available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The EU PNR framework decision proposal: Towards completion of the PNR processing scene in Europe

Paul De Hert [a,b], *Vagelis Papakonstantinou* [a,c,1]

[a] *Vrije Universiteit Brussels (LSTS), Belgium*
[b] *Tilburg University (TILT), The Netherlands*
[c] *PKpartners Law Firm, Athens, Greece*

Keywords:
Data protection
PNR
EU PNR
Bilateral EU PNR agreements

ABSTRACT

The entry into force of the Lisbon Treaty has suspended discussions over the release of a EU PNR processing system. Plans to introduce an intra-EU PNR processing system initiated since 2007, although strongly supported by the Commission and the Council, did not bear fruit before the ratification of the Lisbon Treaty and the, institutional, involvement of the Parliament. While discussions have been suspended since October 2009 and most probably a new draft proposal will be produced, it is perhaps useful to present in brief the proposal currently in place so as to highlight its shortcomings for European data protection and suggest ways individual protection may be strengthened in future drafts.

1. Introduction[2]

The entry into force of the Lisbon Treaty has suspended discussions over the release of a EU PNR processing system. Luckily, according at least to data protection proponents, plans to introduce an intra-EU PNR processing system (in the form of a "Framework Decision on the use of Passenger Name Records (PNR) for law enforcement purposes") initiated since 2007, although strongly supported by the Commission and the Council, did not bear fruit before the ratification of the Lisbon Treaty and the institutional involvement of the Parliament in the process.

While discussions have been suspended as per the Parliament's request since October 2009[3] and most probably a new draft proposal for the regulation of PNR processing within the EU will be presented, it is perhaps useful to present in brief the proposal currently in place so as to highlight its shortcomings for European data protection and suggest ways individual protection may be strengthened in future proposals.

[1] Paul De Hert is professor at the Vrije Universiteit Brussels (LSTS) and associated professor at Tilburg University (TILT). Vagelis Papakonstantinou is scientific collaborator at the Vrije Universiteit Brussels (LSTS) and Partner in PKpartners Law Firm in Athens, Greece.

[2] The authors would like to thank Rocco Bellanova, Scientific Collaborator, Vrije Universiteit Brussels (LSTS) for his remarks.

[3] EU Passenger Name Record talks on hold in Council until Lisbon Treaty is ratified, European Parliament News, 6.10.2009 (ref. 20091006IPR61955).

2212-473X/$ – see front matter © 2010 Paul de Herts & Vagelis Papakonstantinou. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2010.05.008

2. The PNR processing scene

As is widely known by now, the term PNR data denotes records on passengers kept in computer reservation systems.[4] Such records may include the passenger's full name, date of birth, home and work address, telephone number, e-mail address, passport details, credit card details or method of payment, the names and personal information of emergency contacts, as well as details of any special meal requirements or seating preferences or any other similar requests.

Before 9/11, PNR data were mainly used by the air travel industry (arguably, marginally) in order to make an air travel reservation. They were not systematically collected, reservations could be made only with the person's initials and they generally attracted no great attention.

After 9/11, however, in the belief that the processing of PNR data could contribute to keep terrorists out of its country, the US Bureau of Border and Customs Protection (CBP), implementing the US Aviation and Transportation Security Act 2001, started asking since November 2001 international air carriers for access to their PNR data, which also had to improve in standards of accuracy and quantity.[5]

PNR data obviously constitute 'personal data' within the meaning of EU law. Regardless of the point of view adopted (Data Protection Directive, Convention 108, Data Protection Framework Decision[6]), PNR data undoubtedly fall under the category of "*any information relating to an identified or identifiable natural person*"[7] or "*any information relating to an identified or identifiable individual*",[8] and hence fall within the scope of the EU data protection texts.

Because the American request contradicted European airlines' data protection obligations concerning the PNR data they possessed (export to a third country without having first ensured an "adequate" level of protection), air carriers were faced with the dilemma as to which law to break. After repeated attempts at European Community level the issue was reconciled with the USA, an outcome however that only came after three regulatory attempts, in 2004, in 2006 and in 2007 respectively, as will be immediately demonstrated.

In the meantime however PNR data processing became central to security agencies outside the USA. This is why again at EU level, agreements were entered with Canada, in 2005, and Australia, in 2008.

As will be shown, PNR contracting between the EU and third parties has largely been a matter of political power. PNR Agreements have been entered only with EU's larger international partners – if PNR processing were indeed as central to combating terrorism as proclaimed to be, evidently any law-abiding country in the world would have been expected to profit from it. In addition, even among the existing three altogether, PNR processing agreements differences exist that may reflect the lack (or excess) of negotiating power: most notably, the USA is allowed to retain in its systems European PNR data for a period of 15 years, Canada for 6 years and Australia for 5.5 years.

