

# No Dream Ticket to Security

PNR Data & Terrorism

Frank Kuipers

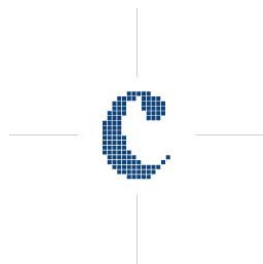
July 2007

Netherlands Institute of International Relations  
Clingendael

CIP-Data Koninklijke bibliotheek, Den Haag

Kuipers, Frank

No Dream Ticket to Security - PNR Data & Terrorism / Frank Kuipers –  
The Hague, Netherlands Institute of International Relations Clingendael.  
ISBN-978-90-5031-754-2



Desk top publishing by: Karin van Egmond

Nederlands Instituut voor Internationale Betrekkingen Clingendael  
Clingendael 7  
2597 VH Den Haag  
Phone: +31 (0)70 – 3245384  
Fax: +31 (0)70 – 3746667  
P.O.Box 93080  
2509 AB Den Haag  
E-mail: [CSCP@Clingendael.nl](mailto:CSCP@Clingendael.nl)  
Website: <http://www.clingendael.nl>

© Netherlands Institute of International Relations Clingendael. All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the copyright holders. Clingendael Institute, P.O. Box 93080, 2509 AB The Hague, The Netherlands

## LIST OF ABBREVIATIONS

---

ACS	-	Australian Customs Service
API data	-	Advanced Passenger Information - data
ATS	-	United States Automated Targeting System
ATSA	-	United States Aviation and Transportation Security Act
CBP	-	United States Customs and Border Protection, subdivision of DHS
CBSA	-	Canadian Border Service Agency
DHS	-	United States Department of Homeland Security
EU	-	European Union
KLM	-	Royal Dutch Airlines
NCTb	-	Dutch National Coordinator for Counterterrorism
PIU	-	Passenger Information Unit
PNR data	-	Personal Name Records data
POE	-	Port of Entry
TSA	-	United States Transport Security Agency, subdivision of DHS
TSC	-	United States Terrorist Screening Center
TSDB	-	United States Terrorist Screening Database
US-VISIT	-	United States Visitor and Immigrant Status Indicator Technology program



# I. EXECUTIVE SUMMARY

---

## **Why this study?**

The diverse threat of terrorism requires a multi-faceted approach to mitigate its many risks. Acting on this threat, the European Commission presented on November 6, 2007 its proposal to oblige airlines operating flights to and from Europe to transfer the Personal Name Records (PNRs) of their passengers. This should be done to enable a risk analysis of the passenger on board. Supposedly, PNR data records are one of the cornerstones of an effective effort to keep terrorists off airplanes and outside Europe.

This paper questions that assumption. Its guiding principle in this is one simple objective: to determine the need and necessity to transfer and collect PNR data. Subsequently, it also probes the need and necessity to introduce this regulation Europe-wide.

## **What this paper found:**

It must be concluded that it remains unclear whether the transfer and collection of PNR data actually contributes to the attainment of its stated purposes. This confusion is due in part to a lack of information on how to frame the results achieved thus far. Another problem is the lack of openness from the side of policymakers. Those responsible for devising counterterrorism policies appear time and again unwilling to share with the public what demonstrable information convinced them of the fact that PNR

data contributes to counterterrorism efforts. This can mean two things. Either there are no demonstrable results, or they are kept secret. In both circumstances a ‘known – unknown’ exists about the merits of PNR data, which causes genuine indistinctness as to whether the implementation of a European rule is necessary or needless. Apart from this disturbing lack of information, questions can be raised as to whether PNR can be used for their stated purposes, since successful outcomes may require profiling to identify security risks. Yet, such profiling efforts are strictly forbidden under European law. Finally, there exists the risk that the potential of this new rule is overrated, as generic PNRs hold only information on a very small number of data elements.

These findings have not led, however, to the conclusion that PNR data has no place among Europe’s counterterrorism arsenal. More information is needed. Many questions within the ‘PNR data constellation’ still beg to be answered, particularly on critical procedural issues. Therefore, this paper calls upon policymakers in the possession of results, generated through the use of PNRs, to come forward and to show their cards in order to make a genuine debate possible. European countries or the Commission should elaborate why they consider the introduction of such a scheme necessary by making public the ‘demonstrable’ results on which they draw in their assessment, but which are not shared with the wider public. Positive results may convince skeptics of the need and necessity; a lack of results can point those very policymakers to the fact that PNRs may not be the be-all and end-all of counterterrorism.

# TABLE OF CONTENTS

---

List of Abbreviations .....	i
I. Executive Summary.....	iii
Why this study?.....	iii
What this paper found:.....	iii
Table of Contents .....	v
1. Introduction .....	1
1.1 The Debate .....	1
1.2 The Questions .....	3
1.3 Outline.....	5
2. Data Debated .....	7
2.1 Introduction .....	7
2.2 What are PNR Data?.....	8
2.3 How Do PNR Data Separate themselves from Other Datasets? ...	10
2.4 What Factors Propelled Data Collection to Prominence? .....	14
2.5 Legal Obligations for the Exchange of Personal Data .....	15
2.6 Conclusion .....	18
3. Exchanging PNR Data .....	19
3.1 Introduction .....	19
3.2 Agreements and a Proposal.....	20
3.3 Conclusion .....	31

4. Do PNRs actually ‘work’? – Arguments For and Against the Transfer of PNRs .....	33
4.2 Why PNRs Work.....	34
4.3 And Critique on this Viewpoint .....	39
4.4 Why PNRs Do Not Work... ..	42
4.5 ...And Critique on this Viewpoint .....	48
4.6 Conclusion .....	50
5. Conclusions, Findings and Recommendations .....	53
5.2 Need and Necessity.....	55
5.3 Suggestions for Improving our Understanding on PNRs .....	56
5.4 Implications for The Netherlands .....	57
Annex 1 .....	59
Annex 2 .....	65
About the author.....	69

I am particularly grateful to Klaas Bruin, Privacy Officer at KLM, Sophie in ‘t Veld, Member of the European Parliament, and staff members of the NCTB and the Dutch Ministry of Justice for the collaboration in the early and final stages of this project and for providing important insights. For valuable comments, I thank Bibi van Ginkel, Sico van der Meer, Michael Andrew Berger, Michiel de Weger, Steven Westervelt, and Polyna Berlin.

*“I have to make a choice between law enforcement and people investigating on international crime and explaining to the public opinion why PNR is useful.”<sup>1</sup>*

*“There is little evidence that the gathering of mountain upon maintain of data on the activities of every person in the EU makes a significant contribution (to tackle terrorism).”<sup>2</sup>*

# 1. Introduction

---

## 1.1 The Debate

On the morning of September 11, 2001, terrorists employed aircrafts to fulfill their lethal ambitions. Although the events of that day are stored in our collective memory, the threat of another terrorist attack through the means of air travel remains alive. The foiled 2006 plot to blow up transatlantic airliners destined for America revealed that terrorists continue to consider, and plan for an attack through the use of airplanes.<sup>3</sup> Also, airplanes constitute the favorite mode of transportation for terrorists to get from training camp to target site. More often than not, those with terrorist intentions arrive by aircraft. As such, aircrafts may serve terrorists in two ways: as a means to attack and as a means to go from the home country to the country where the

---

1 Opinion of Mr. Franco Frattini as voiced on 25 January 2008. ‘Statement on SIS2 and EU PNR by Minister of the Interior Dragutin Mate and Commissioner Franco Frattini’. See: <[http://www.ue2008.si/fr/Media\\_Service/Audio\\_Archive/index.html](http://www.ue2008.si/fr/Media_Service/Audio_Archive/index.html)>, last accessed 23/07/2008.

2 Opinion of Mr. Tony Bunyan from the UK liberties group Statewatch, speaking on the Commission’s proposal, quoted in: Euobserver.com (5 October 2007). ‘Lucia Kubosova - Brussels could extend anti-terror rules to EU flights’.

3 The Guardian (10 August 2006). ‘Mark Oliver, David Batty and agencies – Mass murder terror plot uncovered’. See: <<http://www.guardian.co.uk>>, last accessed 03/04/2008.

attacks are to be conducted. Put differently, jets are oftentimes the crucial linchpin between intentions on the one hand and chaos on the other.

Naturally, countries seek to counter this threat. They devise counterterrorism measures that aim to keep terrorists off planes. Hardening airports, increasing the number of surveillance personnel, or introducing more strict rules on hand luggage items are all examples of such a response. In line with the closer watch on personal belongings is the closer watch on the passenger. Border agencies increasingly try to monitor the traveler by conducting passenger screens. The screening can be done in many ways. One way is through thorough passport controls. Another option is comparing names on tickets against terrorist watchlists. Finally, data contained in the machine readable strip of an individual's passport can be disseminated and analyzed. All these efforts share the same characteristic: they draw on reasonably reliable facts to apprehend felons.

Recently, however, a new screening method that relies on less unequivocal data has gained prominence. The information contained in a passenger's Personal Name Record (PNR) could help to mark the individual as a potential security threat. Much is unknown as to how PNRs can contribute to the identification of risks, and how important they are within this effort. Also, the substance of the precise procedure is unclear. More to the point, questions remain whether PNRs are run against existing criminal data or used outside such points of reference. In the latter case, PNRs would be run against predictive 'risk indicators', which were in themselves extrapolated from the PNRs, characteristics and information of previous terrorists.

The European Commission's submission of its proposal to adopt a Framework Decision for the exchange of Passenger Name Records in November 2007 can be considered a clear sign of the growing value that is attributed to this measure.<sup>4</sup> In fact, the proposal is a culmination of experiences and political pressure on this issue. In the years prior to this proposal, a number of countries made experiences with PNRs to expose and to stop felons. Their results lead European policymakers to view PNRs as the be-all and end-all to stop terrorists from boarding airplanes. Given their supposed value, European officials have begun to advocate the disclosure of all PNRs to the intelligence community of all passengers on flights to and from Europe.

Yet, coincidentally, a growing number of members of the European Parliament, privacy organizations, airlines, and data protection authorities worry about the

---

4 EU Commission (06 November 2007). 'Proposal for a Council Framework Decision on the Use of Passenger Name Record for Law Enforcement Purposes'. COM (2007) 654/F.

fact that personal files are transmitted without approval of the individual affected; are afraid that private information may fall into the wrong hands; or believe that the exchange of PNR data contributes little to securing borders and airplanes against terrorists. This contradiction in viewpoints is not unique. Since 9/11, many measures that are intended to counter terrorism and that involve the making available of private information have triggered a debate about need and necessity. Recurring dilemma is how to reconcile the state's duty to protect its citizens and the right that that very citizen has to privacy. What may tip the balance is that the measure can be reasonably expected to produce results. Put differently, need and a necessity to give up fundamental rights to attain safety should be clear.

In essence, the PNR-issue taps too into this debate as opponents question the very assumption that underlies the agreements on the exchange of PNR data – the usefulness of PNR data as a tool to combat terrorism. This paper will demonstrate that views on the use of PNRs for such purposes differ significantly, with both sides claiming the high ground. Elucidating and clarifying this disagreement, together with an honest discussion on the possible implications that such a transfer may carry for passengers, are the drivers for this study.

## **1.2 The Questions**

Two key structural problems cloud the PNR debate. The first obstacle is a lack of understanding as to the subject's dimensions, which complicates efforts to untangle what constitutes part of the debate and what does not. Clearly, the outer limits of the subject need to be formulated before a more thorough assessment can be made. The second problem is the absence of evaluations or reliable reports that contain hard information on the actual merits and costs of such an exchange. Little is known up to now as to how PNRs may help to apprehend terrorists and how successful this approach is.

The research questions that relate to the first deficiency are:

- What are Personal Name Records and how do they differ from other passenger data? (Chapter 2)
- What are the origins of the notion that passenger data are a complimentary tool in the efforts to fight terrorism? (Chapter 2)
- What are the terms of the different understandings that arrange for the transfer of PNR data between Europe and third countries? (Chapter 3)

The research questions posed in correlation with the second problem are:

- What results and problems can be noted after an analysis of the identifiable merits and detriments that are attached to PNRs and the purpose for which they are put to use? (Chapter 4)
- How do the results weigh up to the problems and what should be concluded about benefits and detriments up to this point? (Chapter 5)

In order to tackle the latter deficiency, this paper draws on statements contained in reports to assess the pro's and con's that involve the transfer of PNR data. As to the former problem, this paper will highlight which beliefs, events, and agreements underlie the exchange of data sets, together with a transparent description as to what PNR are – and, more importantly, what they are not. By doing so, this paper hopes to achieve two objectives: [1] to contribute to a clear understanding of the entire 'PNR constellation' and [2] to make a preliminary assessment as to the need and necessity to transfer PNR data. From the understanding generated by this effort, hopefully, the value of PNRs as a counterterrorism tool can be assessed. Also, a balanced choice may be made in support of or against the exchange of PNR data.

Throughout this study, it is important to bear in mind that the number and the scope of experiences with the transfer and processing of PNR data are few. Moreover, official reviews fall short to provide such information. The reason for this is that PNR data collection is a relatively new approach within the greater spectrum of data collection for the purpose of counterterrorism and there exists no publicized review that assessed results. As a result, little scientific research has been conducted into the merits of this specific counterterrorism approach. This study must rely in its assessment on anecdotic examples and common sense, giving it in turn an explorative character. While 'hard' empirical facts would be the preferred set of data to rely on, this paper is careful to acknowledge its limitations and functions primarily as an indicator of the possible ways that this topic can be approached.

That said, although the absence of such information and coinciding inquiries hinders a thorough research tremendously, it should not mean that this topic should not be further explored altogether. Quite the contrary, this study hopes to enhance our knowledge on the subject matter and to fill the void that arises from the dominant question 'what is the use of PNRs for counterterrorism efforts?' Moreover, in view of the possibility that the transfer of such data can have to gravely impinge on the proceedings and procedures of airlines, security personnel, customs officials, data analysts, and policy makers, such an inquiry into merits and detriments is not only justified, but indeed necessary. This is all the more true, especially when the making available of PNR information can set off a plentitude of side effects, such as

the branding of travelers or unfounded arrests.<sup>5</sup> In sum, this topic deserves to be explored more in-depth to establish an understanding of the need, necessity, proportionality, and usefulness of such a design.

### **1.3 Outline**

The question ‘what are PNR data’ guides chapter two. Also, chapter two will discuss other data sets; the underlying rationale for authorities to seek the transfer of PNR data; and the trajectory towards the respective legislation under which the transfer of PNR data is required. Following, chapter three probes the content of the two agreements with the US and Canada that Europe signed under this legislation. In addition, this chapter discusses the dimensions of Europe’s own proposal. To assess whether PNRs have a place among the counterterrorism arsenal, chapter four discusses the arguments that have led both sides to either oppose or support the transfer of PNR data. It also elaborates on judicial and practical pitfalls in relation to PNR data. Finally, chapter five will provide a conclusion of the findings and points of reference on how to move forward.

---

5 One example is the arrest of Maher Arar, a 34 year old Canadian citizen, who was apprehended in the US while in transit from Zürich to Montreal and subsequently moved to Syria, where he was questioned and held for the duration of one year. For more information on his case, see: <<http://www.maherarar.ca>>, last accessed 30/06/2008.



