nor is there any other legal basis for the widening of this legal protection. Also, it is doubtful whether this extension offers non-US citizens the same legal protection as US citizens. The possibility of 'redress' as referred to in the policy decision implies an administrative and not judicial procedure.[33] The 2007 EU–US Agreement itself does not include any reference to the individual rights or available remedies. On the contrary, it explicitly states that it "does not create or confer any right or benefit on any other private or public person or entity".[34]

Furthermore, it should be noted that some issues within the 2007 Agreement diminish the legal protection of individuals. For example, compared with the text of the 2004 Agreement, the purpose for which the data must be transferred has been widened. The goal of the 2004 Agreement was limited to the prevention and combating of terrorism and related crimes and other serious crimes, including organised crime, that are transnational in nature. According to the 2007 Agreement, in addition to these purposes, the data may also be used "where necessary for the protection of the vital interest of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law". In addition, the Agreement of July 2007 allows for further transmission of PNR data to other US governmental authorities (including federal, state, local and tribal agencies), as well as foreign governmental agencies and domestic or foreign organisations in either the public or private sector. The purposes for which this data may be transferred not only include public security or counterterrorism-related cases, but also the enforcement of civil or criminal laws.

Despite the emphasis of various organisations, including the European Parliament, the EDPS and the UK House of Lords, on the importance of review and making the reports of review publicly available, the 2007 Agreement does not include any safeguards pertaining to such transparency whatsoever. For example, the periodic joint review by US DHS and the EU, which is foreseen in the Agreement, does not include the involvement of national or EU data protection authorities. The modalities of how the review will be carried out were to be mutually agreed by the EU and the DHS. Earlier practices have shown that members of the EU team participating in the joint review of the implementation of the EU–US Agreement were hampered by

[32] This point is further dealt with in Part Two.

[33] See also Paul de Hert and Rocco Bellanova (2008), p. 34 (op. cit.).

[34] See the Agreement between the European Union and the United States of America (Brussels and Washington, D.C., 23–26 July 2007) on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ L 204/18, 4.8.2007.

procedural standards imposed by their US counterparts.[35] Limitations were imposed on the number of records that could be accessed by the EU team and on the "provision of hard copy versions of certain staff procedural guidance". All the members of the EU team were required to sign confidentiality agreements imposing criminal sanctions for any breach. One of the areas of concern as described by the EU team during the joint review was that until May 2005, the CBP was not able to identify complaints or requests with regard to EU PNR data, so it could not provide any information on whether there had been any complaints or requests from EU passengers. Moreover, the EU team recommended the provision of clearer guidance to CBP officers as to the meaning and interpretation of 'serious crimes that are transnational in nature', which forms part of the purposes for which the CPB may collect PNR data.

One of the goals of the negotiations between the EU and the US on the transfer of PNR data was to prevent different EU member states from signing separate bilateral agreements with the US authorities. This goal, however, does not seem to have been reached given that during 2008 the US DHS signed some Memoranda of Understanding with some of the EU governments on a visa waiver scheme. These Memoranda introduce electronic travel authorisation for EU citizens, including the exchange of personal data on passengers gathered by the relevant law-enforcement authorities and the transfer of PNR data. The transmission of the latter data should be 'consistent' with the PNR Agreement between the EU and US of July 2007. Yet 'consistent' is not the same as 'in accordance with'.

The PNR Agreement between the EU and the US cannot be dealt with separately from the more general development of information sharing between the EU and the US. For this purpose, general standards are being developed by the High Level Contact Group on information sharing and privacy and personal data protection.[36] It is important to note that in this framework, the negotiators pointed out the different interpretations of definitions used. For example, this was illustrated in the report of the High Level Contact Group on the definition of 'law enforcement purposes' by the EU and US authorities. EU law enforcement purposes means prevention, detection, investigation or prosecution of any criminal offence. The US negotiators, however, described this definition as follows: prevention, detection, suppression, investigation or prosecution of any criminal offence or violation of law related to border enforcement, public security and national security, as well as for non-criminal judicial or administrative proceedings related directly to such offences or violations. According to the High Level Contact Group, these different definitions reflect respective domestic legislation and history "but may in practice coincide to a large extent".[37] Although there has been tension between the EU and US for a number of years on the transfer of personal data from one continent to the other, on the occasion of the EU-US summit on Tuesday 10 June 2008 in Brdo (Slovenia) Europeans and Americans said they were ready to conclude an international framework agreement on data protection.

---

[35] European Commission, *Joint review of the implementation of the US Bureau of Customs and Border Protection of the Undertakings set out in the Commission Decision 2004/535/EC of 14 May 2004*, Commission Staff Working Paper, COM(2005) final, Brussels, 12 December 2005.