At any event, this international PNR data processing scene would therefore leave intra-EU security agencies essentially as the only ones not profiting from their processing. In this context, at the same time as the last EU–USA PNR agreement was concluded, in June 2007, the Commission declared its intention to present a proposal for a framework decision establishing a EU PNR system; its first draft was presented six months later, in November 2007.

2.1. *PNR data processing between the EU and the USA*

As already discussed it was the USA that initiated the PNR data processing scene. After 9/11 the processing of Passenger Name Records (in practice holding information on more than 30 fields per individual) gained importance in its security policies.

The First PNR Agreement was entered in May 28, 2004 between the European Commission and the USA (Department of Homeland Security).[9] Nevertheless, a couple of months after it was concluded, on July 27, 2004, the European Parliament, which had not been involved in the negotiations, filed against it in front of the European Court of Justice. The Court

[4] See http://en.wikipedia.org/wiki/Passenger_Name_Record; there it is also clarified that "*although PNRs were originally introduced for air travel, they are now also being used for bookings of hotels, car rental, railways, etc.*". It is also noted that by now few airlines (both in the EU and in the USA) host their own passenger databases; in fact, most 'outsource' the processing of their PNR data altogether to third (data processing) parties that ultimately upload airlines' PNR data to the so-called Global Distribution Systems (SABRE, Galileo, Amadeus, Worldspan), see Hasbrouck E, 'What's in a Passenger Name Record', http://hasbrouck.org/articles/PNR.html.

[5] The contribution of PNR data processing *per se* to the international combat against terrorism is widely disputed. However, despite widespread skepticism regarding PNR data processing as an effective anti-terrorist tool no security or other agency anywhere in the world has ever presented any evidence (statistical or other) to its defense; in effect, security agencies customarily ask the public to simply take their word as to their effectiveness on account of "national security" (see Papakonstantinou V & De Hert P, 'The PNR Agreement and transatlantic anti-terrorism co-operation. No firm human rights framework on either side of the Atlantic', *Common Market Law Review*, vol. 46, No. 3, p. 916).

[6] Corresponding thus to the distinction between First and Third Pillar and the respective data protection instruments before the Lisbon Treaty came into effect.

[7] Art. 2 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive), *OJ* L 281, 23/11/1995 p.0031ff.

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

[9] Before that the Commission issued its Decision "on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection" (Commission Decision 2004/535/EC, *OJ* 2004, L 235/11-22) and the Council its own Decision "on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection" Council Decision 2004/496/EC, *OJ* 2004, L 183/83 respectively. See also Papakonstantinou V & De Hert P, 'The PNR Agreement', l.c., p.907.

reached its decision two years later, on May 30, 2006.[10] It found that the First PNR Agreement was based upon a wrong legal basis and thus effectively annulled it.[11] The Court subsequently set a deadline (September 30, 2006) for a new PNR Agreement to be entered into.

Negotiations for conclusion of the Second PNR Agreement began in July 2006, this time implementing the correct legal basis as per the Court's decision, namely Art. 24 of the, then, TEU. However, given the tight deadline and the tense feelings that the Court's decision raised within Europe, the conclusion of another PNR Agreement before September 2006 seemed unrealistic. Rather than that, an Interim PNR Agreement was entered on October 18, 2006 that would remain in effect until the end of July 31, 2007, when the Second PNR Agreement would, presumably, be concluded.[12]

Contrary to the general expectation that the Second PNR Agreement would be impossible to conclude until expiration of the Interim PNR Agreement at the end of July 2007, a text was indeed entered between the EU and the USA on June 29, 2007.[13] Although it observed closely the set timetable, it is not certain that the Second PNR Agreement equally observed traditional European data protection principles, as explained below.

The Second EU–USA PNR Agreement, still in effect today, essentially follows the rule-making methodology of its predecessors, whereby a broad text incorporated into the body of an international agreement is complemented by more "technical" annexes (in the first two Agreements, the "Undertakings"; now, the "DHS Letter"), whose "relationship" however to the main text has been left ambiguous.[14]

Data protection concerns were raised on various accounts.[15] The purpose of PNR data processing by American authorities, as set in Chapter I of the DHS Letter, is: "*strictly for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organised crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above*". As clearly stated, combating terrorism (as per the post 9/11 climate) is not the only reason European PNR data may be processed by American authorities; instead, a relaxed purpose description covering "*other serious crimes*" is preferred.