## 2. DATA DEBATED

---

### 2.1 Introduction

The events on September 11, 2001 (henceforth 9/11) were the most dramatic outing of a threat that had simmered for years. In their conduct and impact, the attacks unveiled a serious and enduring threat to Western society.<sup>6</sup> In order to counter this threat, respond to its dimensions, and to mitigate possible risks, a number of initiatives were employed after 9/11. This was done on the basis of new legislation and agreements. Many involve or include in their provisions the acquisition of traveler's data to screen for human threats in order to separate terrorists from tourists and tradesmen.

---

6 While the systemic nature of the threat of terrorism can certainly be contested, such is not the focus of this paper. It notes that even those critical of the introduction of certain counterterrorism measures do not question the threat altogether. As a result, this paper will work from the premise that terrorism indeed poses a threat to Europe and the US, and that a number of policy makers have become convinced of this threat and the urge to act. This attitude explains the development of numerous initiatives, including the proposal for a European PNR scheme.

See, for instance, the website of Ms. Sophie in 't Veld, member of the European Parliament and a critical observant of the proposed PNR scheme, who claims on her website that the threat of terrorism is real, but that some measures to fight this threat are disproportionate. <[http://www.sophieintveld.nl/news/item/PASSAGIERSGEGEVENS\\_HOE\\_ZIT\\_HET\\_E\\_CHT\\_/56?mid=100013](http://www.sophieintveld.nl/news/item/PASSAGIERSGEGEVENS_HOE_ZIT_HET_E_CHT_/56?mid=100013)>, last accessed 23/07/08.

This chapter's purpose is twofold: it seeks to disseminate and to distinguish among the different sets of data currently available in order to build an understanding of the concept of 'PNR data'. More to the point, it is crucial to understand what PNR data are, but also what they are not. This is particularly important when comparing PNRs to other passenger related personal data, collected in the full travel process. Also, this chapter aims to retrace the origins that underlie the perception that the acquisition of personal data is a crucial tool in keeping terrorists out of planes and off territories.

## 2.2 What are PNR Data?

Among the many international initiatives to combat terrorism is the 2007 EU Commission's Framework Decision Proposal to make PNR data available to law enforcement agencies. But why would the Commission advocate such a procedure? To answer that question, it is imperative to know what PNRs are and what their function is.

A PNR record is the unique set of reservation and requested service data of a passenger. Whenever a traveler makes a reservation for a particular trip, a Personal Name Record (PNR) is created, which consists of information on all transportation components of the trip, most often containing air components.<sup>7</sup>

An airline can receive PNR information from passengers in three possible ways: [1] either through a direct reservation by the airline; [2] through indirect contact by a travel agent; or [3] interactively, by receiving data from central reservation systems, which are used by internet travel agencies, such as [www.expedia.com](http://www.expedia.com) or [www.cheaptickets.nl](http://www.cheaptickets.nl). Airlines only process PNRs in their databases and departure control systems for operational use. Part and

---

7 Because this creation process is primarily a digital – and hence invisible - process, for clarity purposes an imaginary reservation is made to elucidate this process. Consider the following simple example: a male individual plans to fly from Amsterdam to New York with KLM, where he intends to stay at the Waldorf Astoria Hotel for four days and rent a specific type of car. The individual is Jewish and books his trip online. During the booking process, not only will he make the reservation for the flight, hotel, etc., but he will fill out particular designated fields, which relate to, for instance, his credit card information, frequent flyer data, billing address, rental car preference, and other personal preferences, such as his request for a kosher meal. Upon completion of the booking, a PNR number – the confirmation number, a random combination of 6 letters and numbers – is created. In order to ensure a smooth trip, this information is made available to all 'hosts' within this trip, here: the hotel, the airline, and the rental car firm. The airline, *however*, transfers only the information in the PNR that pertains to the flight(s), not the data that relates to accommodation, or other components of the journey.

parcel of this use is a mandatory submission of such data through a ‘push’ method to the United States’ Customs and Border Protection (US-CBP) and the Canada Border Services Agency (CBSA).<sup>8</sup> Yet, these records are first and foremost put to use for airline service purposes: by entering this number in reservation systems, airlines and other hosts can view the subsequent PNR and examine all pertaining details to this trip, such as flights, and requested services, but also the number of people traveling. The number and nature of fields in a PNR differ from airline to airline and from passenger to passenger. In general, a PNR can consist of anywhere between 10 and 30 fields.<sup>9</sup> At the same time, a generic PNR holds oftentimes only between 6 and 10 elements.<sup>10</sup>

There is a logical explanation for this discrepancy. Passengers, not airlines provide the data in a PNR. Consequently, what is comprised in a PNR is in principal the work of the passenger, who selects flights, indicates travel companions, and puts down service requests with his/ her subsequent travel host. By supplying additional data, more information is also gathered and transferred; handing down less information means that less information can also be submitted by the airline. As such, airlines do not create the content of a PNR – the passenger creates it –, nor do airlines influence the amount of data included. Instead, it is the passenger, who enters practical data, requests, and preferences for the ‘travel host’. This host stores in turn this information only for operational and commercial, but certainly not for law enforcement purposes. Airlines therefore view PNRs principally as a ‘service request’, not as a counterterrorism tool.<sup>11</sup>

A number of Member States of the European Union believe that PNRs can have an additional function. They claim that in addition to the service function, PNRs can also play an important role in identifying potential security risks. In the Commission’s explanation of the grounds for the proposal, it is argued that “since 9/11 law enforcement authorities around the world have come to realize the added value of collecting and analysing so-called PNR data in combating terrorism and organised crime” whereby such

---

8 Law enforcement agencies in the United States can obtain PNR data in two ways. The first way is to oblige airlines to ‘push’ PNR data, the other option is that such agencies enter the airlines’ reservation systems and ‘pull’ such information to their databases.

9 Personal interview with Mr. Klaas Bruin, Privacy Officer at KLM Royal Dutch Airlines, conducted on 6 December 2007. In fact, the number of data can even exceed the 30 required fields, as can be found at <<http://www.statewatch.org/news/2003/oct/a1-ibcom1.htm>>, last accessed 20/01/2008.

10 *Ibid.* Bruin.

11 I am indebted to Mr. Klaas Bruin for the term ‘service request’.

an analysis and collection allow “law enforcement authorities to identify high risk passengers and to take appropriate measures”.<sup>12</sup>

Moreover, policymakers oftentimes claim that the transfer of PNR data should not be presented as an additional burden for airlines ‘on top’ of other obligations. Airlines already collect such data anyway. In their view, the only genuine change is that this data must now be shared with law enforcement agents.<sup>13</sup> Viewed whichever way, there exists in any case a discrepancy between passengers and airlines on the one side and the Council of the European Union and the European Commission on the other. The passenger sees the making available of data as a tool to enjoy greater comfort and the airline as a tool to provide this service; some of Europe’s policy makers view such undertakings by passengers as a tool to enjoy greater identification possibilities.

### **2.3 How Do PNR Data Separate themselves from Other Datasets?**

Counterterrorism officials and field agents base their assessment of an individual’s potential risk on gathered data pieces on that particular person. For this ‘risk scan’, they can rely in principal on three sets of data. In addition to PNR data, they can possibly draw on biometric data and Advanced Passenger Information (API) data.<sup>14</sup>

---

12 EU Commission (06 November 2007). ‘Proposal for a Council Framework Decision on the Use of Passenger Name Record for Law Enforcement Purposes’. COM (2007) 654/F, pp. 2.

13 This perception was conveyed to me on March 11, 2008 in a private conversation with Mr. Stefano Signore, former member of Mr. Franco Frattini’s Cabinet on Home and Justice Affairs.

14 Gathering passenger information and data is a relatively new feature of international counterterrorism efforts. While more countries are undertaking efforts to collect and disseminate such data, North American countries are the frontrunners of such developments. This explains why the storing of biometric data, and the transfer of PNRs is done primarily by the governments of the United States and Canada. Even *Advanced Passenger Information Data*, the most commonly transferred set of data is not collected globally.

### 2.3.1 Biometric Data

All air travelers to America are obligated to bequeath biometric data when they seek entrance to the US. Depending on whether the traveler's country of residence is a country under the Visa Waiver Program<sup>15</sup>, every non-US citizen must submit in advance or upon arrival, but in any case prior to passage through customs, a digital photograph and a digital fingerprint of all ten fingers. These items are stored in a database and gathered "to verify identity and screen persons against watch lists".<sup>16</sup> Through this effort, internationally sought offenders should ideally not be able to slip through the net.

Since 2003, the collection of biometric data is done under the United States Visitor and Immigrant Status Indicator Technology or US-VISIT program, a subdivision of the American Department of Homeland Security (DHS). By collecting such data, US-VISIT monitors the entry and exit of foreign nationals<sup>17</sup>, which in turn should "enhance the security of US citizens and visitors (...) and facilitate legitimate travel and trade".<sup>18</sup> Tracking the arrival and departure of incoming passengers is no small task. According to estimates, roughly 440 million individuals cross America's borders annually. Maintaining oversight over air traffic is thus relatively easy in comparison to the number of passengers who cross American landlines by boat, car or bus. Contrary to, for instance, a bus company, an airline keeps accurate and up-to-date records of the individuals on board. This information, plus the facilities in place at airports make it easier to screen all passengers in one setting. Counter to the US, Europe is unfamiliar with a procedure similar to US-VISIT. It does place with incoming travelers from certain non-Schengen residents the obligation to apply for a visa prior to arrival; however, a recent –

---

15 The Visa Waiver Program (VWP) relieves the passenger from the obligation to apply for a visa prior to departure, if the traveler's country of residence is a partner in the program. Passengers must still apply for a visa, but they can do this through the completion of an I-94 form upon arrival. In practice, this program applies mostly to passengers from Europe (22 European countries are VWP-partners, including The Netherlands). This means that, contrary to passengers from non-VWP countries, these travelers can submit a picture and a fingerprint upon arrival in the US and are not required to do this in advance. In both cases, however, the screening of the passenger is performed before the individual goes through customs.

For more information on the Visa Waiver Program, see <[http://www.dhs.gov/xtrvlsec/programs/content\\_multi\\_image\\_0021.shtm](http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0021.shtm)>.

16 Thompson, Bennie G. (June 2007). 'America's Unfinished Welcome Mat: US-VISIT a Decade Later'.

17 US Department of Homeland Security – Notice of Proposed Rule Making. Published in the Federal Register, vol. 73, No. 80. 'Collection of Alien Biometric Data Upon Exit From the United States at Air and Sea Ports of Departure'.

18 *Ibid.* 16, pp.3

not digital – photograph is required for that procedure. Furthermore, there exist no obligation for any incoming passenger to submit fingerprints upon arrival, although the European Commission recently initiated the introduction of such a system.<sup>19</sup>

### 2.3.2 *Advanced Passenger Information*

The collection of biometric data is but one approach in an encompassing effort to be able to screen all incoming passengers. In contrast to collection of the aforementioned biometric data, which is first and foremost an American affair, a number of countries, including all members in the European Union, request airlines to screen passengers on incoming flights on the basis of API data. Additionally, API data are oftentimes transferred to a receiving authority in the country of destination, for instance, in the case of the US, to the American Customs and Border Protection (CBP), a branch of DHS.

The acronym API refers to Advanced Passenger Information<sup>20</sup>, commonly understood as the set of data which is stored in the traveler's passport. Examples of 'machine readable passport information' include a full name; date, place and country of birth; a social security number; and a valid passport number. In addition, in the case of the US, an address within the US at which the traveler intends to stay, together with the traveler's current country of residence are also part of the API data. As can be noted, despite the fact that API data are widely exchanged between airlines and many countries, there exists no conformity as to the content of the data.

API data are put to use by a limited number of countries and airlines in their efforts to screen passengers and to flag those individuals, whose name in the passport appears on 'No Fly' or 'Selectee' watchlists.<sup>21</sup> These lists are in themselves again extracted from the consolidated Terrorist Screening Database (TSDB) by America's Terrorist Screening Center (TSC), who

---

19 EU Commission (13 February 2008). 'Communication From the Commission to the European Parliament, the Council, The European Economic Committee and the Committee of the Regions'. COM (2008) 69/F.

See also: International Herald Tribune (26 January 2008) 'Dan Bilefsky – Tough new EU controls are sought on travelers' and Deutsche Welle (25 January 2008). 'EU plans fingerprints, eye scan for visitors'.

20 American officials refer to this information as "APIS", which acronym stands for Advanced Passenger Information System. In both instances, however, they refer to the same dataset.

21 Although the names of the lists are self-evident, individuals whose name on the 'No Fly' list are always refused to embark; those on the 'Selectee' list are identified for further screening upon arrival. In July 2008, a total of approximately 1,000,000 names of individuals appear on TSC's watch lists. See: American Civil Liberties Union (23 July 2008). 'ACLU Watch List Counter. See: <<http://www.aclu.org/privacy/spying/watchlistcounter.html>>.

transmits these lists to airlines.<sup>22</sup> They use these lists also for non US- bound flights. The names of the lists are self-evident: any person, whose name appears on the ‘No Fly’ list and reports to the gate will be refused to embark, a passenger with a selectee status will find his boarding pass riddled with S’s. This individual is likely to experience additional screening upon arrival at a Port of Entry (POE).<sup>23</sup> Besides from European and North American destinations, airlines must send API data of passengers on flights to Australia, New Zealand, Mexico, South Korea, and China to those governments in order to screen the names against the aforementioned watchlists. Finally, airlines need to make, upon specific request, API data available to requesting authorities in European Member States, if the country has legislation on this issue.<sup>24</sup>

In conjunction, CBP obliges airlines to make API data available to the agency under the 2001 American Transportation Security Act (ATSA). While many airlines in the immediate aftermath of 9/11 did not yet have the necessary technical facilities to ‘push’ API data to the CBP, over the recent years, both CBP and most airlines adapted and updated their computer systems accordingly. Indeed, as of 19 August 2008, CBP will take over all screening efforts from the airline companies and will receive API data before departure of passengers on flights destined for the US from the airlines’ departure control systems. This will be done through a ‘push’ procedure. The processor of data, CBP, indicates that a prime reason to collect API data is that it provides “the ability to identify potential threats and coordinate with carriers and foreign law enforcement to prevent the boarding of a person of interest” by cross-checking passport information with watchlists.<sup>25</sup>

At present, there exists no agreement or obligation that conclusively addresses the transfer of API data from American airlines to European countries or institutions. API data thus flows into one direction across the Atlantic. In that sense, any form of reciprocity between the European Union and the US is absent. Instead, this matter is left to be addressed by individual countries as deemed appropriate and necessary. As the CBP also acquires API data from American airlines underway to Europe and runs this data too against watchlists, European countries rely for now for their external safety on their

---

22 GAO (8 November 2007). ‘Terrorist Watchlist Screening’, pp. 7.

23 Originally, CBP intended to take over the screening obligation from airlines. This deadline was recently postponed to August 19, 2008. See, for the original provisions, Federal Register 19 CFR parts 4 and 122.