[36] See Council of the European Union, *Final Report by the EU–US High Level Contact Group*, Council Doc. 9831/08, Brussels, 28 May 2008. See also the EDPS, Opinion on transatlantic information sharing for law enforcement purposes: Progress is welcomed, but additional work is needed, EDPS, Brussels, 11 November 2008.

[37] Council of the European Union, Council Doc. 9831/08, 28 May 2008 (*supra*).

It is clear that the different measures dealing with use of passenger data affect both the right to privacy and the right to data protection. What receives less attention, except for the detailed comments of the Fundamental Rights Agency, is the right to non-discrimination and the consequences of the use of passenger data, and in particular the use of profiling for the protection of this fundamental right. This part of the study will focus on the relation of the EU PNR system to the right to private life and the right to non-discrimination. As data protection law has been dealt with elaborately by other organisations, for example the EDPS, only some main issues are considered below.

5. The right to private life – Article 8 ECHR

The jurisprudence of the ECtHR and the criteria used to conclude that there has been infringement of the right protected in Article 8 ECHR leave no doubt that private life is at stake. As has been underlined several times by the ECtHR, the systematic collection and storage of personal information, including administrative data, fall within the scope of Article 8 ECHR.[38] One very important decision is the judgment of 16 February 2000 in *Amann v. Switzerland*, applying Article 8 to the storage of information relating to an individual's private life by a public authority, regardless of the sensitivity of the data and regardless of the use that is effectively being made by third parties.[39] In *Rotaru v. Romania*, the ECtHR referred more explicitly to the criterion of systematic collection and storage.[40] This case concerned the complaint by Mr Rotaru about the information stored about him since 1948 by the Romanian Intelligence Services. According to the ECtHR, even public information may fall within the scope of private life when it is "systematically collected and stored in files held by the authorities". This would be all the more true when such information concerns a person's distant past.

5.1 Necessary in a democratic society

Dealing with the question of whether any interference in the right to private life meets the criterion 'necessary in a democratic society', the ECtHR generally leaves a wider margin of discretion to the national authorities when it comes to national security or the prevention of disorder or crime than it would in regular cases. Nevertheless, even when national governments invoke internal security objectives, the ECtHR requires evidence of a substantiated balance of the different interests at stake. Also, the ECtHR requires the availability of procedural guarantees concerning not only the scope and time that the specific measures are being used, but also to allow independent courts or authorities to assess the necessity and proportionality of the security measures.

The proposed EU PNR data system concerns systematic data processing on large groups of persons. These passengers, EU and non-EU citizens, are (generally) not suspected of any crime, nor are they the subject of a criminal investigation or security

[38] This jurisprudence has also been dealt with by the European Union Agency for Fundamental Rights (FRA) in the Opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, FRA, Vienna, 28 October 2008.

[39] See the case *Amann v. Switzerland*, 16 February 2000, Application No. 27798/95, ECHR 2000-II, § 68-70.

[40] See the case *Rotaru v. Romania*, 4 May 2000, Application No. 28341/95, ECHR 2000-V, §§ 43-44.

measures. The only reason their data are submitted to either the governments of third countries, or the law enforcement and immigration authorities of the member states, is because they have booked a flight. As the ECtHR in the aforementioned *Amann* judgment made clear, the fact that the information are only stored or transferred and not always subsequently used in practice is irrelevant for the application of Article 8 ECHR. The ECtHR developed criteria for the necessary balance of powers between the data-collecting authorities on the one hand and the protection of the interests and rights of the individual on the other. These criteria include limitations on the exercise of powers to store and use the information; the duty to inform the person concerned in advance about the storage of his or her information; clear definition of the kind of information that may be recorded, of the categories of individuals against whom surveillance measures may be taken and the purposes for which the information can be used. With respect to the latter criterion, in the case of *Segerstedt-Wiberg v. Sweden*, the ECtHR assessed in particular whether the powers of the Swedish security service to store information in secret police registers for 'special reasons', as provided under the Swedish Police Data Act, included unfettered powers for these authorities.[41] In this case, the ECtHR concluded that the scope of discretion conferred upon the competent authorities and the manner of its exercise were indicated with "sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference".