As far as the amount of data disclosed is concerned, PNR data under the Second PNR Agreement include nineteen (19) fields, rather than thirty-four (34), as was the case with its predecessors. Close observation, however, of the previous thirty-four fields and the current nineteen reveals otherwise: the reduction constitutes rather a rationalisation than an actual decrease in the quantity of data held.[16] The significance of *per se* collecting so much data from every individual can hardly be overlooked, particularly when the data processing is not going to be restricted to its apparent purpose, which is simply allowing the airline company to provide a better service. Indeed, the PNR data transfers system leads to the creation of a database with comprehensive information on all basic individual data, such as residence and workplace, payment preferences, age, etc. Moreover, by collecting and correlating information like 'special meal requirements' or 'seating particularities' or even by 'efficient' use (profiling) of the same individual's name, inferences may be made about such sensitive issues as the religion or health condition of the passengers.[17]

In addition to the above, the USA having "*ensured an adequate level of protection for PNR data transferred from the European Union*" fully expects that "*concomitantly, the EU will not interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds*".

Regarding the PNR data retention period, while under the First and the Interim PNR Agreements personal data of EU citizens would have been held in American databases for a period of 11.5 years altogether (3.5 years immediately accessible and another 8 years "dormant"), under the Second PNR Agreement this period has been increased to 15 years (8 + 7 years respectively).

Finally, a lot of attention has been given to whether a *push* or a *pull* system would be established for the technical transmission of data. Data protection proponents customarily press for a *push* system (whereby PNR data will be transmitted by airlines to the USA, as opposed to a *pull* system whereby USA authorities may access them directly from European airlines' systems); the Americans ultimately conceded to a *push* system (in Part. 2 of the Second PNR Agreement).

2.2. PNR data processing between the EU and Canada

The EU–USA PNR Agreements created a suitable background for other bilateral PNR data processing agreements to be entered between the EU and third parties. Canada profited from the initiative towards PNR data processing back in 2001 and, although arguably its initiative towards PNR (and API – Advance Passenger Information, see below) processing begun before 9/11,[18] secured a bilateral Agreement, as early as in 2005, with the EU, that remains in effect until today.

[10] Joined Cases C-317/04 and C-318/04, 30.05.2006.

[11] Par. 71–74, ECJ Decision. See also Gráinne G & Jorrit R, 'Case Law', *Common Market Law Review*, 2007, vol. 44, pp. 1081–1099.

[12] See Papakonstantinou V & De Hert P, 'The PNR Agreement', *l.c.*, p. 903.

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

[14] See Papakonstantinou V & De Hert P, 'The PNR Agreement', *l.c.*, p. 910.

[15] See also A Busch, "From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic", (2006) 3:4 *SCRIPTed* 304 <http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/busch.asp>.

[16] See Papakonstantinou V & De Hert P, 'The PNR Agreement', *l.c.*, p. 914.

[17] In this context, at least according to First Pillar distinctions, such data would constitute "sensitive data", requiring thus additional safeguards to "common" data processing (see Art. 8 of the Data Protection Directive).

[18] See Opinion 3/2004 of the Art. 29 Data Protection Working Party; however, the Canadian API/PNR Program appears to have been initiated on 25 October 2001.

Negotiations began in 2002 and the respective Agreement was entered on July 18, 2005.[19]

Canada arguably has implemented a more "data protection" friendly approach that the USA.[20] It had a Privacy Act since 1983 regulating processing of personal information collected and used by the government and in 2000 it introduced a Personal Information Protection and Electronic Documents Act applying to the private sector when processing personal information in the course of commercial activities. It also has an independent Privacy Commissioner. To this end, Canada received recognition of the "adequacy" of its level of protection afforded to the processing of personal information, as per the Data Protection Directive Art. 25.2 conditions, back in 2002.[21]

Although negotiations for PNR data processing between the EU and Canada began in 2002, it took more than three years and two formal Opinions on Canada's adequacy of processing[22] to finally reach agreement.[23]

As far as its scope is concerned, the Canadian PNR data processing agreement does not limit itself to the combat of terrorism; instead, the Canadian Border Services Agency "will use API and PNR information collected from European and other carriers only to identify persons at risk to import goods related to, or persons who are inadmissible to Canada because of their potential relationship to, terrorism or terrorism-related crimes, or other serious crimes, including organised crime, that are transnational in nature" (Art. 2 of the Commitments).

As far as the amount of data is concerned a first point to be noted is that the Agreement between the EU and Canada does not just include only PNR but API data too. All in all the Canadian authorities shall collect some 25 fields of data; some of them (as is the case of the "API data", no. 2 in the list) may lead to further fields. Nevertheless, the Agreement expressly clarifies that "for greater certainty, "sensitive data elements" within the meaning of Art. 8.1 of Directive 95/46/EC, and all "open text" or "general remarks" fields, will not be included within these 25 data elements". (Art. 4 of the commitments)

Finally, as far as the data retention period is concerned, "where the API and PNR information relates to a person who is not the subject of an investigation in Canada […] [data] will be retained […] for a maximum of 3.5 years […] in an increasingly de-personalized manner", meaning that name data will be available to viewing officials only under certain conditions (Art. 8 of the Commitments), whereas for "interesting" individuals data will be kept for up to 6 years.