24 Council of the European Union (29 April 2004). ‘Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data’.

25 Customs and Border Police (10 August 2007) DHS. ‘Fact sheet APIS’.  
See: <[http://www.cbp.gov/linkhandler/cgov/travel/inspections\\_carriers\\_facilities/apis/apis\\_factsheet.ctt/apis\\_factsheet.pdf](http://www.cbp.gov/linkhandler/cgov/travel/inspections_carriers_facilities/apis/apis_factsheet.ctt/apis_factsheet.pdf)>.

American counterparts. That said, the European Commission articulated in Communication 69/ Final its intention to establish a European system to monitor the entry and exit of third country nationals.<sup>26</sup>

#### **2.4 What Factors Propelled Data Collection to Prominence?**

9/11 was a decisive event for aviation security, spurring a plentitude of new security measures. The level of security on both domestic and international flights was recognized as both critical and inadequate. The belief that security should be shored up was internalized particularly – and logically - by policy makers within relevant departments in the US. They launched a number of proposals to enhance security on such flights, with the objective to keep terrorists and criminals at bay. After securing the appropriate legal foundation, these proposals were transformed to action plans and security measures.

While it is beyond the scope of this paper to discuss all initiatives individually, it is fair to conclude that any effective effort to keep terrorists off airplanes was supposed to include a risk assessment, or a screening of passengers through the use of data collection and data dissemination. Specifically, one method of screening – security profiling on the basis of PNR data – became viewed by those within the intelligence community as a new, but crucial tool to ward off terrorists. The potential value that the acquisition of PNR data may constitute in counterterrorism efforts was first recognized in the United States. In retrospect, it is easy to retrace the factors that have helped to shape the conviction that PNR data are of added value to the fight against terrorism and that, as a result, these data should become available to law enforcement agencies. Two principal events should be noted to frame this belief.

First, the gruesome events on 9/11 promulgated a rethinking of the policies in place, aimed to decrease the risk of terrorist attacks via the use of airplanes. If 9/11 had revealed one thing, it was that policies to secure air travel were by no means adequate. In the years leading up to 9/11, air travel, particularly in the US, became increasingly known for its high levels of convenience, not for its standards of excellence in security measures. An instant result of 9/11 was therefore a rethinking of policies aimed to secure mass public transportation as a whole and airlines explicitly. The value attributed to PNR data and the ensuing demand to make such data available to law enforcement agencies is a clear example of this process of ‘rethinking’.

---

26 *Ibid.* COM (2008) 69/F.

Second, with hindsight information, PNRs appeared to have been the golden formula to stop terrorists. While much of our knowledge as to what went wrong, both on that particular Tuesday in September 2001, but also in the months leading up to the attack, stems from the work of the 9/11 Commission, one grudging, but crucial fact on the handling of individual data was instantly clear. Had the various US agencies had the ability to access data other than passport and visa data and had they been able to cross-check PNR data against other data, the chances of the occurrence of the attack would have seriously decreased, because explicit ties between the hijackers would have surfaced. These could have prompted action.<sup>27</sup> Although initiatives to enforce airlines to make passenger data available were already well underway by the time the 9/11 Commission Report was published, the 2004 final report concluded with authority what many knew informally: analyzing passenger data may facilitate the exposure of terrorists. The report notes that screening on the basis of personal data was a tool “to establish that people are who they say they are and are seeking access for their stated purpose, to intercept identifiable suspects, and to take effective action”.<sup>28</sup> Legitimacy was herewith given retroactively to data screening, particularly if done on the basis of previously unexploited PNRs.

Gradually then, facts that became available about the failures and misfortunes of intelligence organizations in relation to the country’s national trauma, both in the press and through an authoritative report, nourished the notion among US policy makers that personal data was an invaluable tool in the fight against terrorism, and specifically counter ‘airline-terrorism’ efforts. As a result, the 9/11 Reports’ convictions served to cast the attributed value of the acquisition of data – PNR and other data - for law enforcement purposes in a completely different light. The transfer of PNR data to deflect future attacks became the cause for future PNR exchange negotiations. The legacy of these negotiations are a number of agreements between the European Union and third countries.

## **2.5 Legal Obligations for the Exchange of Personal Data**

The changing perspective on screening efforts via personal data, particularly with regard to their potential, created among a number of countries the desire to oblige airlines to make passenger data, held within their computer and reservation systems, available to law enforcement authorities.

---

27 The 9/11 Commission Report (August 2004) ‘*Final Report of the National Commission on Terrorist Attacks upon the United States*’. New York: W.W. Norton & Company, pp. 384.

28 *Ibid.* pp. 387-389.

Not surprisingly, the first country to do so was the United States. On November 19, 2001, the US Aviation and Transportation Act (ATSA) passed. Under Title 49, ATSA requires foreign airlines to submit and make available passenger manifests and other passenger data - including, but not restricted to PNRs - to US Customs and Border Protection.<sup>29</sup> In a 2003 communication from the European Commission to the Council and the European Parliament, the Commission summarizes the width and depth of the measure as follows: “airlines operating passenger flights to, from or through the United States [must] provide US authorities, upon request, with electronic access to PNR data (...)”.<sup>30</sup>

Also in 2001, the Canadian Border Service Agency (CBSA) received authorization to initiate procedures that would allow for the collection of API and PNR data on all passengers traveling to and from Canada under section 107.1 of the Customs Act and the Passenger Information (Customs) Regulations. Principally, Canada’s regulations mirror the objectives and operating directives of the United States with regard to the collection of passenger data by carriers and their further transfer. And, similar to the US, Canada too requires from airlines admission to personal traveler’s data, i.e., both Canada’s BSA and America’s CBP would get access to airlines’ reservation systems and ‘pull’ data to their processing units. With hundreds of flights daily from Europe to America and Canada and vice versa, it is clear that European airlines, their host governments and thus the European Union as a whole would directly be affected by these measures, in particular when the consequence of disobedience could be financial penalties or the suspension of landing permissions.<sup>31</sup>

---

29 49 U.S.C. §49909 (C).

30 Communication from the European Commission to the Council and the European Parliament – Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, pp. 3. See: <[http://www.statewatch.org/news/2003/dec/apis\\_en.pdf](http://www.statewatch.org/news/2003/dec/apis_en.pdf)>, last accessed 22/01/2008.

31 Guardian (20 February 2003). ‘Jeevan Vasager - US Demands Air’ travelers Data’. See: <<http://www.guardian.co.uk>>, last accessed 05/06/2008. According to OAG Back Aviation Solutions, this could affect approximately 50,000 flights annually. See: <<http://www.oag.com>>, last accessed 18/07/2008.

Torn between own economic interests and the concerns of governments with regard to terrorism, airlines realized in addition that any compliance with the aforementioned obligations may conflict with the 1995 EC Data Protection Directive on the processing and free movement of personal data.<sup>32</sup> Logically, airlines were wary to submit such data without approval from Brussels, which is why they looked to European law- and policymakers to negotiate jurisdiction which would remove inherent precarious obstacles.<sup>33</sup> Recognizing the airlines hesitations and concerns, the European Commission, through then Commissioner for the Internal Market Frits Bolkestein, notified officials in Canada and the US that these provisions indeed had the potential to infringe upon the jurisdiction of individual Member States and on the jurisdiction of the Community as a whole. Consequently, the Council of the European Union tasked the European Commission to draft agreements with the Canadian and American governments, which content and provisions would neither infringe upon European Community law, nor circumise American, Canadian and European counterterrorism efforts, but would instead create a legal basis for the exchange of PNR data by airlines so as to ensure that European airlines would not be refused permission to land due to an absence of data, or a failure to transfer PNR information altogether.

The legacy of these bilateral negotiations comprises five agreements: [1] the 2004 EU – US PNR agreement, which the European Court of Justice in 2006 ruled to be founded on the wrong legal basis; [2] the 2005 EU- Canada agreement on API and PNR data; [3] the 2006 EU – US Interim PNR agreement, which functioned to replace the annulled 2004 agreement, but was in itself replaced in the summer of 2007 by [4] a new and definitive EU – US agreement on the submission of PNR data, and [5] the PNR agreement

---

32 European Parliament & the Council (24 October 1995). ‘Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data’.

33 As the request for data applied to all European Member States with flights to and from Canada and the US, Member States opted to negotiate with the US and Canada through the European Commission, rather than on an individual basis. The obstacles that arose out of this choice were the extent to which the European Parliament would be involved in these negotiations and on which legal basis these agreements would be founded. As to the latter question, some argued that the transfer of PNRs, collected for commercial purposes, constituted a community policy-matter (pillar one). Others claimed that the transfer of such data was a criminal matter in which the police and the judiciary cooperated, hence a third pillar issue. During the negotiations on the first agreement, the European Parliament (EP) was included as the request was considered a ‘first pillar’ issue. At a later stage, the purpose for which these data would be transferred was more perceived as a ‘third pillar’ issue, which resulted in the side-lining of the European Parliament, as issues, falling within the field of Police and Judicial Cooperation in Criminal Matters can be decided upon without EP approval.

between the European Union and Australia from June 2008. In addition to the previous agreements, the European Commission put forward in November 2007 its own proposal to follow into the footsteps of Canada, America and Australia and to also become an actor to whom airlines from those countries outside the European Union should submit PNR data.<sup>34</sup>

## 2.6 Conclusion

Crucial in the debate on the need and necessity of the exchange of PNRs in order to counter ‘airline terrorism’ is to have an understanding of the constellation that surrounds the term ‘PNR data’. This chapter colored this term and explained on which points PNR data differs from other personal data sets. This is important, as the purpose of the underlying proposal of the European Commission is to keep terrorists off airplanes by putting PNRs to use. They are considered to provide substantial information on the background of the individual on which an accurate risk analysis can be made. It also discussed the two factors that significantly channeled the way of thinking after 9/11 with regard to passenger screening: the circumstances surrounding the event itself and the conclusions from the 9/11 Commission Report. Finally, this chapter highlighted the pieces of legislation that arranged for the transfer of PNR data between Europe and the US and Canada, as the conditions of the agreements with these countries can impact transatlantic flights most significantly. The next chapter will discuss the different agreements that resulted from the aforementioned legislation and extract the specific data fields that airlines are required to transfer under the appropriate agreement.

---

<sup>34</sup> South Korea has also indicated that it wishes to receive the PNRs of passengers on flights from the European Union. However, no final agreement has yet been concluded between the EU and South Korea that arranges for the transfer of such data.

## 3. EXCHANGING PNR DATA

---

### 3.1 Introduction

The content and provisions of three agreements and one proposal command the discussion within this chapter. These agreements are the 2005 EU – Canada Agreement on the processing of API and PNR data; the 2007 EU – US PNR Agreement; and the 2008 EU – Australia PNR Agreement; the proposal is the 2007 European Commission Proposal for a Framework Decision on the transfer of PNR data. The main purpose is to highlight cross-cutting differences and to make a distinction between the extent of ‘controversy’ of the three agreements and Europe’s own proposal. While the content of all documents arranges for the transfer of PNR data to countries (USA, Canada, and Australia) or entities (European Union), remarkable differences can be noted among and within the different provisions that stipulate the content of the data to be transferred. This is all the more important as Europe enjoyed a choice in the drafting stages of its own Proposal: it could shape it to emulate either the Canada agreement, or to that with the US. Its choice to have its proposal mirror that with the US, not with Canada, bodes that Europe sides with the American, not the Canadian approach on PNR matters.

### 3.2 Agreements and a Proposal

Three agreements are concluded on the transfer of PNR data from European airlines to American, Canadian, and Australian customs agencies. In addition, in November 2007 the EU Commission on Justice, Freedom, and Home Affairs made public a proposal to come to a European-wide system to collect PNR data from airlines. Main purpose is to stop terrorists by closing perceived security breaches of and between individual member states. The content and specific provisions are discussed hereafter, whereby a special focus lies on four precarious elements within the agreements and the proposal: [1] number and content of PNR data fields; [2] data retention; [3] safeguards against infringement upon privacy rights; and [4] evaluation procedures to measure the effect of the undertakings.<sup>35</sup> These elements are not chosen at random: in most discussions on this issue, the debate centers commonly on one or all of these aspects.<sup>36</sup>

#### 3.2.1 *The 2005 EU – Canada PNR Agreement*

As noted earlier, in 2001 the Canadian government passed legislation which sought to make PNR components available to law enforcement agencies. Initially, the transfer of this data would commence on October 7, 2002 (API data) and in July 2003 (PNR data). Due to analyzing inhibitions, the starting dates for the collection of PNR and API data were shifted back by Canada's CBSA, and finally took effect in the summer of 2005.

Recognizing the urgency to address this matter, the Council of the European Union authorized in response the European Commission to engage in negotiations with Canadian officials on this issue; the result being the 2005 EU – Canada API/PNR Agreement.<sup>37</sup> As part of this agreement, the transfer of PNR data from airline companies to Canada's competent authority, CBSA, the Canadian Border Service Agency, is specified. Particularly, the distinct data fields that fall within the terms of the agreement are elaborated on. In total, CBSA may seek access to 25 data elements through a 'pull' method, in

---

35 It should be noted that only the 'active' agreement with the US is discussed in this paragraph, given the fact that both the 2003 and 2006 agreements with the US were recently replaced by the encompassing 2007 agreement.

36 See, for instance, Article 29 Data Protection Working Party. 'Joint Opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007', WP 145 WPPJ ref: 01/07

37 Contrary to the 2003 agreement between the Europe and the US, the 2005 agreement was based on Article 95 and 300 (2) of the Treaty establishing the European Union – in the eyes of many, particularly the European Parliament, a more appropriate legal foundation for the conclusion of this and future accords.

which the competent body extracts the PNR data from Table 1 from the departure system of the subsequent airline.

Data elements to be disclosed to CBSA	
1	PNR Record locator
2	Date of reservation
3	Date(s) of intended travel
4	Name(s)
5	Other names on PNR
6	All forms of payment information
7	Billing address
8	Contact telephone numbers
9	All travel itinerary for specific PNR
10	Frequent flyer information
11	Travel agency
12	Travel agent
13	Split/ Divided PNR information
14	Ticketing field information
15	Ticket number
16	Seat number
17	Date of ticket issuance
18	No show history
19	Bag tag numbers
20	Go show information
21	Seat information
22	One-way tickets
23	Any collected API information
24	Standby
25	Order at check in

**Table 1:** PNR data fields submitted to Canadian authorities under the 2005 EU-Canada PNR agreement<sup>38</sup>

---

38 European Commission (19 May 2005). ‘Council Decision 2005/0095 (CNS) on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data’.

Anticipating the discussion of the 2007 EU- US agreement and the 2007 Commission proposal, one should note the absence of the field 'general comments' in this list, which is included in other agreements. The field 'general comments' is the primary field where a passenger can make specific requests; in the example from chapter 2, for instance, the preference for a kosher meal. Yet, it is also the field where an airlines' service employee can possibly enter personal experiences with the passenger, which may cast suspicion on the individual unintentionally. One example is such a comment as 'difficult customer' or 'passenger requested specifically for seat 16B'. While this information in essence should be harmless, it could become potentially harmful to the passenger, when risk assessors value such comments over established facts or, even worse, act solely on such information.