5.2 In accordance with the law

The criteria as developed by the ECtHR on the basis of Article 8(2) ECHR should also be taken into account when assessing the current proposals for the EU PNR system. Notably important are the criteria on the 'accessibility and foreseeability' of the law. In the *Huvig* and *Kruslin* case law, the ECtHR defined a set of criteria for lawful telephone tapping that should have been provided for in French law. These criteria include the categories of persons liable to have their telephones tapped by judicial order and the nature of the offences that may give rise to such an order; the lack of an obligation to set a limit on the duration of telephone tapping; the circumstances under which recordings may or must be erased or the tapes destroyed, in particular when an accused party has been discharged by an investigating judge or acquitted by a court.[42] Interestingly, a comparable list of criteria is given in *Rotaru v. Romania* with regard to the law regulating the collection, recording and the archiving of information in secret files. Assessing the 'quality' of the Romanian law involved, the ECtHR concluded that this law did not include any limits on the exercise of the powers on the storage and use of the information by the Romanian intelligence services. Furthermore, Romanian law did not specify what information could be collected or stored and against which categories of individuals or under what circumstances these surveillance measures were allowed. Also, the ECtHR denounced the absence of limits on the length of time for which the information could be stored.[43] In the view of the ECtHR, the criteria of "in accordance with the law" and "quality of law" of Article 8(2) require supervision procedures and adequate and effective safeguards against abuse of the rule of law.[44] Since the Romanian system did

[41] See the case *Segerstedt-Wiberg and Others v. Sweden*, 6 June 2006, Application No. 62332/00, § 79.

[42] See both cases of 24 April 1990, *Kruslin v. France*, Application No. 11801/95, Series A, 176A § 35, and *Huvig v. France*, Application No. 11105/84, Series A, 176B § 34.

[43] *Rotaru v. Romania*, § 41 (op. cit.).

[44] *Rotaru v. Romania*, § 43 (op. cit.).

not provide such safeguards or a supervisory mechanism, the ECtHR ruled that the refuted storage and use of information by the intelligence service was not "in accordance with the law".

Considering this criterion of 'accessibility of law', one has to note that the whole process of PNR data transmission on the basis of the draft framework decision shall be covered by at least four legal regimes: i) EC Directive 95/46 for the data collection by the air carriers, ii) the draft PNR framework decision, which will apply to the data transfers by the airline companies to the PIUs, iii) the Framework Decision on data protection for the data transfers to third countries, and finally iv) the data transfers between PIUs and national law enforcement authorities, which will be covered by national data protection law. Also, the legal rules dealing with the collection and use of passenger data, the competences of the PIUs, the powers of national authorities and the authorities of third countries, the rights of data subjects and data protection authorities are still insufficiently clear and precise. These deficiencies, as we have seen, have also been emphasised by the FRA, the EDPS and the European Parliament.

5.3 Limitations within the national constitutional laws

When dealing with the current EU measures for information processing, national authorities should not only take into account the EU and international standards of human rights, but also their own constitutional laws. In this regard, recent judgments of the German Constitutional Court have established some clear and strict limitations for the storage and use of personal data. For example, on 27 February 2008, the Constitutional Court annulled the new law of Nord Rhine Westfalen allowing secret spying on personal computers and the use of the internet, because these laws were in breach with the constitutional right to privacy.[45] For the same reason, on 11 March 2008 the Court annulled a new provision in the police laws of Hessen and Schleswig Holstein on the automatic identification and storage of vehicle registration plates of private cars.[46] These laws provided for the registration of these plates by video cameras without prior suspicion to enable the comparison of these data with information in the existing police files. Also on 11 March 2008, the Constitutional Court (partially) suspended (because of a so-called '*Eilantrag*' or interim appeal of 30,000 citizens) the German implementation act for the EC Directive on Data Retention.[47] Generally, criteria used by the German Constitutional Court to conclude that the refuted measures were in breach of the constitutional right to privacy were the lack of legal certainty or transparency, the absence of a clear purpose limitation, the disproportionality of the data processing measures and the absence of concrete justification for the data collection. This case law of the Constitutional Court in Germany, and especially the latter judgment dealing with the Data Retention Directive, are a signal that because of the structural shortcomings in the EU instruments themselves, the implementing measures at the national level risk annulment by national courts or supervisory authorities.

[45] Constitutional Court, 1 BvR 370/07, 27.2.2008.

[46] Constitutional Court, 1 BvR 2074/05, 13.3.2008.

[47] Constitutional Court, 1 BvR 256/08, 11.3.2008.

6. The right to data protection

An important step for the meaning of the right to data protection in practice has been its inclusion as a fundamental right in the EU Charter of 2000. Although this inclusion affirmed the separate and autonomous meaning of data protection, its relation to the right to private life remains clear.[48] Considering the current developments in the use of passenger data, the following central data-protection principles need careful examination:

- purpose limitation principle,
- prohibition of automated decision-making,
- quality of data,
- time limits,
- individual access and correction rights,
- supervision by national and European data protection supervisors,
- adequate level of data protection in third countries, and
- security of data.