EU institutional data protection proponents such as the EDPS and the Art. 29 Data Protection Working Party welcomed the fact that the Canadian PNR data processing Agreement has "major differences compared to the agreement with the USA; as a result the shortcomings of the latter agreement do […] not apply, at least not to the same extent" (Opinion 2005 of the EDPS). In addition, the issue of the lawfulness of its legal basis notwithstanding, the "democratic deficit" noted in the case of the US or Australia (see below) was perhaps not met in the case of the Canadian PNR data processing agreement. To this end, both the Art. 29 Data Protection Working Group (in its 1/2005 Opinion) and the EDPS (in his 2005 Opinion) note that the Commission expressly consulted with them during the negotiations process.

2.3. *PNR data processing between the EU and Australia*

The third (and final, to-date) international bilateral agreement for the processing of PNR data between the EU and a third country was entered with Australia. Its relevant PNR Agreement followed closely the Second EU–USA PNR Agreement of 2007.[24] Negotiations began a few months after the EU–USA Second PNR Agreement was entered into in November 2007, and the Agreement itself was entered into on June 30, 2008.[25]

[19] Council Decision of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data (2006/230/EC). It should be noted, however, that this Agreement as the EDPS noted (in his 2005 Opinion) was "*the second in a row, after the agreement of 17 May 2004 (1) between the European Community and the United States of America, of which the legality was contested by the Parliament under Art. 230 of the EC-Treaty*"; as we know by now the First EU–USA PNR Agreement was annulled – the Canadian PNR Agreement had exactly the same legal basis.

[20] See also, Hobbing P, 'Tracing Terrorists: the EU–Canada Agreements in PNR matters', *CEPS Special Report*, September 2008, http://www.ceps.eu/system/files/book/1704.pdf, p. 41, Nino M, 'The protection of personal data in the fight against terrorism. New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon', *Utrecht Law Review*, January 2010, vol. 6, issue 1, p. 79.

[21] 2002/2/EC, Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, *OJ* L2, 4.1.2002, p.13ff. See however the Art. 29 Data Protection Working Group one year in advance, highlighting certain limitations (Opinion 2/2001).

[22] Opinions 3/2004 and 1/2005 of the Art. 29 Data Protection Working Party.

[23] 2006/253/EC, Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, *OJ* L091, 29/03/2006p.49ff. A first evaluation of this adequacy Decision was performed in 2006 (Commission Staff Working Document: The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act).

[24] In any event it should be noted that Australia has adopted a more "friendly" approach to data protection than the USA; see for instance Opinion 1/2004 of the Art. 29 Data Protection Working Party "on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines".

[25] See Council Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the European Union, of an 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, *OJ* L 213, 8.8.2008, p. 47.

The EU–Australia PNR Agreement, although arguably less detrimental to European data protection,[26] shares some of the data protection concerns raised with regard to its USA and Canadian equivalents. For instance, here again the scope of processing is set too broadly, away from its anti-terrorism roots that justified PNR data processing, as an excessive but necessary measure, in the first place: "strictly for the purpose of preventing and combating' terrorism and related crimes […] and other serious crimes, including organised crime, that are transnational in nature" (Art. 5.1) or even "on a case by case basis where necessary for the protection of the vital interest of the data subject or other persons; in particular as regards the risk of death or serious injury to the data subject or others" (Art. 5.2), or when related to "a significant public health risk" (Art. 5.2).

As far as the amount of data disclosed is concerned, PNR data under the Australia–EU PNR Agreement are exactly the same as its US equivalent: 19 fields that however constitute in effect a rationalisation (and by no means a reduction) of the original 34 fields to be found in the first (EU–USA) PNR Agreements.

Regarding the PNR data retention period such data are agreed to be maintained in Australian systems for a total period of 5.5 years (see Annex, point 12), a period substantially less than that of the US 2007 equivalent.

The EU–Australia PNR Agreement was criticized both by the Parliament[27] (for data protection but also for other grounds, for instance on account of its "lack of democratic legitimacy") and by the European Data Protection Supervisor.[28] In particular, the Parliament expressly asked for more participation in the law-making process and expressly reminded the Council that "*in the event of the entry into force of the Treaty of Lisbon, Parliament should be associated on a fair basis with the review of all the PNR agreements*".[29] This was a reminder that held its importance when it came to releasing an EU PNR system later on (and closer to the formal adoption of the Lisbon Treaty).