The EU – Canada Agreement dedicates not a single word to the retention of data. However, it has become known that data is kept for a total of 3.5 years.<sup>39</sup> Whether this retention period is proportional or not is unclear. In any case is the period of data storage significantly longer than the number of years airlines store PNR's. They remove PNRs from their on-line databases within 24 hours after the passing of the last leg of the trip. Another cause for ambiguity is the fact that no official review has been undertaken yet that could convincingly prove the need to store data for the duration of 3,5 years. At the same time should the 3,5 years time span for storage be considered a mild retention period in comparison to the 15 years that data are to be kept under the 2007 EU – US Agreement.

PNR data are to be submitted to CBSA, the only competent authority to receive this data, and remains only in their hands from the moment of transfer until the moment of deletion. Moreover, a passenger, who feels wrongfully identified as a potential security risk is ensured proper redress options to correct wrongdoings under article 3 of the Agreement.

Interesting to note with regard to the evaluation of the functioning of the agreement are the Agreement's articles 6 through 9, which propose the installment of a committee, drawn up of European and Canadian officials to 1] oversee the implementation of the agreement; 2] serve as main communication tool between both parties; 3] arbitrate over differences between parties; and 4] arrange for joint evaluations. As of July 21, 2008, no official review of this agreement had been conducted.

---

39 Article 29 Data Protection Working Party. 'Joint Opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007', WP 145 WPPJ ref:01/07, pp. 9.

### 3.2.2 The 2007 EU – US PNR Agreement

	Data for all passengers
1	PNR Record locator
2	Date of reservation
3	Date of intended travel
4	Name(s)
5	Address and Contact Information (telephone number, e-mail address)
6	All forms of payment information, including billing address
7	All travel itinerary for specific PNR
8	Frequent flyer information
9	Travel agency/ travel agent
10	Travel status of passenger, including confirmations, check-in status, no show or go show information
11	Split/ divided PNR information
12	General remarks (excluding sensitive information)
13	Ticketing information, including ticket number, date of ticket issuance, and one-way tickets, Automated Ticket Fare Quote Fields
14	Seat number and seat information
15	Code share information
16	All baggage information
17	Number and other names of travelers on PNR
18	Any collected API information
19	All historical changes to the PNR listed 1 to 18
<b>Table 2: PNR data fields submitted to American authorities under the 2007 EU-US PNR Agreement<sup>40</sup></b>	

Confronted with an invalid agreement from 2004, an interim agreement which was set to expire on July 31, 2007, and mounting pressure from the side of American border officials, European policymakers finally concluded the negotiations on the transfer of PNR data by European airlines on July 23, 2007.<sup>41</sup> Under this agreement, the PNR data from Table 2 are to be transmitted. As for the number and content of PNR data fields, only 19, not 25 elements are to be transferred. This does not mean that American security officials require less PNR information than their Canadian counterparts. Rather, to arrive at 19 fields, American diplomats *merged*, not *deleted* data fields. Less fields is therefore a mere optical illusion in terms of information-gathering. Bothersome is too that not only are more data accrued, but they are also more ambiguous in their nature. More in the sense that one particular field - the 'general information' field - is added, which is not included in the

40 *Ibid.* 39

41 Council of the European Union (July 23, 2007). 'Agreement on the Processing and Transfer of Passenger Name Record Data by Air Carriers to the United States Department of Homeland Security - "PNR", 11304/07

EU – Canada agreement. It is also more ambiguous in the sense that this extra field is also the most likely to hold sensitive or judgmental information.

It is namely in this field that meal requests – perhaps indicating a particular belief – or other preferences can be included.<sup>42</sup> While the Department of Homeland Security pledges in the agreement to delete such information immediately, this data must still be processed in order for it to be understood as ‘sensitive information’. Moreover, the DHS promise should not be overvalued: a pledge remains a pledge, especially in the absence of ramifications.

As for the retention of data, the EU and the US agreed that the number of years data can be preserved would be set at 15, whereby the data is stored in an active database for seven years and in a ‘dormant’ database for another eight years thereafter. The same retention conditions will apply in retroaction to the data accrued under the 2004 and 2006 agreements. Interesting to note is that the European Union, as its signatory, bestows considerable trust upon the DHS in their procedures to protect precarious data against further - improper - distribution. The agreement goes as far as mentioning that DHS is “deemed to ensure an adequate level of protection for PNR data transferred from the European Union”. This is saying with different words that the EU believes that DHS can ensure an adequate level of protection for passenger data received from European airlines, effectively relying on DHS’ safety provisions, rather than demanding that narrow defined European criteria must be met. The signing off of the responsibility to ensure a proper protection of data is all the more remarkable when considering that the EU is a more strident promoter of data protection than the US.

Finally, the procedure for a review of the agreement constitutes a remarkable element within the provisions. While the success of the agreement can only be gauged on the basis of regular and conclusive reviews, that incorporate hard data on the number of PNR files transferred or the number of arrests made on the basis of such information, the accord is remarkably silent on a timeframe or practical arrangements of the review.

---

42 Indeed, there remains unclarity as to whether information on meal preferences are included or excluded from the screening process. While the profiling on the basis of religion is strictly forbidden, information as to ‘specific preferences on board’ *can* be drawn upon. Such preferences can include, amongst others, meal preferences, which can indicate in turn a particular belief. This could again make profiling on the basis of religion possible, albeit indirectly.

The intention is expressed to “periodically review” the agreement, but the term ‘periodically’ is just as unclear as the span and results of the first and only review conducted thus far.<sup>43</sup> Inevitably then, all parties involved, but especially the general public, must rely on assuring statements to be convinced of the agreements’ effectiveness, rather than on factual information that points to net results. Moreover, the absence of cemented arrangements on the conduct of a review may postpone a thorough assessment or put off such an analysis altogether, unless some agency or individual is compelled to critically and publically evaluate the agreements’ results.

### 3.2.3. *The 2008 EU – Australia PNR Agreement*

The 2008 EU – Australia PNR Agreement is again different from the agreements with both Canada and the US. First of all, it is much smaller in scope as only three airline routes fall under this agreement. The only direct routes between Europe and Australia are namely from London to Sydney, respectively Melbourne, and the route Frankfurt – Sydney. By contrast, the accord with the US applies to the passengers on an average 136 flight per day. The difference between the agreements with Canada and the US and Australia lies also in the number and the content of data fields, which size and substance resembles the provisions in the EU – US Agreement.<sup>44</sup> Another difference is the number of years that data is to be stored, which stipulation resembles more the content of the agreement with Canada. Data can be kept up to a maximum of 5,5 years by Australia’s competent authorities, a time span that lies in between of Canada [3,5 years] and America’s [15 years]. It should be noted that Australia will retain data for 3,5 years actively, after which this information is stored for another 2 years.<sup>45</sup>

---

43 The width and depth of the first review is unclear until the day. According to the former EU- Counterterrorism coordinator, Mr. Gijss de Vries, this review sought to determine whether the US interpreted the data sharing provisions under the 2004 EU – US Agreement in a similar fashion as its European counterparts. To this end, DHS sent a letter to the Council of the European Union and the European Commission to clarify “our understandings with regard to the interpretation of a number of provisions of the Passenger Name Record (PNR) Undertakings issued on May 11, 2004 by the Department of Homeland Security (DHS)”.

Council of the European Union (11 October 2006). ‘Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the undertakings issues by DHS on 11 May 2004 in connection with the transfer by air carriers of passenger name record (PNR data)’, 13738/06.

44 Council of the European Union (10 June 2008). ‘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’, 9946/08.

45 *Ibid.* pp. 13 (Annex)

As this agreement also paves the way for custom’s officials to access the ‘general remarks’ field, the annex to this agreement stipulates that, similar to the provision included in the EU – US Agreement, “customs shall filter out all sensitive EU-sourced data and shall delete all such data without any further processing”.<sup>46</sup> The inclusion of this provision should, however, not be understood that PNRs holding sensitive information are not viewed. Rather, this information prescribes that such information, after being marked as sensitive, is not to be analyzed further.

	Data for all passengers
1	PNR Record locator
2	Date of reservation/ issue of ticket
3	Date(s) of intended travel
4	Name(s)
5	Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.)
6	Other names on PNR, including number of travelers on PNR
7	All available contact information (including originator information)
8	All available billing/ payment information
9	Travel itinerary for specific PNR
10	Travel agency/ travel agent
11	Code share information
12	Split/ divided PNR information
13	Travel status of passenger (including confirmations and check-in status)
14	Ticketing information, including ticket number, date of ticket issuance, and one-way tickets, Automated Ticket Fare Quote Fields
15	All baggage information
16	Seat information, including seat number
17	General remarks (excluding sensitive information)
18	Any collected API information
19	All historical changes to the PNR listed 1 to 18

**Table 3:** PNR data fields submitted to Australian authorities under the 2008 EU-Australia PNR Agreement

Australia is – next to Canada - also seen as a partner to whom PNR data can safely be transmitted. Already in January 2004, the Article 29 Working party “assumes that Australia ensures an adequate level of protection [...] with regard to the processing of Passenger Name Record Data from airlines to

---

46 *Ibid.* pp. 7 (Annex). The agreement understands ‘sensitive data’ as: “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life”.

Australian authorities”.<sup>47</sup> Five agencies and departments can receive PNR data, being the Australian Crime Commission; Australian Federal Police; Australian Security Intelligence Organisation; Commonwealth Director of Public Prosecutions; and the Department of Immigration and Citizenship.<sup>48</sup> This information is rather remarkable, as it states clearly who may receive data and who not – a provision unseen in the agreement with the US. Finally, the EU and Australia voice in the agreement their intentions to “periodically undertake a joint review of the implementation of this agreement”.<sup>49</sup> This intention suffers, however, from the same drawbacks as the review proposals within the other agreements: it remains unclear when this is done and whether the success of the measure as a whole is reviewed, or only whether Australia’s Customs Service abides to the provisions on data protection, as was the case with the review of the 2004 EU – US PNR Agreement.

#### 3.2.4 *The 2007 EU Commission Proposal*

Europe was to follow Canada and the US suit. By November 2007, it had become time for Europe to put forward its plans to introduce a similar PNR data collection effort. Then commissioner Frattini made public the Commission’s proposal to come to a system for the collection of PNR data from passengers from ‘third countries’ to Europe and vice versa. In many aspects, the proposal mirrors the 2007 Agreement with the US, as can also be observed in the PNR fields that the different European countries would require and acquire access to. Similar to the provision in the agreements with the US and Australia the EU too seeks access to the field in which ‘general remarks’ may be contained.

At the same time, Mr. Frattini’s proposal deviates partially from the provisions under the 2007 EU – US Agreement in terms of data retention. In comparison to that accord, the Justice Commissioner proposes to store data in an active database for 5 years (7 under the US agreement) after which data is moved to a dormant database for another 8 years (identical to the US agreement).<sup>50</sup> Also, the outer characteristics of the database in which data is kept are different. In the United States, PNR and API data are combined into one national database: the Automated Targeting System (ATS) of the Customs and Border Protection (CBP). A combination of such data should “assist the CBP officer’s decision-making process about whether a passenger

---

47 Article 29 Data Protection Working Party (16 January 2004). Opinion 1/2004 on the protection ensured in Australia for the transmission of Passenger Name record data from airlines’, 10031/03/EN/WP85, pp. 13.

48 *Ibid.* 44, pp. 13 (Annex)

49 *Ibid.* 44, pp. 13

50 *Ibid.* COM (2007) 654/F.

or crewmember should receive additional screening prior to entry into or departure from the country because the traveler may pose a greater risk for violation of US law”.<sup>51</sup> By contrast, Mr. Frattini proposes the establishment of 27 ‘Passenger Information Units’ (PIU), rather than one EU-wide database. The main reason for doing so, is that a majority of member states preferred this option over one European database – a preference that is not further substantiated on in the proposal.<sup>52</sup>

Preferably, despite obvious possible differences in data storage methods, and language and access procedures, these databases should still be able to exchange accurate data quickly and efficiently.<sup>53</sup> At the same time, one can readily imagine the organizational rigmarole for European and third countries’ airlines to comply with the prerequisites of 27 different databases. Moreover, it begs the question just how many airlines from third countries are able to comply with these provisions.

---

51 DHS (22 November 2006). ‘Privacy Impact Assessment for the Automated Targeting System’, pp.4

52 EU Commission (06 November 2007). ‘Proposal for a Council Framework Decision on the Use of Passenger Name Record for Law Enforcement Purposes’. COM (2007) 654/F, pp. 5.

53 *Ibid.* COM (2007) 654/F.

	Data elements to be disclosed to the EU- PIU's
1	PNR Record locator
2	Date of reservation
3	Date of intended travel
4	Name(s)
5	Address and Contact Information (telephone number, e-mail address)
6	All forms of payment information, including billing address
7	All travel itinerary for specific PNR
8	Frequent flyer information
9	Travel agency/ travel agent
10	Travel status of passenger, including confirmations, check-in status, no show or go show information
11	Split/ divided PNR information
12	General remarks (excluding sensitive information)
13	Ticketing information, including ticket number, date of ticket issuance, and one-way tickets, Automated Ticket Fare Quote Fields
14	Seat number and seat information
15	Code share information
16	All baggage information
17	Number and other names of travelers on PNR
18	Any collected API information
19	All historical changes to the PNR listed 1 to 18

**Table 3:** PNR data fields submitted to Europe's Passenger Information Units under the 2007 EU PNR Proposal 54

Similar to the US and Australia agreements, the European Commission here too stresses that PIUs should immediately delete information pertaining to possibly discriminatory facts. In the wording of the proposal, “(t)o the extent that the PNR data of a passenger as collected, includes (...) special categories of data that would reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life of the passenger concerned, the Passenger Information Unit shall delete such data immediately”.<sup>55</sup> This promise obscures, however, again the fact that data must first be processed in order for it to be understood as inappropriate data – meaning the data will land on the plate of a data disseminator in any event.

54 *Ibid.* COM (2007) 654/F, pp. 24.

55 *Ibid.* COM (2007) 654/F.

Lastly, with regard to review procedures to gauge the success of the provisions within the proposal, the Commission suggests to conduct such a review “within five years after this Framework Decision enters into force”. Such a critical analysis of the operation of the transfer and collection of PNRs should be based on the statistical data that Member States will be required to collect on the number of arrested, screened, or stopped passengers.<sup>56</sup> Indeed, this provision is laudable for its arrangements and indicates the Commission’s inclination to monitor sharply the exchange of PNR data. However, exactly because hard data is essential to gauge the success or the failure of the Framework Decision, it begs the question why the European Commission was unable or unwilling to include a similar provision in either the 2005 EU – Canada or the 2007 EU – US Agreement through which the need and necessity for the underlying proposal would be easily assessable.

A further cross-comparison between the two agreements and the proposal indicates an additional number of distinct features.

Although each Member State is encouraged to establish its own PIU, countries can also jointly establish a PIU. States who may consider this option are those that experience few international flights from ‘third countries’ or those, for whom the establishment of such a ‘data center’ is financially not feasible, because they receive few flights in general from third countries’ airlines.

Data received can only be transmitted by the national PIU to designated law enforcement agencies – non specified ‘competent authorities’ - within the respective country. In all cases, the international exchange of data will occur at PIU level, not at the – lower – law enforcement level so as to ensure privacy standards. Conversely, if a receiving country has not established a PIU, Member States may submit PNR data to law enforcement authorities from these countries if the request is deemed appropriate and the data adequately protected. A particular point of critique in this respect is that undemocratic states, with unclear and unreliable data protection safeguards may require airlines too to disclose PNR data on their passengers on a reciprocal basis.