Special attention is merited by the principle of *purpose limitation*, which is at risk of being undermined by the inclusion of vague and open criteria in the current proposals. According to Article 6.1(b) of EC Directive 95/46, personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes. This principle includes different layers of protection. First, it prohibits the collection of personal data for unknown or unspecified purposes. Second, it prohibits the use or disclosure of personal information for purposes other than the specific purpose for which the data have been collected. Third, the principle of purpose limitation provides that data should not be retained any longer than is necessary for the specified purpose. Purpose limitation is closely linked to the principle of purpose specification, which implies that data holders should specify and make transparent the purposes of the relevant data processing. Both the purpose limitation and the purpose specification principle reflect the idea that data processing should be foreseeable for the data subject and should not go beyond the reasonable expectations of the person concerned.[49] As we have seen above, in its jurisprudence on the protection of the right to private life, the ECtHR explicitly emphasised the importance of "foreseeability" concerning the processing of personal data by governmental authorities.[50]

As noted above, the Council currently envisages allowing the use of PNR data not only for the fight against terrorism and organised crime, but also for integrated border management and the investigation of other serious crimes. Also, the proposed

[48] This has been confirmed in the aforementioned case of *Österreichischer Rundfunk* (C-465/00), in which the ECJ ruled that if national courts were to conclude that national legislation with regard to the processing of personal data is incompatible with Article 8 ECHR, that legislation would also be "incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46".

[49] See Dag Elgesem, "The structure of rights in Directive 95/46 on the protection of individuals with regard to the processing of personal data and the free movement of such data", *Ethics and Information Technology*, Vol. 1, No. 4, pp. 283–293, 1999.

[50] See the judgment in the case *Peck v. United Kingdom*, 28 January 2003, Application No. 44647/98.

interconnection with other databases, including the SIS and VIS – open issues at present as to which authorities and third countries will obtain access to the passenger data – are important for the question of whether the standards of the purpose limitation principle are met.

Another subject to be dealt with further is the principle on the *prohibition of automated decision-making*. Article 15 of EC Directive 95/46 provides that every person has the right "not to be subject to a decision which produces legal effects concerning him or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.". In light of the current EU developments, in which measures on border and immigration control tend to be based increasingly on automated data processing, the banning of 'automated decision-making' becomes even more important. Data stored within a database or the outcome of group profiling should never be the sole basis for an individual decision.

Preamble 20 and Article 3(5) of the Commission's proposal of November 2007 provides that no enforcement action shall be taken by the PIUs or the competent authorities of the member states solely on the basis of the automated processing of PNR data. A new text has been proposed within the Council, stating that "the PIU's shall not take any decision which produces an adverse legal effect concerning a person or significantly affects him based solely on the automated processing of a passenger's PNR data".[51] A comparable provision has been included with regard to the tasks of the competent authorities in Article 4(6). This proposed provision is to be welcomed, but it should be taken into account that for individuals it is difficult to assess on which grounds, other than PNR data, he or she will be submitted for more specific checks or refused entry. For this reason, the prohibition of automated decision-making is closely related to the right of a person to be informed of the grounds of the decision-making.

7. Profiling and the right to non-discrimination

As has been made clear in the *Impact Assessment* study accompanying the proposal for the framework decision and in the discussions of the EU Council, profiling will be an important tool for the implementation of the EU PNR data system. Its meaning will be twofold. In the first place, PNR data transmitted by air carriers to national authorities of the EU member states will be assessed on the basis of current profiles, resulting in possible identification of high-risk passengers. Second, the transmitted PNR data will be used, by the PIUs or by the national authorities of the receiving states, for the establishment of new profiles to be used for current or later investigations.

Despite the sovereignty of governments in controlling their borders and differentiating their own citizens from foreigners and in using intelligence tools to safeguard internal security, it is clear that the powers of border guards are restrained by the right of non-discrimination as protected by the Convention on the Elimination of All Forms of Racial Discrimination (CERD), EC law and Article 14 ECHR.

[51] This is based on the last public version of the proposal (Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, Council Doc. 7656/3/08, Brussels, 19 June 2008).