3. The EU PNR framework decision initiative

At the same time that the Second EU–US PNR agreement was concluded, in June 2007, the former Vice-President and Commissioner for Justice Liberty and Security declared his intention to present a proposal for a Framework Decision establishing a EU PNR system within a few months (until October 2007).[30] Indeed, the first Commission proposal for a draft Framework Decision "*on the use of Passenger Name Record for law enforcement purposes*" was introduced on November 6, 2007.[31]

3.1. *Background*

Until that time, as discussed, PNR data processing attracted rather limited attention within the EU. On the contrary, much more institutional work has already been undertaken with regard to their API relevant: in the wake of terrorist attacks in March 2004 the Commission introduced in April Directive 2004/82/EC "*on the obligation of carriers to communicate passenger data*".[32] This Directive, given its timing, did not attract as much criticism from a data protection point of view as its name would suggest. To begin with, it only concerns API information. API information is the information contained in the machine readable parts of EU passports; consequently it is not expanded as much as typical PNR data.[33] And, although the Directive applies to both EU citizens and visitors, it only covers air travel and, at any event, data are to be deleted if found of no interest within 24 h.

By 2007, however, API data processing was not considered sufficient for intra-EU security purposes, especially while more extensive PNR Agreements were being concluded with third countries. EU security officials appeared thus deprived of a useful tool that their colleagues in the USA, Canada and Australia were being offered.[34]

At any event, the proposal for a Framework Decision on PNR data processing by no means constituted a surprise; its timing may have actually coincided with attempted terrorist attacks in London and elsewhere in Europe, but discussions on this issue were at least as old as the First EU–US PNR Agreement or even older than that. In a Communication to the

[26] For instance, when warranting that the Australian Privacy Act will apply unabridged to EU citizens or when setting that in the event of a dispute arising between the parties to the Australian PNR Agreement the EU data protection authorities may exercise their powers to suspend data flows to protect individuals with regard to the processing of their personal data where there is a substantial likelihood that the provisions of the Agreement are being infringed. See also Nino M, 'The protection of personal data', *l.c.*, p. 81.

[27] See European Parliament recommendation of 22 October 2008 to the Council concerning 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 (2008/2187 (INI)).

[28] See Comments of the EDPS on different international agreements, notably the EU–US and EU–AUS PNR agreements, the EU–US TFTP agreement, and the need of a comprehensive approach to international data exchange agreements, 25.01.2010.

[29] See European Parliament recommendation of 22 October 2008, (3).

[30] Mr. Frattini declaration is quoted by Statewatch on 15 July 2007 (www.statewatch.org/news/2007/jul/03eu-pnr.htm).

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

[32] *OJ* L 261/24, 06.08.2004.

[33] In fact, only type of travel document, nationality, full name and date of birth, as well as, particular travel details (border crossing point, plane code etc) (Art. 3).

[34] In a way, the USA processing initiatives created a "spillover" effect (Pawlak P, 'Made in USA? The influence of the US on the EU's data protection regime', *publication of the Centre of European Policy Studies*, 2009, p.9, see also De Busser E, 'EU data protection in transatlantic co-operation in criminal matters Will the EU be serving its citizens an American meal?', *Utrecht Law Review*, January 2010, vol. 6 Issue 1, p. 96).

Council and the Parliament the Commission asked for a "global EU approach" as early as in 2003.[35]

The global EU data protection timing is also of concern. In late 2007 negotiations for the Data Protection Framework Decision were well under way[36]; the data retention Directive[37] was introduced only two years earlier (but not all Member States had implemented it at national level). The PNR Agreement with Australia was being concluded. Indeed it could be maintained that those were (or, arguably, still are) times when security concerns took precedence over data protection rights.[38]

Since the first Commission draft, the proposal has already raised several issues, ranging from the choice of the legal instrument[39] to the time-schedule of the proposal, from the scope to the data protection regime. Discussions mostly took place within the Multidisciplinary Group on organised crime (MDG).[40] As already noted, negotiations were halted, as per the Parliament's request,[41] in October 2009[42] and a new draft proposal is now to be expected. Nevertheless, given the relevance of such a proposal, and the European and international impact of such a system in case of approval, it seems important to sketch an outline of its main provisions and then discuss some of the main issues raised.

3.2. *Content of the EU PNR proposal*

The EU PNR Proposal broadly follows the structure of the Data Protection Framework Decision: a statement of purpose and a set of definitions are followed by provisions on data transfers, the rights afforded to individuals and the Comitology terms.

With regard to its objectives, the EU PNR Proposal "provides for the transfer or the making available by air carriers of PNR data of passengers of international flights to the Member States, for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious crime, as well as the processing of those data, including their collection, use and retention by the Member States and their exchange between them" (Art. 1). Its purpose therefore expands to cover terrorism and serious crime as well. On the other side, the scope of the Proposal is limited to cover international flights, therefore excluding intra-EU flights and other modes of transport; its purpose also seems to exclude the use of PNR data for immigration management.