Air carriers will be obligated to transmit PNR data to PIU’s on two occasions: 24 hours before departure and immediately after departure by ways of a ‘push’ method, i.e., an electronic transmission of data by the airline to the PIU. In exceptional cases, PIU’s may demand from airline companies to submit PNR data even further in advance.<sup>57</sup>

---

56 *Ibid.* COM (2007) 654/F.

57 *Ibid.* COM (2007) 654/F.

### **3.3 Conclusion**

The EU has engaged in a number of discussions with third states in order to conclude agreements on the transfer of PNR data from European airline companies to respective screening authorities within the US and Canada. These agreements differ significantly, whereby the EU – Canada agreement can be considered as potentially less ‘harmful’ than the EU – US agreement. In addition, the EU itself launched late 2007 its own proposal to also commence the collection of PNR data from passengers on flights heading to and originating from ‘third countries’. By modeling such a proposal in the first place, the European Commission indicates that it itself has become convinced of the need and necessity to collect PNR data, and has internalized assumptions as to the data’s added value in efforts to counter terrorism. Moreover, by sculpting the proposal on the example of the EU – US agreement, and not on the EU – Canada agreement, the Commission shows that it has become convinced –without specific motivation - of the extra merits that the additional data incorporated in the EU – US Agreement offer over the ‘stripped’ set of data collected under the EU – Canada Agreement. The fear to ‘miss out’ on certain information may explain this choice, but it should be noted that the added value of America’s data set over Canada’s has not yet been demonstrated beyond reasonable doubt.

Chapter four will discuss the stated results thus far of the acquisition of PNR data. While for some these results are a reason to point to the benefits of collecting PNR data, others highlight the detriments and flaws that are inherent in the collection and transfer of PNRs particular with respect to the objective for which PNR data may eventually be used: profiling. The next chapter will discuss both viewpoints at length.



## 4. DO PNRs ACTUALLY 'WORK'? – ARGUMENTS FOR AND AGAINST THE TRANSFER OF PNRs

---

### 4.1 Introduction

This chapter will discuss identifiable merits and detriments of the exchange of PNR data. Main goal is to assess whether PNR data collection and analysis actually 'work' and are an appropriate tool to counter terrorism. Depending on the outcome, standing opinions on the proposal may have to be reviewed.

The fault line along which the PNR debate is fought, centers around one crucial question: does the collection, transfer, and processing of PNRs appear to function in such a way that it is possible to conclude that PNRs 'work'? Or can too many drawbacks be observed, programmed within the entire cycle of collection, transfer, and administration, which could warrant the claim that PNRs do not work?

Supporters of these claims can be found on either side. But it would be wrong to look at their 'claim to fame'. Rather, their arguments and the experiences from which they draw should matter. To assess whether the transfer and collection of PNRs 'works' and is appropriate merely means to understand why proponents could subscribe to this belief; to understand why PNRs 'do not work' requires undertaking an assessment into the arguments of opponents.

Before entering into the discussion as to the costs and benefits of PNR data, it is important to note that, until this date, there exists no single report that

holds hard data on the number of arrests, warrants, etc. in relation to PNR data. This deficiency also implies that the conclusion can be drawn that PNRs appear to work or not. Hard facts are lacking, a lacuna that inevitably lifts appraisals and critiques – oftentimes reflecting personal opinions or interests – to prominence. These result-estimates make in turn an assessment more difficult in terms of reliability. After all, in the absence of hard-nosed facts, it remains possible to fiddle with results for personal opinions.

Ostensible results, promulgated by representatives of the American and the British government, are the dominant proof of evidence that PNRs indeed function accordingly; evidence that is supplemented by the conclusion of a report prepared by the British House of Lords. Against this deduction are a number of critiques, submitted in response to specific proposals, draft resolutions, or agreements that involve PNRs. These opinions – by default – focus on and criticize the specific aspects of the very document they respond to, rather than to cast light on the need and necessity of the collection of PNR data as a whole. However, valid overarching points as to the regulations' benefits and detriments can still be derived from their content, through which an estimate as to why PNRs do not work can be made.

#### **4.2 Why PNRs Work...**

In general, proponents of the use of PNRs have one overarching argument for the introduction of a PNR scheme: PNRs can deliver the results they are expected to deliver.<sup>58</sup> More to the point: the value of PNRs lies in the fact that they can and have proven to 'work'. Not only must this statement mean that PNRs have contributed to the apprehension of, among others, terrorists, but also that no other factors inhibit the utilization of PNRs for counterterrorism efforts. Logically, such an opinion requires support. This support is provided by, what can be considered as, three main arguments. At the same time, these arguments are never explicitly mentioned as such. Contrary to the counterarguments of opponents, proponents refrain from discussing why PNRs do work on a detailed level. They let 'results' speak for themselves. That said, proponents are rarely asked to discuss why PNRs are effective, because the audience is commonly indifferent, ill-informed on the subject matter, or already convinced. After all, if it can be concluded that PNRs work and the sought after results are accomplished, why look any further? These

---

58 Letter of the State Secretary of Foreign Affairs of the Netherlands (29 January 2008). 'Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie'. Beoordeling Nieuwe Commissievoorstellen (BNC) advice 22112, no. 608, pp. 6. This letter states that PNRs led to 'demonstrable results' in the fight against terrorism and transnational crime.

arguments are thus not so much opinions specifically put forward by proponents, but rather arguments that the author considers supportive to the supposition that PNRs function for counterterrorism efforts.

The first argument in support of the assumption that PNRs work, is that experiences with the collection and transfer of PNRs have indeed produced results. Those in favor of the PNR cycle generally point to such results to make their case. One good example of a body supportive of the transfer and analysis of PNRs is America's Department of Homeland Security, and more specifically Secretary Michael Chertoff. In response to a request put forward by members of the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs – the LIBE Committee - Mr. Chertoff laid out in a letter eight instances<sup>59</sup> where PNR data were useful to expose, amongst others, possible terrorists inside or 'en route' to US. Although only two out of eight examples relate indirectly to acts of terrorism, Mr. Chertoff argued on the basis of this information that the sharing and analysis of PNR data are both "effective" and a "necessity" and urged the Committee "not to take away this valuable counterterrorism tool away from border law enforcement professionals by limiting or restricting the kind of information sharing and analysis that has already proven effective".<sup>60</sup>

Another country that collects PNRs is the United Kingdom. This is done under Project Semaphore. The program relies on, amongst others, PNR and API data to strengthen UK border control by recording people as they travel in and out of the UK, and improve security.<sup>61</sup> Its Parliamentary Under-secretary of State, Meg Hillier, too argues that PNRs produce results. She noted that "1300 arrests for crimes including murder, rape and assault, the offloading of passengers who would not qualify for entry to the UK, and seizure of many false documents, tobacco, and drugs" occurred.

She continues by pointing out that, "[the project] has covered 38 million passenger movements, issued over 17,000 alerts" and that "the system only flagged a small proportion of travelers (1 in 2200) for further intervention, but of those nearly 1 in 12 were arrested". These results serve to demonstrate "the value of passenger information for bordercontrol and law enforcement purposes and in the protection of the vulnerable" and, as a result, "[the EU] need[s] a permissive framework (...) which sets a basis for collection and sharing of PNR and enables our authorities to use this data to maintain the security and integrity of all our borders". Underscoring her point, Meg Hillier

---

59 See: Annex 1.

60 *Ibid.*

61 Meg Hillier (20 November 2007). Personal letter to EU Home Affairs Commissioner Franco Frattini on 'EU PNR Proposals'. A copy of this letter is attached under Annex 2.

states: “such passenger and crew information is key to a fundamentally more effective, efficient and secure border”.<sup>62</sup> – The Dutch government appears to subscribe to the assumption that PNRs help to secure borders: “these experiences indicate that also a European PNR-system can carry benefits for the fight against terrorism and the maintenance of law and order”.<sup>63</sup>

The second reasoning that is applied in the discussion on whether or not to transfer PNRs is the argument that it is not proven that the collection and transfer of PNRs does not not work for counterterrorism purposes. The argument is that because claims as to PNRs value have not been falsified, their collection and transfer becomes automatically useful. One body who reasons along these lines is the English House of Lords, who issued on June 5, 2007 a report in anticipation of the upcoming EU – US PNR Agreement. The authors of the report provide policymakers with ammunition to convince those who have not taken a position on this issue by concluding that, “having received no evidence to the contrary, we are prepared to accept that PNR data constitute a valuable weapon in the fight against terrorism and serious crime, and that their continued use is both necessary and justified.”<sup>64</sup>

Interesting to note is that this report does not rely on results to arrive at this conclusion, but that it is produced on the basis of written and oral statements averted by invited experts and politicians from across the board. Their statements induced the House Commission to conclude that the evidence against the collection of PNRs wears more thin than the facts in favor of it. It does note that, even after its own inquiry, fundamental questions that pertain to the need and necessity of the transfer of PNR data remain unanswered and particularly laments the absence of “sufficient evidence” to support assumptions as to the value of PNR data.<sup>65</sup> Yet, this caution is not the point that sticks after reading the report, nor was this thought sufficient to alter the dominant finding of the report.

The final argument is not so much an argument in favor of the transfer and collection of PNRs. It is, however, an argument that advocates that the purpose for which PNRs are analyzed is attainable and permissible, but only if the procedure is fixed to a number of restrictions. What is meant here is this: the analysis of PNR records is intended to identify ‘unknown’ security risks.

---

62 *Ibid.*

63 Letter of the State Secretary of Foreign Affairs of The Netherlands (29 January 2008). ‘Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie’. Beoordeling Nieuwe Commissievoorstellen (BNC) advice 22112, no. 608, pp. 6.

64 House of Lords (5 June 2007). ‘The EU/ US Passenger Name Record (PNR) Agreement’. Prepared by the House of Lords’ European Union Committee, 21<sup>st</sup> Report of session 2006-07, pp.12.

65 *Ibid.* pp.12.

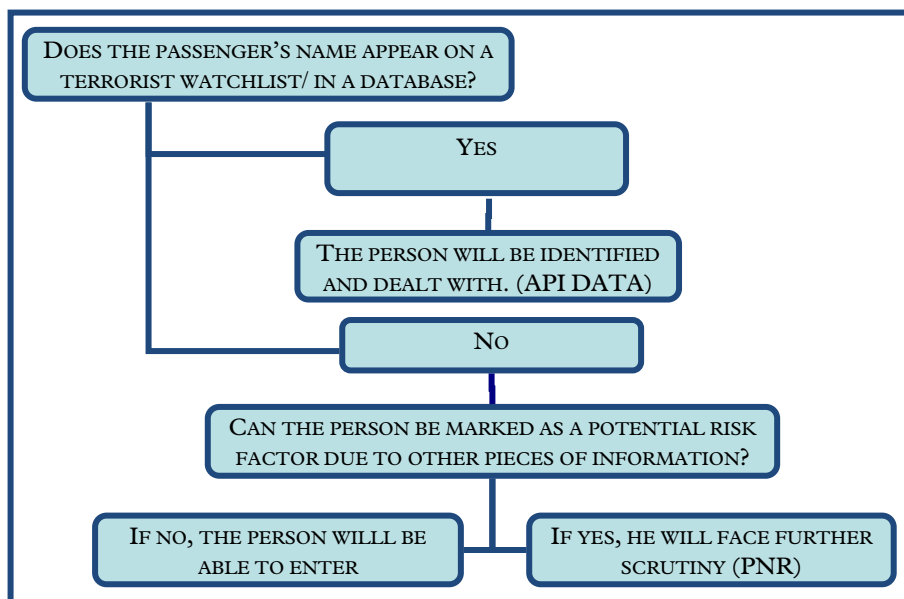
The Commission's Proposal, but also the other agreements mention that, in order to damask unknown security risks, a "risk assessment" should be performed.<sup>66</sup> Yet, the substance of the term 'risk assessment' is multi-interpretable. Whereas chapter 4.4. will focus on the second interpretation, the first way is to understand a risk assessment as the process, in which any given PNR is run against data from already existing criminal records.

Such a procedure may work. Criminal files become the point of reference against which PNRs are held to see whether a positive match can be established between the two. A prerequisite for the successful processing of PNRs would be the establishment of a massive databank with numerous data on terrorist and terrorism, whereby key words from the PNR are run through a search engine against criminal data, similar to a databank with fingerprints. Should there be a match between data contained in a PNR and other data, this does not automatically imply that the individual is a terrorist, but it could be a reason for further questioning. If there is no match, then the individual should be considered 'clean'. The restriction thus lies in the fact that the program, that executes the 'risk assessment', should only match data, not draw conclusions. If the term 'risk assessment' is interpreted in this way, a risk assessment that draws on PNRs may indeed prove to 'work'. At the same time, this procedure can still be subject to a malfunctioning interpretation process.

The procedure would then look as follows: an individual with terrorist intent, but unknown as such, books a flight. His passport is satisfactory, and the information contained in his passport (API data) does not raise eyebrows. The next question is obviously whether the terrorist from our example can be considered a potential threat because the individual can be linked to known terrorists or terrorist groups on the basis of bequeathed addresses, telephone numbers, or matching credit card information. Again, the answer can here be yes or no. Is the answer positive, the individual is identified on the basis of pieces of information that have been gathered in a different criminal investigation that may not directly relate to him, such as credit cards or addresses previously used by terrorists. In that sense, the person is essentially flagged on the basis of information that can only be indirectly attributed to him. In the case that the answer is negative, our terrorist will be able to enter, unless he makes a mistake, unrelated to the screening procedure, elsewhere in the entry-process.

---

66 EU Commission (06 November 2007). 'Proposal for a Council Framework Decision on the Use of Passenger Name Record for Law Enforcement Purposes'. Article 3 (5). COM (2007) 654/F, pp. 13.



**Figure 1:** The Screening Process on the Basis of API and PNR Data.  
Information in brackets indicates the data source on which the individual was signaled.

As can be seen, the procedure, as described above, could be able to identify unknown individuals with a possible terrorist intention, but only in combination with secondary information.<sup>67</sup> This can be considered an important step forward. In the past, a passenger was only screened on the basis of API data, which, if found in order, rendered little reason to undertake action. Now, an extra security layer is built into the system through which suspect individuals can additionally be analyzed and still be flagged, even though this will be on the basis of indirect and sometimes perceptual evidence. In fact, one could argue that, with the use of additional PNR data, law enforcement have doubled the chances of terrorists being apprehend in comparison to the times when PNR data was not available. It is for this reason too that PNRs may be believed to work in order to stave off risks.

---

67 The European Union Committee of the House of Lords concludes that “PNR data, when used in conjunction with other data from other sources, can significantly assist in the identification of terrorists, whether before a planned attack or after such an attack”. See: House of Lords (11 June 2008). ‘The Passenger Name Record (PNR) Framework Decision’, pp. 19.