7.1 Article 14 and the 12th Protocol to the ECHR

Article 14 ECHR obliges member states to secure the enjoyment of the rights and freedoms as protected in the ECHR without discrimination on any ground such as gender, race, colour, language, religion, political or other opinions, national or social origin, association with a national minority, property, birth or other status. Aside from Article 14 ECHR, Protocol No. 12 to the ECHR includes a right protecting the "enjoyment of any right set forth by law" without discrimination on the aforementioned grounds.[52]

The relevancy of the right of non-discrimination in the field of border controls has been underlined by the ECtHR in the case *Timishev v. Russia*.[53] This case concerned the complaint of a Russian national of Chechen ethnicity, who was refused passage across administrative borders within Russia by the Russian authorities. The ECtHR ruled that there was a violation of Article 14 ECHR in combination with Article 2 of the 4th Protocol (dealing with the freedom of movement). According to the ECtHR, "no difference in treatment which is based exclusively or to a decisive extent on a person's ethnic origin is capable of being objectively justified in a contemporary democratic society built on the principles of pluralism and respect for different cultures". The ECtHR also emphasised that racial discrimination is "a particularly invidious kind of discrimination and, in view of its perilous consequences, requires from the authorities special vigilance and a vigorous reaction" (para. 58). It should be emphasised that the individual's right to liberty of movement and freedom to choose his/her residence within the territory of a state as protected by the 4th Protocol applies to everyone lawfully within that state. This includes third-country nationals. The considerations in the *Timishev* case and the prohibition of different treatment that is solely based on ethnic origin has been repeated in the cases *Nachova v. Bulgaria* and *D.H. and others v. Czech Republic*.[54]

In this regard, it is important not to focus solely on the rights of EU citizens, as the underlying proposals will affect third-country nationals residing or seeking access to the territory of the EU member states as much if not more. As has been emphasised earlier by the Commissioner of Human Rights of the Council of Europe, this latter group of persons are especially vulnerable to wrongful actions or decision-making based on the use of incorrect or incomplete data: "While biometric identity documents, which operate between countries, are important security measures, the effect of mistake[s] on migrants will be much greater than on citizens where a computer malfunctions, and misidentifies an individual, or fails to record a legal entry, and so nullifies lawful entry; appeals should be a part of immigration law."[55]

---

[52] Council of Europe, Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No. 177. This protocol entered into force on 1 April 2005.

[53] See the case *Timishev v. Russia*, 13 December 2005, Application Nos. 55762/00 and 55974/00, paras. 58–59.

[54] See the cases *Nachova and Others v. Bulgaria* [GC], Application Nos. 43577/98 and 43579/98, ECHR 2005–, and *D.H. v. Czech Republic*, 13 November 2007, Application No. 57325/00, ECHR 2008/5.

[55] Council of Europe Commissioner for Human Rights, *The Human Rights of Irregular Migrants in Europe*, CommDH/IssuePaper (2007)1, Strasbourg, 17 December 2007.

7.2 UN Convention on the Elimination of Racial Discrimination

The International Convention on the Elimination of All Forms of Racial Discrimination or CERD has been ratified by all EU member states and must therefore be observed when implementing the PNR instruments at stake.[56] Article 1(1) CERD defines racial discrimination as any distinction, exclusion, restriction or preference based on race, colour, descent or national or ethnic origin that has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life. Article 2 of the CERD obliges the state parties to engage in no act or practice of racial discrimination against persons, groups of persons or institutions and to ensure that all public authorities and public institutions, national and local, shall act in conformity with this obligation (Article 2(1)(a)). Also, on the basis of Article 2.1(c), state parties must take effective measures to review governmental, national and local policies, and to amend, rescind or nullify any laws and regulations that have the effect of creating or perpetuating racial discrimination wherever it exists. Considering the definition of racial discrimination, Article 2(1)(a) therefore does not allow any justification for different treatment on the basis of ethnicity or origin by governmental authorities. The committee tasked with the supervision of the CERD in its General Comment No. 14 of 1993 with regard to the meaning of Article 1(1) only accepted the adoption of positive actions for certain groups as legitimate: "The Committee observes that a differentiation of treatment will not constitute discrimination if the criteria for such differentiation, judged against the objectives and purposes of the Convention, are legitimate or fall within the scope of Article 1, paragraph 4, of the Convention." Article 1(4) only includes differentiating measures taken for the sole purpose of securing adequate advancement of certain racial or ethnic groups or individuals requiring such protection as may be necessary to ensure such groups or individuals equal enjoyment or exercise of human rights and fundamental freedoms.

Even if the CERD does not prohibit distinctions, exclusions, restrictions or preferences made by a state party to this Convention between citizens and non-citizens, Article 1(3) of the Convention makes clear that national legal provisions concerning nationality, citizenship or naturalisation are only legitimate as far they do not discriminate against any particular nationality. This means that when particular measures are directed against persons of certain national or ethnic origin, they may be in breach of the CERD. With respect to border control measures, this meaning of the CERD has been emphasised in the conclusions of the UK House of Lords in 2004 in the case *R v. Immigration Office at Prague Airport*.[57] This case concerned the so-called 'pre-flight checks' by British officials at the airport in Prague to prevent illegal immigration to the UK. Based on special instructions published by the UK ministry of home affairs, these officials specifically checked Czech nationals of Roma origin. In her conclusions, which were supported by the majority of the House of Lords, Baroness Hale concluded that these pre-flight checks entailed an infringement of Article 1(2) CERD.