Art. 3 of the EU PNR Proposal establishes the Passenger Information Unit (PIU), at the moment in a "*law enforcement*" and not simply administrative format. The PIU will be charged with two key tasks: collecting the PNR data from air carriers and processing such data in order to carry out a real-time risk assessment of the individuals concerned, identifying who requires further examination by the competent authorities of the respective Member State. The purposes of the risk assessment is to identify persons who are, or may be, involved or associated to terrorist and serious crime offences, to create and update risk indicators for the assessment and to provide intelligence on travel patterns and other trends. Evidently such risk assessment is of major importance for individuals because in effect whoever is "flagged" will subsequently be thoroughly scrutinized and potentially may have to resolve the issue in person with security authorities. This is why the criteria of this assessment matter. To this end the EU PNR Proposal merely asks for them to be "*in compliance with national law*", simply "*taking due account of the recommendations for common general criteria, methods and practices*"[43]; in practice this means that each Member State may set the criteria it pleases, hardly a harmonising effect for a Framework Decision.

Air carriers will be obliged to make available PNR data at two different moments: 48 h before the departure and immediately after flight closure (Art. 5). Nevertheless, in specific and exceptional cases, a PIU can request access to data even prior to the 48 h standard. Data shall be transmitted according to a "push" method, that is to say by sending data to PIUs, but when this is not the case and they do not have a "push" technical architecture, data should be made

[35] Communication from the Commission to the Council and the Parliament, Transfer of PNR data: A global EU approach, 16.12. 2003, COM(2003) 826final.

[36] See *De Hert P & Papakonstantinou V*, 'The data protection framework decision of 27 November 2008 regarding police and judicial co-operation in criminal matters – A modest achievement however not the improvement some have hoped for', *Computer Law & Security Review*, 2009, vol. 25, pp. 403–414.

[37] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[38] See for instance, The Economist, "Terrorism and Civil Liberty", in its special "Civil liberties: Surveillance and Privacy" series, 27 September 2007.

[39] For instance, "*the LIBE committee has again highlighted the problems concerning individual rights and committee members have also agreed that such a framework directive might be uncalled for, since there might be no need for a European-wide passenger name records system (A. Alvaro, interview, January 2009)*" (in Ripoll Servent, A. (2009). 'Setting Priorities: Functional and Substantive Dimensions of Irregular Immigration and Data Protection Under Co-decision', *Journal of Contemporary European Research*. 5 (2), pp. 225–242. Available at: http://www.jcer.net/ojs/index.php/jcer/article/view/172/143).

[40] On the role, in principle, of the MDG in data protection issues see De Hert P & Papakonstantinou V, 'The Data Protection Framework Decision', *l.c.*, p. 407.

[41] The role of the Parliament in future releases of the EU PNR Proposal cannot yet be predicted: As Ripoll Servent (*ibid*) notes, in the past the Parliament, particularly through its LIBE Committee, has demonstrated a consistency and long-term engagement towards data protection, that nevertheless has at times led it at confrontations with the Council. The Parliament however may ultimately wish to "strengthen its functional dimension" and portray itself as a "a reasonable and *mature* institution capable of reaching inter-institutional compromises" – leaving thus its role in intra-EU PNR processing drafting unpredictable.

[42] The draft proposal that shall be elaborated in this paper is Council of the European Union, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, doc. 5618/2/09 REV 2, Brussels 29.06.2009 ("EU PNR Proposal").

[43] In Art. 3.4. It is expressly set however that they shall "in no circumstances be based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual orientation" – in other words on "sensitive" data (see also Art. 6 of the Data Protection Framework Decision).

accessible to PIUs by the "pull" method, thus providing PIUs the capability to directly extract the data from the databases.

PNR data covered by the EU PNR Proposal are 19, covering biographical, contact and travel data (Annex II). They are the same categories of data covered by the EU–US agreement, as well as the EU–Australia agreement (therefore all noted above as to their exact breadth apply here as well).

Chapter III, Arts. 11(a bis i) and 12, establishes the *ad hoc* frame of data protection for EU PNR data processing conducted by a PIU.[44] The minimum standards are expressly set by the Data Protection Framework Decision[45] and the Convention 108. Subsequently, attention is given specifically to some of the basic data protection principles (for instance, of proportionality and adequacy in Art. 11 and to data security and confidentiality of processing in Art. 11h and 12, but not to the purpose limitation principle); to sensitive data (Art. 11a); to establishment of an *ad hoc* notification system (Art. 11b); to the basic data protection rights of individuals (right to information, access and rectification in Art. 11c, d and e respectively); as well as to the establishment of an independent national supervisory authority.

Nevertheless, the wording of this *ad hoc* data protection framework is almost always obscure and introducing numerous exceptions and reductions to the level of protection. Although the basic data protection principles and rights to individuals, as known in national EU Data Protection Acts and incorporated in the Data Protection Directive, are there for everyone to see, close examination of their exact wording and circumstances leaves ample space for processing-prone derogations (see for instance the restrictions introduced to individuals' access rights in Art. 11d).

The data retention period of PNR data amounts to a total of ten years[46] but it is split into two phases (Art. 9). Data will be initially kept in a database for a period of three years, starting from their transfer to the initial PIU. This first phase will be followed by a second period of seven years, where PNR will be stored in an "inactive" database, where access is submitted to stricter rules and for exceptional circumstances (for instance, specific and actual threat or risk). After this period, PNR data shall be deleted.