### 4.3 And Critique on this Viewpoint

Obviously, neither the arguments, nor the reasoning behind the assumption that PNRs work are infallible. A number of issues can and should be critically encountered in order to balance the proposition that PNRs work. As for the first argument – the results from PNRs legitimize the introduction of a continuous transfer and analysis program – the following should be noted: first, bothersome to observe in Mr. Chertoff's comments is the absence of other data that may frame these results. More to the point, the DHS Secretary does not provide the Parliament with a point of reference as to the actual number of arrests, the number of opened criminal investigations on the basis of PNR data, the number of people 'flagged' as a result of peculiar PNRs, nor what data element spurred action. Moreover, it remains unclear within which timeframe the results were accomplished. Were they achieved in the six years following 9/11; since 2004, when the EU – US Agreement took effect; or are they the results over 2006? In other words, it is unclear what the proportion of these eight instances bears to what total and whether sparseness determines their significance.

Also, Mr. Chertoff weakens in the same letter the statement that PNRs - in their own right - are a valuable counterterrorism tool, when he concedes that PNR data are always used in combination with other data: "PNR does not alone [stress by author] tell us who is and who is not a terrorist", but that these data "simply help our officers make a more complete assessment at the border to decide who warrants further scrutiny prior to entry".<sup>68</sup> This is saying in other words that PNR data are never the sole set of information on which law enforcement agents rely. It also means that PNR can possibly complement already existing counterterrorism intelligence, but that they are in themselves not a crucial set of data on which the apprehension of terrorists hinges. And finally, it curbs statements that without the collection of PNR data, potential threats cannot be identified and counterterrorism efforts would be nowhere. Essentially, the information provided only tells us that in a very small number of cases PNR data together with other data may have helped to stop possible criminals with a likewise intent. Of this, by all means, small number of cases, even less relate directly or indirectly to terrorism. While stopping criminals is laudable in every way, such information bears not the characteristics of an 'invaluable tool' to counter terrorism, nor does it prove that PNRs work, particularly not on a stand-alone basis. It does provide us with some insight, however, as to how the Secretary of the Department of Homeland Affairs views efforts to assess passengers on the basis of solely PNRs, i.e., outside a framework that can match PNR data with criminal data, which is interesting for a later discussion.

---

68 *Ibid.* 60.

Ms. Hillier's comments are also worth further examination, particularly when read in conjunction with the Commission's proposal. The Commission namely goes as far as saying that "the UK was able to report (...) gaining valuable intelligence in relation to terrorism in the two years of the operation of its pilot project"<sup>69</sup> Apart from the fact that 'gaining valuable intelligence' is not the same as 'identifying unknown security risks' and that thus the project may be inappropriate as a point of reference to persuade others of the fact that PNRs work, Ms. Hillier subscribes nowhere in her letter to this supposition, i.e., she makes no reference to arrests or criminal investigations that were initiated under the pilot program against terrorists. While the exposed criminal activities fit perfectly within the program's objective to strengthen UK border control, and also resonate the Commission's objective to combat serious crime, the content of the letter fails to support the EU Commission's claim that PNRs work for counterterrorism purposes. Although the absence of a reference to such results in a personal letter is by no way proof that these results were not achieved, it would have made sense for Ms. Hillier to disclose these results. They would have carried significant weight and would support the assumption as to the specific value of PNR data to counter acts of terrorism considerably *if* such results could have been noted. The question remains therefore whether PNRs 'work' for counterterrorism efforts.

As for the logic that PNRs work because it cannot be demonstrated that they do not work, here too caution is required not to accept such a statement on face-value. While the point that PNRs work may be correct, the path towards this assumption is partially flawed and the report's reasoning to arrive at this point is in essence reversed logic. It is flawed, because the assumption appears to be based solely on the opinion of experts, not on factual data. The choice for experts may have been induced by the objective to escape the 'few results – few conclusions' cycle, but the proposition would carry more weight if it had been founded on hard data. Now, the report relies heavily on convictions, invoked by obscure experiences. Moreover, the House of Lords' reasoning is illogic when it concludes that PNR data are useful to combat terrorism as *too little* information was known to warrant such a statement. If a genuine assessment is daunting in the here and now, the House should have refrained from making such sweeping statements back in 2007. After all, much of the essential information for making such an assessment was at the time of publication still unknown – just as it is now –, partly because thorough reviews still had to be undertaken. The House of Lords did not conduct such reviews

---

69 EU Commission (06 November 2007). 'Proposal for a Council Framework Decision on the Use of Passenger Name Record for Law Enforcement Purposes'. COM (2007) 654/F, pp. 2.

and are therefore not in the position to make such claims in the absence of so much crucial information.

Also, reversed logic is applied to arrive at the conclusion that a further use of PNRs is justified and necessary. For practically all countries, 'non transfer' of PNRs is their point of departure; the decision for the transfer of PNRs is the deviation from the rule. In this light, any argument to do so should logically come from the side of proponents of the scheme, as they are the ones who must convince opponents and make clear that PNRs indeed have value. However, the House of Lords' report places this burden upon opponents, effectively claiming through the insertion of the words 'having received no evidence to the contrary...' that the exchange of PNR data is justified and necessary until proven otherwise. In other words: the inability to falsify the supposition makes the preposition correct – a clear null hypothesis that is not constructive to the debate. Sadly, the debate around the transfer of PNR data suffers therefore not only from the absence of unequivocal reports on this matter, but also from the manipulative shuffling of such burdens of proof.

Finally, a substantial part of critique can be put forward to the process of assessing risks on the combination of PNRs and other criminal data. While the screening process may work, there is also the chance that it works too well – possible matches may be overvalued in terms of their significance and importance. What is meant here is this: overzealous intelligence officials may attribute too much value to information in PNRs and disregard other inconclusive evidence. For example, let us consider a third, and potentially highly explosive case. A passenger without terrorist intent submits in his PNR the address of friends he will visit – coincidentally also the address where a known terrorist shelter was housed for a substantial period. Alert intelligence officers may connect these dots, flag this individual and pull him out of the line for further questioning. For whatever reason, they are dissatisfied with his answers and ultimately arrest the individual. It is here that the potentially harmful effects of PNR screening surfaces, as the person is apprehended on misinterpreted information, given the fact that the new owners only have the address and not the objectives in common with the former residents. The danger of such a situation to occur has made law enforcement agencies wary to pull an individual from the queue – and should make us wary to accept the notion that the combination of criminal evidence and PNRs functions on a fail-safe basis.

#### 4.4 Why PNRs Do Not Work...

Opponents of the distribution of PNR data by airline carriers to national competent authorities have two major concerns with regard to PNR data, particularly with respect to the recent Commission Proposal. On the one hand, they question whether a sufficient legal basis exists for the purpose for which PNR data are put to use, i.e., whether the way to come to its objectives is legitimate. Secondly, they raise concern over a number of practical issues that stick to the transfer of PNR data, effectively questioning the correctness of assumptions and possibilities of PNRs.

##### 4.4.1 *Legal Objections*

The legal objections against the transfer of PNRs come from the objective to execute risk assessments. As section 4.2 already indicated, the term 'risk assessment' can be interpreted in two ways, particularly because the Commission's Proposal does not spell out how it itself takes these words. Given the statements by Mr. Chertoff, we should for now assume that the way in which PNRs are used in the US include an effort to match PNRs – and thus individuals – to criminal and terrorist intelligence. This 'matching process' may make everyone suspect, but it is in essence less controversial, as only those data and individuals that indeed match are singled out for further inspection, and only on the basis of a reasonable suspicion.

If, however, this reasonable suspicion is based on a match between PNRs and 'risk indicators'<sup>70</sup>, here understood as specific characteristics commonly attributed to terrorists, than the purpose for which PNRs are collected does become controversial. Such a procedure would namely mean that Passenger Information Units would engage in profiling efforts.

This profiling procedure, as envisaged under objective 2, is explicitly prohibited under Articles 8 of the European Charter of Fundamental Rights

---

70 The proposal identifies four sub-measures for which PNRs could be used. These include the objective "to identify persons who are or may be involved in a terrorist or organised crime event, as well as their associates"; "to create and update risk indicators for the assessment of such persons"; "to provide intelligence on travel patterns and other trends relating to terrorist offences and organized crime"; and "to be used in criminal investigations and prosecutions of terrorist offences and organized crime". As can be noted, measure one indicates against whom the profiling is directed; objective two and three command efforts to 'sharpen the pencil' of intelligence bodies; and measure four makes the additional value of PNR in criminal procedures clear. How the Commission aims to attain these objectives is unclear, however. EU Commission (06 November 2007). 'Proposal for a Council Framework Decision on the Use of Passenger Name Record for Law Enforcement Purposes'. Article 3 (5). COM (2007) 654/F, pp. 14.

(ECFR) and Article 8 of the European Convention on Human Rights (ECHR), which both deal with access to and distribution of personal data. Instead, personal data may only be made available for specified purposes on a legitimate basis laid down by law<sup>71</sup>, something that profiling or 'risk assessments' on the basis of 'risk indicators' will inevitably lack, as profiling is inherently a purpose in itself. Thus, if the objective of conducting a 'risk assessment' is read as an profiling objective, the Commission finds itself confronted with two options: either to remove from the proposal the objective to identify unknown individuals who may be involved in acts of terrorism through acts of profiling and to only carry out screening efforts directed at known terrorists or on a combination of PNRs and criminal data, or to go directly against European law, which would not be a wise choice, as such a decision is likely to be challenged in court.

The aforementioned situation creates a nettlesome conflict. If PNR data are used for profiling procedures, these measures collide with notions cemented in long standing European conventions. But, if PNR data are not used as such, it may lose its entire value within the spectrum of counterterrorism tools and bring us back to the situation we find ourselves currently in. As the Commission has neither specified nor decided how it envisions these risk assessments, it is equally unclear whether the Commission has set its mind on profiling or considers matching a good alternative. In turn, PIU's may find themselves empty-handed if the Commission remains gung-ho about profiling. Amidst this confusion, the European Data Protection Supervisor concludes rightfully, "while the purpose of fighting terrorism and organised crime appears to be clear enough and legitimate, the means used to reach this purpose leave room for discussion."<sup>72</sup>

#### 4.4.2 *Practical Objections*

In addition to legal questions, meaningful limitations that underlie PNR records and analysis procedures can be highlighted. More specifically, the notion of profiling as an effective counterterrorism tool can be contested. Also, the overall value of a PNR record in the light of the data that PNRs generally hold can be questioned. It is for these practical issues that opponents assume that PNRs do not work.

---

71 Charter of Fundamental Rights of the European Union, Article 8.

72 European Data Protection Supervisor (20 December 2007). 'Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes'. See: <[http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20\\_EU\\_PNR\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_EN.pdf)>, last accessed 07/06/2008.

With regard to the first issue, let us assume for now that the purpose for the transfer and analysis of PNRs is indeed to establish and update risk indicators against which individuals can be profiled. An interesting issue would then be to find out, whether profiling has the capability to separate tourists from terrorists. A number of experts have pointed to problems in profiling efforts and that profiling, here understood as an extension of data mining, may not be the invaluable tool it is often perceived as. In support of this critique is a CRS report for the American Congress entitled *Data Mining and Homeland Security: An Overview*, in which Jeffrey Seifert sums up the possible flaws in profiling efforts geared towards the exposure of evildoers.

Broadly defined, there are three main limitations, being [1] the limited value that can be attributed to revealed patterns; [2] the limited value that identified connections reveal about the causal relationship between individuals with a supposed connection; and [3] the limited value that predicative models have in the absence of 'known instances' of particular behavior, or, put differently, the number of incidents are too few and too unique to enable the creation of valid predictive models on which to make risk considerations.<sup>73</sup> In the light of these limitations, a different paper, entitled *Effective Counterterrorism and the Limited Role of Predicative Data Mining*, prepared by the CATO Institute, is led to conclude that "data mining (...) is not well suited to the terrorist discovery problem".<sup>74</sup>

Moreover, opponents see their views strengthened by the report's observation that "it would be unfortunate if data mining for terrorism discovery had currency within national security, law enforcement, and technology circles because pursuing this use of data mining would waste taxpayer dollars, needlessly infringe on privacy and civil liberties, and misdirect the valuable time and energy of the men and women in the national security community".<sup>75</sup>

In the case of PNR data, analysts have the task to correctly 'connect dots' that should be connected. This procedure, however well executed, leaves room for unwanted errors so long as there are too few examples on which risk profiles can be based. For now, the recent Commission proposal therefore explicitly prohibits arrest made *solely* on the basis of processed PNR data<sup>76</sup>, but is

---

73 Seifert, J. (19 July 2007). 'Data Mining and Homeland Security: An Overview'. CRS Report for Congress RL31798, pp. 3.

74 Jones, J. and Harper, J. (11 December 2006). 'Effective Counterterrorism and the Limited Role of Predicative Data Mining'. CATO Institute Policy Analysis No.584, pp. 1-2.

75 *Ibid.* pp. 3

76 EU Commission (06 November 2007). 'Proposal for a Council Framework Decision on the Use of Passenger Name Record for Law Enforcement Purposes'. Article 3 (5), pp. 14. COM (2007) 654/F.

unclear whether this precaution indicates doubt from the side of the Commission that profiling can ever distinguish between harmless and harmful passengers, or that it is done as a precaution so as to avoid arrests based on a system that is neither fail-proof nor judicially approved. The provision should not be read, however, as an enduring ban on profiling – the Commission, if it had wished for intelligence agencies never to apply profiling methods could have made that clear in its proposal, something it chose not to do.

Finally, a practical problem that comes from the profiling objective should not be overlooked: in order to identify a traveler as a potential security risk, benchmarks need to be established that distinguish between the characteristics of a potential terrorist and a tourist. But on what basis are such risk indicators established? Perhaps on the outer characteristics of exposed terrorists? Or will those on seat 17b, which may have surfaced as the optimal terrorist seat, be singled out for further interrogation? And can businessmen, who fly regularly, be exempted from this process? Moreover, even if we were able to establish such ‘short lists’ of specific characteristics of possible terrorists beyond reasonable doubt, such lists are worthless, as it is strictly forbidden to transfer characteristics that may indeed tell something about possible intentions of an individual – primarily religion, and correlated categories, such as food preferences – under the provisions of all agreements. At any rate, if profiling is indeed the overarching objective of this proposal, PNRs may simply not be as effective as when used in correlation with other data, as the accuracy and appropriateness of the benchmarks to separate terrorists from other travelers can be questioned.

In addition to the practical constraints in the process of assessing the risk a particular individual constitutes to national security, there is another practical obstacle: the number of elements PNRs generally hold.