---

[56] Adopted by the UN General Assembly Resolution 2106, 21 December 1965, with entry into force 4 January 1969.

[57] House of Lords, 9 December 2004, *R. v. Immigration Office at Prague Airport and another (Respondents) ex parte European Roma Rights Centre and others (Appellants)* [2004], UKHL 55, para. 101.

7.3 Article 8 ECHR and the stigmatising effect of data profiling

In the aforementioned opinion on the draft PNR framework decision, the FRA underlined the adverse effects of profiling – alienating and victimising certain ethnic and religious groups, and provoking a deep mistrust of the police. An important signal to the EU legislator when developing the EU PNR system further should be the judgment of the German Constitutional Court on the practice of '*Rasterfahndung*' or data profiling by the German police in their fight against terrorism.[58] In this judgment of 2006, concerning the complaint of a Moroccan student, the Court declared the German practice of data profiling unlawful because it would include a disproportional breach of the constitutional right to privacy. For this conclusion, the German Court explicitly referred to the extended scope of the collection of information, the use of many different databases, the increased risk for the person concerned of becoming the target of a criminal investigation. The Constitutional Court also referred to the possibility of stigmatising a group of persons in public life, especially when it concerns, as in the refuted practice of data profiling, persons from specific countries who are also Muslim. In this judgment, the German Constitutional Court explicitly emphasised the higher risk of certain groups being affected by data profiling measures:

> For those persons whose constitutional rights it affects, data profiling means a higher risk of becoming the target of further official investigative measures. This has been demonstrated to a certain extent by the outcome of the data profiling implemented since 11 September 2001. …Furthermore, the very fact of police data profiling having been carried out according to certain criteria – if it becomes known – can have a stigmatising effect on those who meet these criteria. …It is relevant, with regard to the intensity of the effects of the data profiling carried out since 11 September 2001, that it is targeted at foreigners of certain origins and Muslim beliefs, which always involves the risk of spreading prejudice and stigmatising these population groups in the public perception.[59]

According to the Constitutional Court, such a measure could only be justified by a concrete danger of a terrorist attack that would cause great harm, for which the risks of such an attack are based on concrete facts. The Court considered that the general situation of threat that has existed since 9/11 or tensions relating to foreign policy matters are not sufficient reasons to justify the practice of data profiling.

More recently, in *S. and Marper v. the United Kingdom*, the ECtHR also warned against the risks of the stigmatising effect of long-term, systematic storage of

---

[58] Judgment of the Bundesverfassungsgericht [Constitutional Court] of 4 April 2006, 1 BvR 518/02 published on 23 May 2006. The author has dealt with this judgment previously in "The use of biometrics in EU data bases and identity documents: Keeping track of foreigner's movements and rights", in Juliet Lodge (ed.), *Are you who you say you are? The EU and Biometric Borders*, Nijmegen: Wolf Legal Publishers, 2007, pp. 45–66.

[59] Paras. 110–112 state:

> Die Rasterfahndung begründet für die Personen, in deren Grundrechte sie eingreift, ein erhöhtes Risiko, Ziel weiterer behördlicher Ermittlungsmaßnahmen zu werden. Dies hat etwa der Verlauf der nach dem 11. September 2001 durchgeführten Rasterfahndung gezeigt. [...] Ferner kann die Tatsache einer nach bestimmten Kriterien durchgeführten polizeilichen Rasterfahndung als solche – wenn sie bekannt wird – eine stigmatisierende Wirkung für diejenigen haben, die diese Kriterien erfüllen. [...] So fällt etwa für die Rasterfahndungen, die nach dem 11. September 2001 durchgeführt wurden, im Hinblick auf deren Eingriffsintensität ins Gewicht, dass sie sich gegen Ausländer bestimmter Herkunft und muslimischen Glaubens richten, womit stets auch das Risiko verbunden ist, Vorurteile zu reproduzieren und diese Bevölkerungsgruppen in der öffentlichen Wahrnehmung zu stigmatisieren.