Finally, Art. 8 of the EU PNR Proposal sets the rules that apply to transfers of PNR data to third countries. Five conditions must be satisfied. The use purpose of data transferred should be restricted in the "*prevention, detection, investigation or prosecution of terrorism offences or serious crime*", and the receiving authorities should be law enforcement authorities. The third condition applies to data already obtained by another Member State: in those cases of onward transfer, the prior consent of the originating Member State should be obtained (unless an "*immediate and serious threat*" occurs). The two final conditions are the responsibility of the third country: it must ensure an adequate level of protection (not general data protection, only "*for the intended data processing*") and shall not further transfer the data to another third country without the express consent of the Member State.[47]

4. Critical assessment

The EU PNR Proposal could not possibly stand any data protection assessment, because it obviously is not drafted with data protection in mind.[48] Only marginally is data protection mentioned in the (at least questionable, even from a law-making perspective, see immediately below) *ad hoc* data protection framework. The protection of the rights of individuals is evidently not a priority for the EU PNR Proposal: no mention whatsoever about the protection of rights of individuals is made in its Art. 1.[49] Leaving aside any thought about human rights, the EU PNR Proposal could be perhaps judged with relevance to its effectiveness or even its *raison d' être*.

With regard to its effectiveness, even if it was accepted that PNR data processing does help in the fight against (any) crime. The EU PNR Proposal ought, supposedly, to establish mechanisms that at least have a chance of being effective; in other words, mechanisms that fit into existing administrative infrastructures, that warrant openness and accountability and that at least promise not to prove bureaucratic by adding layers of administration. This, as it will be demonstrated, is however not the case with the draft text under consideration.

Finally, with regard to its *raison d' être*, the release itself of a Framework Decision invokes thoughts of harmonisation of legislation between Member States and creating common standards: the EU PNR Proposal, as it will be shown, offers very little to this end.

4.1. *The* ad hoc *data protection framework as an alibi to data protection consideration*

Despite the fact that PNR data processing is inevitably personal data processing and thus falls well within the data protection regulatory framework, Art. 1 of the EU PNR Proposal makes no such acknowledgement. Instead, data protection is treated in a section of the EU PNR Proposal, as if it was a special issue, similar to other matters to be taken into consideration.

The decision to develop *ad hoc* data protection provisions within the EU PNR Framework Decision seems to confirm the

[44] It thus applies only to data accessed, processed and exchanged by PIUs and expressly and intentionally not to the subsequent processing of such data by the, receiving, "competent authorities".

[45] The Data Protection Framework Decision data protection standards are lower than those set by the Data Protection Directive (see De Hert P & Papakonstantinou V, 'The Data Protection Framework Decision', *l.c.*, p. 414).

[46] A reduction of the initial thirteen but still the number of years remains to be finalised because no consensus is found between Member States (some wishing to be left alone to decide on their own).

[47] Evidently, Art. 8 and any implementation of an EU PNR system whatsoever is expected to be without prejudice to any existing bilateral and international agreements, such as, the USA, Canadian and Australian PNR Agreements (see Art. 19).

[48] See also Marie McGinley, 'Die Verarbeitung von Fluggastdaten für Strafverfolgungszwecke', *Datenschutz und Datensicherheit*, 2010, 250–253.

[49] See also the Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (2008 draft).

idea, and the political will, to build a sector-based system of data protection. If the proposal is adopted, it will contribute another piece to the present, complex, puzzle.[50] Moreover, such an *ad hoc* framework shows all the difficulties of this approach, because it does not cover the data *per se*. Provisions on data protection cover only the exchange and the processing of data operated by a specific type of actor: the Passenger Information Unit. Therefore, in the simplest case, the same PNR will be covered by at least two different set of rules, the Framework Decision and national law, not to mention data protection rules that apply to air carriers and booking services. Furthermore, in case of exchange of PNR data, the national rules of other Member States will apply. Such a complex picture contributes only to underline the possible shortcoming of not extending the scope of the Data Protection Framework Decision to national processing.

Apart from its structural difficulties, the wording itself in the ad hoc data protection framework undermines it. In effect, there exists not a single data protection principle (for instance lawfulness of processing, adequacy of data, proportionality, data security) of those mentioned in the EU PNR Proposal (e.g. the purpose limitation principle is omitted) that does not contain a number of exceptions, restrictions and reservations that, if applied, will nullify it from within (see for instance the provisions on the rights of access and rectification for individuals).