As noted in chapter three, the European Union approved the transfer of PNRs to Canada, the US, and Australia on the precondition that only a predetermined number of data elements would be included in the transferred PNR. In the case of Canada, the number of elements is 25, in the case of the US and Australia – but also in Europe’s own proposal – this number is set at 19. This means in effect that, at best, profilers can consider 25, respectively 19 elements. While these fields together can still hold a vast amount of data, both proponents and opponents concede that, generally speaking, a PNR holds far less data elements. According to Klaas Bruin, Privacy officer at Royal Dutch Airlines, the PNR of an average passenger holds only between 6

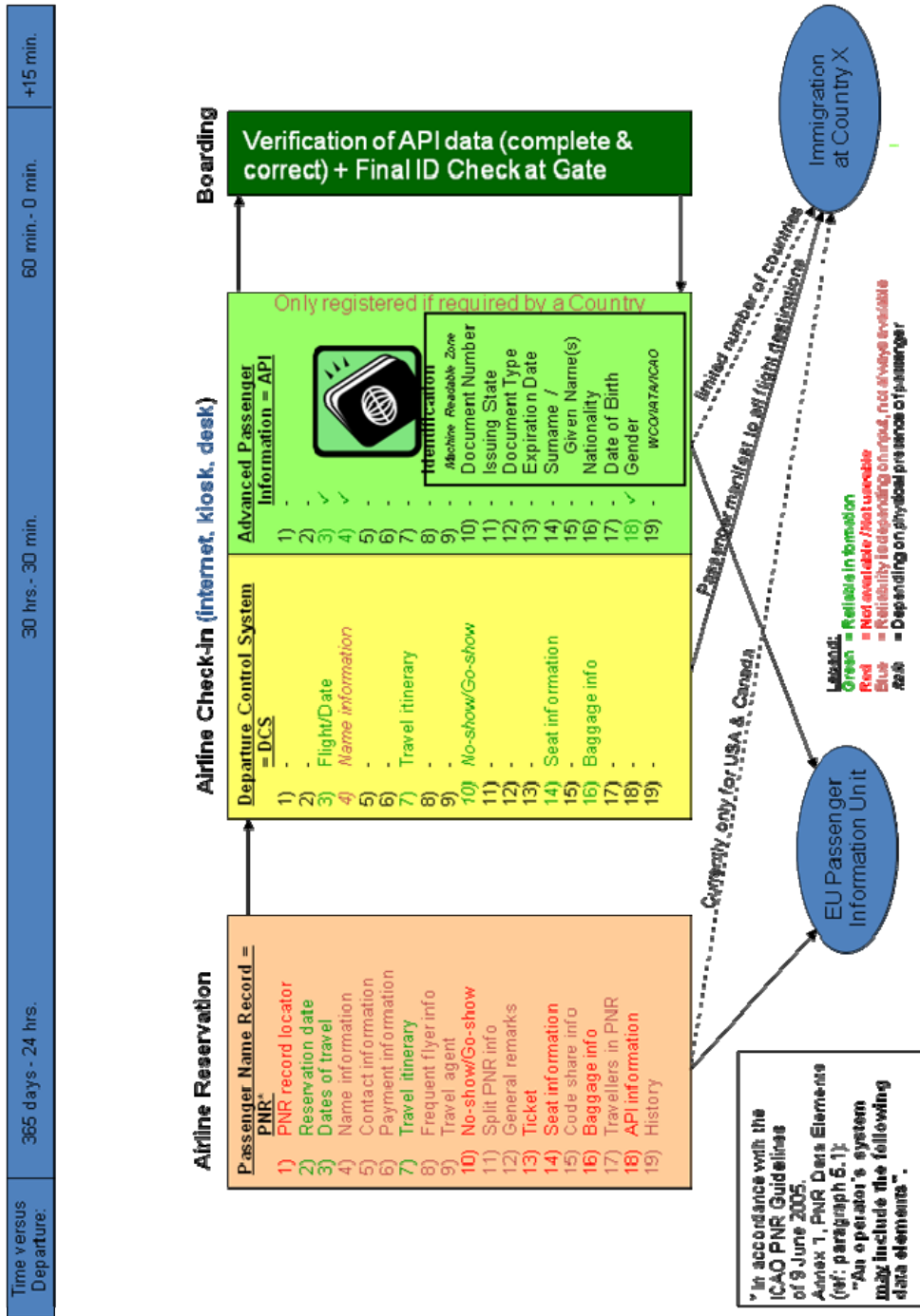
and 10 data fields.<sup>77</sup> Even DHS believes that “(...) it will be rare that an individual PNR will include a full set of the identified data”.<sup>78</sup>

In addition to the fact that few PNRs will hold information in all 19 (or 25) datafields, the content of these data should also be viewed with a critical eye. As figure 2 illustrates, apart from the fact that much data may be missing in a PNR, much information that is available remains ambiguous, even after boarding the aircraft. This is due to the fact that a passenger makes PNRs information available on a voluntary basis, a fact that obligates analysts to remain wary not to accept the content of PNRs on face-value.

---

77 This information was provided to me in a personal interview with Mr. Bruin, conducted on December 7, 2007.

78 DHS (11 May 2004). ‘Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection’, pp. 1.



**Figure 2:** The Reliability of Datasets

In the first column (PNR), all transferrable PNR items are listed. Items in red indicate that this data is either unavailable or unusable at this stage of the process. Items in green are reliable and

available. Items in blue/ purple indicate that the data contained in these fields depends in terms of reliability and availability on the passenger as the passenger can choose to omit such data. The process depicted in column two (DCS) has only the ability the clear information on four items, which were still unclear in column 1. API data, and the procedure to receive such data (column 3) provides only information on three additional data fields. In practice, this means that ambiguity remains, even after boarding over items 6, 8, 9, 11, 12, 15, 17, and 19. In addition, information on field 1 and 13 never becomes available.

If we remember the content of PNRs from chapter three, what is effectively transferred will be meager sets of ostensibly harmless data. Which is certainly ambiguous in nature and pertains in principal to the flight-details. In any event, six fields are unlikely to hold essential qualitative information from which the estimate can be derived that a particular individual is a potential terrorist – either in combination with other data or outside of such references. Yet, if this fact applies to the PNRs of most passengers, is it not logical to question precisely how the transfer of PNRs is an invaluable tool to counter terrorism? Indeed, up to June 19, 2008 no person was apprehended on the basis of PNR data alone.<sup>79</sup> Undeniably, this information questions whether PNRs are indeed the essential tool they are portrayed as, and casts doubt on the assumption that any PNR is useful, irrespective of its content. More generally, the above issues speak to the advantage of opponents, who argue that the net amount of data, together with its stated objectives, do not justify the introduction of such profound measures with ostensibly limited results. This is not to say that PNRs cannot be useful to monitor the movements of a particular individual or that, even in combination with other passenger data, PNRs are worthless. It does mean, however, that assumptions as to the net difference that PNRs can make for the purpose of countering terrorism should be toned down, as a generic PNR will hold little information on which a suspicion can be based.

#### **4.5 ...And Critique on this Viewpoint**

Neither the arguments of proponents of the supposition that PNRs work, nor those of opponents are conclusive. More importantly, counterarguments do not carry more weight in the final equation, even though there may be a tendency to focus on downsides more than on advantages.

As to the legal issue raised, there needs to be clarity as to what the ‘risk assessment’ specifically entails. If it is understood as the effort to analyze the PNR information of all passengers, irrespective of their country of origin, religion, or other characteristics and to hold them against existing terrorist info, then the objective for which PNRs are made available may not present a

---

<sup>79</sup> According to Mr. Klaas Bruin, up to 19 June 2008, it was within the Airline industry not known if arrests have ever been made anywhere on the basis of PNR data alone.

legal obstacle to the introduction of the PNR scheme. To be sure, a permissible procedure still depends on who has access to the information, how the data matching takes place, and how the data is stored. However, if done in an appropriate manner, it can be argued that such a comparison is done to stop terrorists and other felons – an objective for which such associations need not to be unlawful. This is, however, also the furthest that this counterargument runs. If the accumulated data is used to create risk indicators, and to profile PNRs against such parameters, there is indeed a severe risk that the objective to profile will be incompatible with European privacy legislation. Collecting and disseminating data to intercept criminal activities is not forbidden; collecting and disseminating data to establish ‘peril pointers’ on the basis of which malicious individuals may be exposed is, as the objective deviates from permitted objectives under articles 8 of the ECFR and the ECHR.

Secondly, and related, is the point of how profiling can contribute to counterterrorism efforts. While there may undoubtedly exist circumstances where profiling produced the results it was intended to produce, this paper is critical whether such can also be the case for counterterrorism and questions whether this point can be countered. Indeed, if profiling, and more specifically the creation and updating of ‘risk indicators’ constitutes the main purpose of the entire proposal, than is questionable whether PNRs can indeed expose those unknown security risks. This holds particularly true in light of the few results that would facilitate such a process. It is hard to imagine how from the insight deducted from the few successful arrests intelligence bodies should subtract a shortlist of characteristics that may enable an ‘a priori’ assessment.

As to the number of data an average PNR holds, this is certainly an important point, but it should also not be overestimated. It appears that PNRs gain meaning and have a role if used in conjunction with other data, not on a stand-alone basis. If the limitations of PNRs are excepted and intelligence officials do not try to overstretch the assumptions that can be derived from PNRs, then PNRs can possibly complement other data to attain an as complete as possible picture of the individual. This requires in turn from policymakers prudence in their depiction of PNRs: do not project PNRs as a panacea, but as a beneficial tool for counterterrorism efforts. Similarly, work towards the matching of data, not the profiling on risk indicators.

In sum, the arguments of opponents can be countered, but only to a certain extent. If the limitations that come with PNRs are recognized and respected, than PNRs can have a place among the counterterrorism arsenal. However, if the limitations of PNRs are ignored or overstepped, or if politicians willfully continue to present the possibilities of PNRs in such sweeping terms, than it cannot be, but that PNRs are an inappropriate tool to profile and establish

risk indicators. If used as such, the envisaged collection and analysis of PNRs will neither deliver the goods, nor will effectively ‘work’.

#### **4.6 Conclusion**

This chapter mapped the arguments from both proponents and opponents of the exchange of PNR data. First, the three tenets that are believed to back assumptions as to PNRs perceived usefulness were discussed, after which the main points of critique, both from a practical and a judicial standpoint were incorporated. Following, opposing views and critical comments that can be brought forward in response to assumptions from both sides were discussed. These arguments, the correlating critique, and an estimate as to which argument supersedes the other, are laid down in Table 4.

Arguments in favor or against the analysis of PNRs for counterterrorism efforts				
#	Objective for which PNR are used	Argument against (CON)	Argument in favor (PRO)	Strongest argument
1	Matching/ Profiling	If the objective for which PNRs are transferred is understood as part of a <b>profiling</b> effort, the objective is <b>neither attainable nor permissible</b> .	When PNRs are transferred to <b>match</b> such data with other criminal records, the purpose <b>may be attainable and permissible</b> .	-
2	Profiling	<b>Profiling</b> is strictly <b>prohibited</b> under articles 8 of ECFR and ECHR.	-	CON
3	Profiling	<b>Profiling</b> on the basis of risk indicators derived from PNRs is an <b>ineffective tool</b> to unmask terrorists.	-	CON
4	Matching/ profiling	An PNR record analyzed <b>in isolation</b> will hold <b>too little information</b> on which a risk assessment can be based.	PNRs may not be processed in isolation, but <b>in combination</b> . The match between PNR and other data makes <b>PNRs valuable</b> .	If processed in isolation: CON. Otherwise: -
5		Results can neither be framed, nor related directly to terrorism.	PNRs have delivered 14 results.	CON
6		Claims of PNRs value cannot be considered reliable.	Claims as to PNRs value cannot be falsified.	-

**Table 4:** For or against PNRs?

What can be read from the table above is that much of the opinion as to whether PNRs work and whether such a collection is appropriate depends on the purpose for which PNRs are collected. Indeed, 4 out of the 6 arguments deal in one way or the other with the distinction between ‘matching’ or ‘profiling’. Apart then from providing clarity on demonstrable results, clarity should also be given on the means to come to such results. If the process to assess risks is done on the basis of matching, this process may, in all its limitations, indeed be effective, valuable and appropriate.

However, if the process to identify risks is considered a profiling process, than different conclusions must be drawn. If understood in this way, the notion namely surfaces that the gathered information – not evidence – points to the fact that the arguments of opponents as to the need and necessity to transfer PNRs for the purpose of counterterrorism carry more weight than those of proponents. It is simply true that the objective to use PNRs for profiling efforts – ‘establishing risk indicators’ - is currently too far-fetched and legally questionable. Moreover, generic PNRs may hold relatively few data on which a match can be established, but it holds even less information from which risk indicators can be derived, or against which established such indicators can be run.

As for the two points unrelated to the matching/ profiling debate: claiming the discussion’s high ground on the basis of a null hypothesis is not a sign of strength. Moreover, 14 results fail to convince, particularly if the incredible number of passengers underway to the UK and America every day is considered. Also, the number of incidents that have occurred thus far is too limited to conclude, with any certainty, the rightfulness of either side regarding need and necessity, as a substantial lack of hard data further obscures the debate. While PNRs may function as an extra check to stop felons at the border, the conclusion of this chapter is that the necessity to collect PNRs in Europe on such a large scale is unclear as PNRs may contribute little to counterterrorism efforts. Moreover, in view of the indicated limitations, it is questionable whether PNRs are indeed needed as a means to counter terrorism or that other, less controversial procedures also suffice. In any event, the information above signifies that the wording of the provisions in the Proposal demands additional clarification, and the elaboration on why PNRs are useful require further substantiation. Until then, neither need nor necessity are convincingly demonstrated.

## 5. CONCLUSIONS, FINDINGS AND RECOMMENDATIONS

---

### 5.1 General Conclusions

Six years after the events on 9/11, terrorism still has a hold on our society, both in terms of a perceived fear that another attack is likely and imminent, and in terms of the manifold security measures with which we are confronted in everyday life. While many have come to accept the notion that our society has fundamentally changed and a 'heightened state of surveillance' has become an integral part of our everyday lives, the debate about the appropriateness of certain measures has not been settled. This paper examined one issue from the wider constellation of counterterrorism measures that deal with personal data specifically: the need and necessity to transfer PNR data for counterterrorism purposes.

As to 'PNRs in practice' this paper found the following:

PNRs may consist of up to 30 data elements of the passenger. However, neither the type of data, nor the amount of data is in itself sufficient to de-mask terrorists – this should always be done in conjunction with other data available. To this date, no passenger was arrested, nor identified for further inspection on PNR data alone.

The number of data fields to be submitted under the EU – Canada/ US/ Australia agreements and under the proposal varies. To Canadian authorities, European airlines must submit only the information of up to a maximum of 25 fields, and to American and Australian authorities information on maximal

19 fields. To European PIUs, airlines must also submit the information contained in 19 data fields. In addition, the content of the agreements varies substantially, whereby the provisions under the Canada agreement should be considered less harmful or intrusive.

By introducing its own proposal and by molding it to the agreement with the US, the European Commission indicates not only that its slant in this matter mimics America's, not Canada's approach to counter airlines-terrorism, but that it also aims to gather, if not rely on information contained in a very questionable data field. This is particularly remarkable as the merits of the provisions under the American agreement over those contained in the agreement with Canada have not yet been demonstrated.

In addition, this paper encountered during the research stage:

A serious lack of politicians to substantiate opinions on this issue. Many have supposedly become convinced of the need and necessity to collect or transfer PNRs and it appears that experiences made in the US have significantly contributed to the formation of this notion. The exact content, however, of such convincing experiences remain unclear, even when their disclosure is insisted upon.

A worrying gap between the perceived value of the PNR rule and the actual merits that remain after a thorough analysis. Agencies and policymakers involved in the analysis of PNRs should be able to convey exactly how PNRs are useful and complimentary to other approaches so that the value of PNRs can be represented in a truthful manner. Important point of departure is the Commission's objective in this respect: the collection and transfer of PNRs is done to expose terrorists, not to scare them out of flying. This means that, although a deterring effect of this measure is by all means laudable, it is at the same time not the direct objective. When discussing the merits of the collection of transfer of PNRs, focus should lie on assessable results, not on possibly achieved side-effects.