fingerprints and DNA samples of individuals, including minors, who were suspected of having committed criminal offences, but not convicted.[60] In this judgment, the ECtHR found that the applicable UK law violated Article 8 ECHR, particularly on the grounds that these data were stored for indefinite periods and concerned unconvicted persons, and it was thus disproportional. Important in this regard is the consideration in para. 119, in which the ECtHR stated that it was struck by "the blanket and indiscriminate nature of the power of retention in England and Wales" and the fact that "the material may be retained irrespective of the nature of gravity of the offence with which the individual was originally suspected or of the age of the suspected offender". The ECtHR also based its conclusion that there was a violation of Article 8 ECHR on the grounds that there are only limited possibilities for the individual to have the data removed from the nationwide database or to have the materials destroyed (para. 35 of the judgment). Moreover, there was no provision for independent review of the justification for the retention according to the defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

7.4 Inclusion of non-discrimination clauses in the PNR proposal

It is to be welcomed that in the Commission's original proposal, Preamble 20 and Article 3(3) provides that no enforcement action shall be taken by the PIU or the competent authorities of the member states only by reason of a person's race or ethnic origin, religious or philosophical beliefs, political opinion or sexual orientation. This provision has been repeated in Articles 3(3) and 4(6) of the last public version of the framework decision as amended by the Council.[61] Article 3(3) of this Council text furthermore provides that "no risk assessment criterion shall be based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual orientation". These standards, when adopted, provide important safeguards against the discriminatory treatment of passengers. Still, it should be taken into account that profiling as such is always based on the mechanism to differentiate among various groups of persons, on the basis of specific criteria. Even if these criteria are not the (prohibited) grounds mentioned above, certain features – such as food preferences or the use of medicines or names – could be indicative of someone's religion, health or ethnic origin. Before adopting new profiling measures, current instruments used within the EU member states should be systematically evaluated to investigate their possible discriminatory effects.

[60] See the case *S. and Marper v. United Kingdom*, 4 December 2008, Application Nos. 30562/04 and 30566/04, para. 122.

[61] Council of the European Union, Council Doc. 7656/3/08, 19 June 2008 (op. cit.).

PART THREE. GENERAL CONCLUSIONS

8. Assessing the necessity and proportionality of the EU PNR system

Within the EU, tools have been developed without providing supporting evidence that these measures actually assist in the prevention or detection of terrorism or serious crimes. The failure to justify the necessity or proportionality is unlikely to be solved by sunset or review clauses enabling the legislator to adopt at a later stage amendments or improvements to the instruments at stake. Nor can the intrusive effects of data systems be taken away by a general reference to applicable data protection rules, or by granting the data subject limited rights such as the right to apply for access or correction. The exercise of these rights will not (or only marginally) prevent the risk of wrongful use or misuse of data, nor will it prevent the general loss of privacy or data protection caused by the use of surveillance systems.

9. Harmonisation of national practices and definitions

An important problem of the current proposals is the lack of harmonisation of the underlying definitions used for the implementation of these measures. This point concerns for example the use of 'terrorism' or 'serious organised crime' for describing the purpose of the draft PNR framework decision. This means that data processing is taking place on the basis of criteria depending on the policy and priorities of the 27 member states and of third countries gaining access to these data as well. This situation raises doubts about the efficiency of these measures to address joint problems in a coherent way. This problem is not unique to the PNR proposal. It also applies to the inclusion of data in EU databases, for example the registration of 'inadmissible aliens' in the SIS (and the proposal to report 'violent troublemakers' in the SIS). That the diverse instruments are meant to be connected for different purposes and by various national authorities will only increase the problems for assessing the usefulness and reliability of the data. As discussed above, the problem of the use of different definitions also applies to the general cooperation between the US and EU authorities on information sharing.

Dealing with the draft PNR framework decision, the current definitions of the tasks and competences of the PIUs, the national authorities that will gain access to the passenger data and the purposes for which the data may be used are also very vague and open. They allow the national legislators of the member states a wide margin of discretion and offer data protection authorities and courts insufficient means of controlling the use of passenger data by national authorities. The harmonisation of the criteria is necessary to provide the individual in question with effective remedies in which national courts or tribunals are able to assess the criteria for which data have been collected, transmitted or used.

10. Data subject rights: Financial redress or compensation

An important issue concerning the future use of EU databases, including PNR data, is the possibility of lodging a claim for damages caused by the use of information or data processing by governmental organisations in breach of Article 8 ECHR. This applicability of Article 6 ECHR in relation to damage caused by government information files is recognised by the ECtHR in the aforementioned judgment in

Rotaru v. Romania.[62] The ECtHR considered the applicant's claim for compensation for non-pecuniary damage and costs a civil claim within the meaning of Article 6(1) ECHR. The failure of the national courts to consider the claim in this case violated the applicant's right to a fair hearing within the meaning of Article 6(1) ECHR.