Equally problematic are the provisions regulating PNR data flows to third countries. In the case of an exchange, PNR data will be submitted to the receiving country's standards. In fact, the authorities of a third country are only permitted to use the PNR data for the agreed purpose, and prior consent is sought only for onward transfer. A crucial provision is the request for an "adequate level" of protection. However, such an adequacy criterion is limited to the degree of protection of a specific type of processing, and does not cover the entire data protection system of the third country. It is not clear who will be charged with the responsibility to assess such adequate level, and how to investigate and avoid further processing.

The strategic choice of inserting in the EU PNR Proposal an *ad hoc* data protection chapter is at least questionable both as to its intentions and as to its effectiveness.[51] Such an ad hoc framework only burdens an already heavy patchwork of data protection provisions (especially after the Lisbon Treaty came into effect) and its multitude of restrictions and exceptions diminish the protection of individuals.

4.2. *The effectiveness of the suggested EU PNR data processing model*

The administrative model that the EU PNR Proposal aims to introduce is at least confusing. It calls for the creation of a multitude of new state agencies that, notwithstanding the financial issue, do not fit into existing schemes. Additionally, if examined as newly established agencies, their openness and accountability is not warranted particularly with regard to the sensitive data they shall process and store.

PIUs are the organic instrument of data processing in the PNR scene, but very few instructions and even fewer conditions as to their establishment and operation are given in the EU PNR Proposal. As far as it is concerned, they may be "*a law enforcement authority or a branch of such an authority*", "*its staff members may be detached from competent public authorities*" and "*each Member State shall notify its PIU to the Commission*". This is, admittedly, very little information, especially when taken into consideration that PIUs are intended to be new state agencies (or at least departments) with new powers whose actions may prove particularly detrimental to individuals. Apart from that, ambiguity as to whether PIUs shall be part of the law enforcement mechanism or an activity outsourced to other public agencies (that will then have to co-operate with law enforcement agencies) does not add to their image of efficiency and reduction of bureaucracy.[52]

PIUs are left institutionally uncontrolled and unmonitored in their data processing activities, at least as per the EU PNR Proposal. The "National Supervisory Authority" (Art. 11) is seriously restricted in its oversight and monitoring powers, being expressly reduced to "monitoring the application of the provisions on data protection pursuant to this Chapter" (the ad hoc data protection framework). Oversight will therefore be piecemeal and circumstantial at best.

4.3. *Does the EU PNR proposal have a reason to be?*

Under these circumstances the EU PNR Proposal's *raison d'être* is questionable. It does not achieve harmonization among Member States' legislation, leaving substantial space for national derogations and being applicable only to data transfers and not at national level, neither does it warrant a level of protection for individuals. Instead, its sole purpose appears to be (as confessed in Art. 1) to facilitate and institutionalize (for those Member States that do not yet have relevant legislation at national level) PNR data processing and exchanges.

This prioritization was not evident when the initiative for drafting of an EU PNR scheme began: back in 2003 the Commission expressly promised that "*such a policy will have to strike a balance between the different interests involved, in particular between legitimate security concerns and the protection of fundamental rights, including privacy*". No evidence that the EU PNR Proposal adheres to this statement is present in its current text.

[50] See Papakonstantinou V & De Hert P, 'The PNR Agreement', *l.c.*, p. 888ff. and De Hert P, Papakonstantinou V & Riehle C, 'Data protection in the third pillar: cautious pessimism', in *Crime, Rights and the EU* (ed. Martin M), Justice, 2008, pp. 127ff.

[51] See also Boehm F, 'Tit for tat – Europe's revenge for the Canadian and US-American PNR systems? The envisaged European model of analyzing flight passenger data', 2010 paper presented at the *Third International Annual Conference on Computers, Privacy and Data Protection*, Brussels, 28th January 2010 organised by CPDP (www.cpdpconferences.org).

[52] See also Nino M, 'The protection of personal data', *l.c.*, p. 83.

This change of focus is most unwelcome, because it deprives the EU PNR Proposal of its protective content for individuals, leaving it as an instrument of law enforcement co-operation which, if necessary, should be assessed against the general data protection provisions that supersede it.

5. Conclusion

The EU PNR Proposal in its current wording does not acknowledge its legal basis (data protection), departs from its original mandate ("*to strike a balance between security concerns and the protection of fundamental rights*") and creates a hostile (and perhaps ineffective) processing environment for individuals. The ratification of the Treaty of Lisbon is therefore a welcome development because it has led to suspension of negotiations on the current draft and participation of the Parliament in the process. Hopefully the outcome will be a balanced and well structured instrument that will accommodate both data protection concerns and data processing needs in line with the on-going fight against terrorism.

Paul De Hert (*paul.de.hert@uvt.nl*) *is professor at the Vrije Universiteit Brussels (LSTS) and associated professor at Tilburg University (TILT).*
Vagelis Papakonstantinou (*vpapakonstantinou@pkpartners.gr*) *is scientific collaborator at the Vrije Universiteit Brussels (LSTS) and Partner in PK partners Law Firm in Athens, Greece.*