To ensure that the rights of individuals are respected with regard to the storage and use of their personal data, the current legal proposals should include strict rules on the liability of the different authorities involved. Only the inclusion of such rules will allow courts or data protection authorities to impose sanctions when necessary.

11. Effective control by national data protection authorities

Finally, before expanding the existing EU information network, research must be undertaken on the practical effects and meaning of the role of data protection authorities. Until now, the scope of review by data protection authorities has been restricted and their independence and efficiency is threatened by their lack of power and financial resources. It is important that these data protection authorities perform further investigations on the accuracy and reliability of information being stored, not least because of the irregularities already found in existing databases such as the SIS.[63] General inquiries or audits make national authorities aware of their obligations regarding the lawfulness and quality of data held in their systems. Such activities also emphasise the watchdog role of national and European data-protection authorities.

[62] *Rotaru v. Romania*, §§ 74–79 (op. cit.).

[63] The reports of national data protection authorities indicating a lack of accuracy and legitimacy of national SIS reports has been described in Evelien Brouwer (2008, op. cit.).

BIBLIOGRAPHY

Selected institutional and organisational references pertaining to EU legislation

Association of European Airlines (AEA) (2006), *Position Paper: Background Information on Passenger Data Transfer*, AEA, Brussels, 22 August.

Association of European Airlines (AEA) (2007), *Comments on the European Commission Proposal to the Council of the European Union for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, AEA, Brussels, 5 December.

Association of European Airlines (AEA) (2008), *Policy Paper on transfer of airline passenger data to governments*, Brussels, AEA, April.

Council of the European Union (2008), *Report on the thematic work carried out from July to November 2008*, Council Doc. 15319/1/08, 20 November.

European Commission (2008a), Communication on Examining the Creation of a European Border Surveillance System (EUROSUR), COM(2008) 68, Brussels, 13 February.

European Commission (2008b), Communication on Preparing the next steps in border management in the European Union, COM(2008) 69, Brussels, 13 February.

European Data Protection Supervisor (EDPS) (2007), Opinion on the draft proposal for a Council Framework Decision on the use of Passenger Name Records (PNR) data for law enforcement purposes, EDPS, Brussels, 20 December.

European Data Protection Supervisor (2008), Opinion on transatlantic information sharing for law enforcement purposes: Progress is welcomed, but additional work is needed, EDPS, Brussels, 11 November.

European Parliament (2008a), Recommendation of 22 October 2008 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service.

European Parliament (2008b), Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of PNR for law enforcement purposes, B6-0615/2008.

European Union Agency for Fundamental Rights (FRA) (2008), Opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, FRA, Vienna, 28 October.

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

Selected institutional references pertaining to US legislation

European Commission (2005), *Joint review of the implementation of the US Bureau of Customs and Border Protection of the Undertakings set out in the Commission Decision 2004/535/EC of 14 May 2004*, Commission Staff Working Paper, COM(2005) final, European Commission, Brussels, 12 December.

US Department of Homeland Security (DHS), Privacy Office (2008), *A Report concerning Passenger Name Record Information Derived from Flights between the US and the European Union*, DHS, Washington, D.C., December.

Other bibliographical references

Brouwer, Evelien (2007), "The use of biometrics in EU data bases and identity documents: Keeping track of foreigner's movements and rights", in Juliet Lodge (ed.), *Are you who you say you are? The EU and Biometric Borders*, Nijmegen: Wolf Legal Publishers, pp. 45–66.

Brouwer, Evelien (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden/Boston: Martinus Nijhoff Publishers.

Elgesem, Dag (1999), "The structure of rights in Directive 95/46 on the protection of individuals with regard to the processing of personal data and the free movement of such data", *Ethics and Information Technology*, Vol. 1, No. 4, pp. 283–293.

Geyer, Florian (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CHALLENGE Research Paper No. 9, CEPS, Brussels.

Guild, Elspeth and Evelien Brouwer (2006), *The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief No. 109, CEPS, Brussels, July.

Guild, Elspeth, Sergio Carrera and Florian Geyer (2008), *The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?* Policy Brief No. 154, CEPS, Brussels, 5 March.

De Hert, Paul and Rocco Bellanova (2008), *Data Protection from a Transatlantic Perspective: The EU and US move towards an International Data Protection Agreement?* Study for CEPS on behalf of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, September.

Kuipers, Frank (2007), *No Dream Ticket to Security: PNR Data and Terrorism*, Clingendael Netherlands Institute of International Relations, The Hague.

Lodge, Juliet (ed.) (2007), *Are you who you say you are? The EU and Biometric Borders*, Nijmegen: Wolf Legal Publishers.