Those advocating the introduction of a PNR system oftentimes portray the possibilities of PNRs wrongfully. PNRs can produce results, but only in correlation with other data. This is not a problem if proponents acknowledge this and stop presenting PNRs as an invaluable tool and to start portraying it as a complementary tool.

Bearing the critical comments above in mind, this paper found the following as to the merits and detriments of the collection and transfer of PNRs:

By expanding the data against which individuals can be screened, countries doing so have been able to insert an additional layer to their security ring. In this sense, PNR data appears to be beneficial, but first and foremost when

used in conjunction with API- or criminal data. However, it is unclear whether this security layer functions as such, or is merely a symbolic measure. This indistinctness comes predominantly from the manifold ways in which the term 'risk assessment' can be interpreted.

However, if we are to understand the 'risk assessment' as a profiling effort, independent of further criminal data, PNRs may have limited value. Moreover, profiling is, if not on the basis of a clear suspicion, strictly forbidden under European conventions. Unless a solution is found to elucidate this problem, provisions within the Proposal will go against EU cornerstone Human Rights Agreements. This point says little about effectiveness, but all the more about an important drawback if the system is introduced as envisioned.

Leaving this interpretation-debate aside, there is a total number of 14 cases, which possibly result from the transfer of PNR data. However, until this date, these results raise more questions than that they are able to answer. For one, information as to the scope and scale of the number of individuals profiled is absent, while it too remains unclear of what misdemeanor the accused were suspected to commit. Also, it remains unclear how many 'known and unknown' terrorists have been apprehended thus far. Important is, however, that these 14 cases were achieved by matching PNR data to other criminal records.

## **5.2 Need and Necessity**

While the threat of terrorism invites the undertaking of new measures and oftentimes requires the introduction of additional measures, it is impossible to conclude that there exists a need to transfer PNR data records for the purpose of fighting terrorism. On a practical level, other data sets, predominantly API data are able to keep harmful people of flights. By contrast, PNR data are unreliable, particular for profiling efforts, and is in almost all cases too limited in information to genuinely expose people 'who may be involved' in acts of terrorism. A practical downside is too that PNRs in some instances becomes available only upon the immediate moment of embarkation, which leaves virtually no time to run the individual against either criminal data or risk indicators. Last-minute passengers will therefore still be admitted to board the aircraft, even if in hindsight their PNR was a cause for alarm. Furthermore, there appears to exist no pressing necessity to transfer PNR data for counterterrorism efforts on the basis of the results known thus far. The list of results up to this point is by all means meager. All together, 14 incidents have been reported where PNR data appear to have played a crucial role in preventing criminal misdemeanors. If the number of visitors to the US and the UK is considered, and it is remembered that not even all these cases relate

to terrorism, the merits of such a regulation to counter terrorism are questionable. Unless there is a classified report with all results received thus far, one is inclined to conclude that there exists neither a need nor a necessity to transfer of PNR data for its stated purpose.

At the same time, it is equally impossible to conclude beyond any reasonable doubt that there exists no need or necessity to transfer, make available and use PNRs to combat terrorism, as the screening procedure in which PNRs are applied is still undefined. Another reason for this position is that the value cannot be falsified because time and again, reference is made to results that were conveyed in private meetings, but that were not made public. While there may be pervasive arguments to do so, such actions seriously handicap a genuine debate; and the Commission appears to indeed avoid such a debate altogether, as the comment by Mr. Frattini on page 6 all too aptly indicates.

Nonetheless, the Commission should be straightforward about what it finds more important – to build understanding for the introduction of the regulation or to let law enforcement agents build cases against individuals, apprehended on, among other PNR data, without ever explaining why it proceeds the way it proceeds in that particular instance. If it chooses the former, it should give up its monopoly on information that holds arguments for the introduction of such a scheme and explains the relevance of PNRs. If it opts for the latter, it should too refrain from making claims that can neither be proven nor falsified, particularly not if this should be done on the basis of evaluations it chooses not to share with the wider public. In any event, it should wonder whether its opinion as to the value of PNRs is accurate and whether it should present PNRs as the be-all and end-all to fight transnational terrorism.

### **5.3 Suggestions for Improving our Understanding on PNRs**

Having witnessed the difficulties that arise from a lack of trustworthy reports on the merits of the transfer of PNR data, this paper suggests to critically assess the end results and functioning of the 2004 EU – US PNR Agreement. Also, it suggests the planning of a revision of the 2005 EU – Canada Agreement. In order to avoid a biased report, these review could be performed by independent researchers with enhanced security clearances. The reviewers should focus on the proportionality of the data submitted and the experiences with the sharing and dissemination of data, in order to provide both an objective assessment and to come to ‘best practices’ in this field. Given the fact that the quest for PNR data is likely to intensify, not diminish, such knowledge would be of invaluable value for the design of future agreements.

By the same token, this paper calls upon the European Commission and national policymakers to come forward with specific details as to results and experiences thus far of the collection of PNR data that served to convince the Commission on this issue. Preferably, such information is as detailed as possible, but, out of respect for law enforcement efforts, it needs not to go into specifics – a mere indication of the number of arrests or identifications would already make a difference. Such information would help tremendously in building a balanced opinion.

Also, the Commission should elaborate on how it interprets ‘risk assessments’ and how it believes these assessments should be made. One option to do this is to compose a PNR task-force to dispel uncertainty on this and related issues. Although the Commission may have opted intentionally for such ambiguity to exploit PNRs to the fullest, this is truly a critical point. After all, much of the anticipated results from this rule depend on whether PNRs from ‘unknown security risks’ are to be linked to other criminal data, or whether the passenger pops up because his characteristics mirror those oftentimes attributed to terrorists. This paper is of the opinion that the ‘profiling’ approach to PNR data may produce significantly less results, and all the more judicial headaches.

Furthermore, irrespective of the PNR rule’s substance, were the regulation to be introduced, and were first results to be noted, it would be wise to assess these results critically. In particular, it would be interesting to see how the number of ‘flagged’ individuals relates to the total number of people processed, how many criminal charges were finally filed, and how the number of arrests in Spain relates to, for instance, The Netherlands to identify possible discrepancies in screening methods, etc.

In short, it would be wise to continue to monitor and to publicize the merits of the transfer of PNR data, possibly through ‘sunset clauses’. These are fixed dates after which a particular measure is evaluated. Currently, too much is unknown to dismiss the proposal. Conversely, it may also be that PNRs are overvalued as to their benefits. But the absence of information on results conversely demands a critical approach to the proposal and to PNRs for the purpose of combating terrorism as a whole. Rightfully or wrongfully so, for now, PNR data are first and foremost known for its controversy, not for its merits.

#### **5.4 Implications for The Netherlands**

Obviously, the one-million-dollar question is ‘where does the European Union go from here?’ Specifically, with regard to The Netherlands, a valid question is whether the Dutch government should side with proponents or

opponents of such a scheme. And should it support the efforts to come to a European-wide collection of PNR data? The initial signs indicate that the Dutch government indeed supports the transfer of PNR data for the purpose of combating terrorism in the absence of pervasive counter arguments. Similarly, while this report has indicated important practical obstacles in effectively putting PNR data to work, it too has not found truly all-encompassing arguments against the introduction of such a scheme, if introduced as a matching effort between PNR data and other information. If a European PNR rule must be established, this paper advocates the rule to consist of a combination of PNRs with other criminal data. However, this does not mean by default that the transfer and collection of PNR has acquired its place among the counter terrorism arsenal. We need additional evidence to support or falsify this assumption.

Therefore, for The Netherlands, a suggestion could be to construct a pilot program with a temporary PIU to see how the scheme fares and to get acquainted with the program's merits and detriments through first-hand experience. By formulating expected results beforehand, it would set realistic benchmarks on which success can be gauged. The next step would be to communicate preliminary results in an open way, and to discontinue the program if the results fail to meet the expectations, or when the costs appear to outweigh the benefits. At the same time, the government could see whether the current data retention period is appropriate, and evaluate whether less or more agencies should have access to PNR data. By doing the above, the government will acquire through first-hand experience the ability to show accrued results and to convince inherent opponents, and it also retains the option to bring the program to a close without the loss of face in the event of disappointing results. Such an approach is not fail-proof. It does leave room, however, for the Dutch government to claim that it moved carefully on this issue. Even if PNRs indeed have little value, the government can convincingly argue that it moved cautiously while at the same time adhering to its fundamental responsibility to provide for the safety of its citizens.

## ANNEX 1

---

**Letter to the European Parliament By DHS' Secretary Michael Chertoff**



*Secretary*  
**U.S. Department of Homeland Security**  
Washington, DC 20528

## **Homeland Security**

May 14, 2007

Dear Member of the European Parliament:

Thank you for the opportunity to appear today before the Committee on Civil Liberties, Justice, and Home Affairs to further our important dialogue on matters critical to the security of the European Union and the United States.

We face a shared challenge in preventing acts of terrorism against our countries and our citizens. At the same time, we share a fundamental and unwavering commitment to protect the civil liberties and privacy that are the hallmarks of all free and democratic nations.

Recent terrorist attacks in Algeria and Morocco, as well as earlier attacks in Madrid and London, the foiled plot this past August against transatlantic aircraft bound for the United States, and the recent convictions of five British terrorists, underscore the serious nature of the threat we face and the importance of developing common tools and approaches to counter this global menace.

One of these tools is Passenger Name Record (PNR) data, which is a limited set of information provided by air passengers traveling between Europe and the United States. PNR data, used in combination with passenger manifest data, allows U.S. officers to check passenger names and other basic information against lists of known or suspected terrorists and criminals so that we can enhance screening of dangerous people and prevent them from boarding commercial aircraft.

Combined with other intelligence, we use PNR data to check for links that might reveal unknown terrorist connections, such as a traveler who has provided contact information overlapping with a known terrorist. It is our ability to identify these hidden links that has made PNR so valuable to our counterterrorism efforts and the reason it is imperative we reach a new understanding regarding how this information will continue to be shared and protected.

Below are several examples of how analyzing PNR data has prevented dangerous individuals from entering the United States.

- In June 2003, using PNR data and other analytics, one of our inspectors at Chicago's O'Hare airport pulled aside an individual for secondary inspection and questioning. When the secondary officers were not satisfied with his answers they took his fingerprints and denied him entry to the United States. The next time we saw those fingerprints - or at least parts of them - they were on the steering wheel of a suicide vehicle that blew up and killed 132 people in Iraq.
- In January 2003, Customs and Border Protection (CBP) officers in Miami used PNR to disrupt an internal conspiracy within an airline that was smuggling cocaine between Venezuela and Miami. A corrupt ticket counter agent would identify low-risk travelers (typically families) and add an additional bag to their reservation after they

departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami plotted to remove the added bags from circulation prior to inspection by CBP in Miami.

- On March 11, 2005, CBP arrested two individuals for smuggling drugs from London to Chicago. Their PNR information revealed the use of a common credit card. This credit card's reservation history identified a third traveler who had used the same card and listed a second credit card. Analysis of this new credit card number identified three additional travelers. Three of the four new travelers were arrested during subsequent travel for drug smuggling.
- In January 2006, CBP officers used PNR data to identify a passenger posing a high risk for document fraud. The passenger, posing as a citizen of Singapore, was scheduled to depart Korea for the United States. The subject's travel itinerary was targeted by a query using data from recent cases of document fraud in Sri Lanka. CBP officers contacted airline representatives in Korea and requested assistance in verifying the traveler's documents. With airline assistance, CBP determined the subject's travel document was a counterfeit Singapore passport. The subject was in possession of his Sri Lankan passport. The subject was also a positive match to the Transportation Security Administration's No Fly List and suspected of being an armed and dangerous terrorist. The subject was denied boarding for the flight. He was subsequently stopped on another date using the same method of PNR targeting. In the second incident, he attempted to travel to the U.S. using a counterfeit UK passport.
- In February 2006, CBP officers used PNR data to identify a passenger with a high-risk for narcotics possession arriving from the Dominican Republic. The subject, a returning U.S. legal permanent resident, purchased his ticket using cash and made certain changes to his reservation. Upon arrival, the subject was selected for an enforcement exam. During an examination of the subject's personal effects, CBP officers discovered two packages containing heroin. The subject was placed under arrest and turned over to Immigration and Customs Enforcement for prosecution.
- At Boston Logan Airport in April 2006, CBP officers used PNR data to identify two passengers whose travel patterns exhibited high-risk indicators. During the secondary interview process, one subject stated that he was traveling to the United States on business for a group that is suspected of having financial ties to Al Qaeda. The examination of the subject's baggage revealed images of armed men, one of which was labeled "Mujahadin." Both passengers were refused admission.

- In May 2006, PNR analysis identified a high-risk traveler arriving at Atlanta Hartsfield airport from Europe. CBP officers determined that the individual's visa was issued one week prior to September 11, 2001, yet he had never traveled to the United States. The subject's passport listed him as a "flight instructor" and his reasons for traveling to the United States included the plan to "see a man in New York for two days." The individual was ultimately linked to numerous individuals who U.S. law enforcement regards as security risks and immigration violators. The passenger was denied admission.
- In May 2006, CBP officers used PNR data to target a high-risk passenger arriving from Amsterdam. Officers linked the subject to a split PNR; the second traveler was a Palestinian who previously claimed political asylum. The high-risk passenger was also identified through a known telephone number used by terrorist suspects contained within his PNR.
- Upon arrival the subject applied for admission as a Jordanian citizen and was referred to secondary inspection for further examination. The subject revealed that his purpose of travel was to visit a relative for thirty days. During the secondary inspection, the subject revealed that he had been arrested and convicted on terrorist related charges in a third country. The subject also admitted to being a former member of an organization that espoused political views and supported violent acts that include suicide bombings. The Joint Terrorism Task Force and Immigration and Customs Enforcement were contacted and responded to interview the subject. Upon completion of the interview the subject claimed credible fear of returning to Jordan. He later recanted and was expeditiously removed from the United States.

If such a system had been fully developed before 9/11, we might have been spared that tragedy. Consider this: two hijackers, Nawaq Alhamzi and Khalid Al-Midhar, appeared on a watchlist and would have been "flagged" when they purchased their tickets. Through analysis of their PNR data, we could have learned that three other hijackers - including Mohammed Atta - used the same address as Alhamzi and Al-Midhar; five other hijackers used the same telephone number as Atta; and still one other used the same frequent-flyer number. The analysis of PNR and other basic data that we use today would have flagged all nineteen hijackers as connected to Alhamzi and Al-Midhar. If we surrender this tool, we will abandon the real-time defenses that can save our citizens' lives.

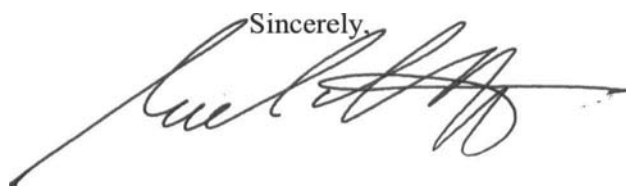
These concrete examples illustrate the necessity of analyzing and sharing PNR data. But it is also important to note the strong privacy protections in place to safeguard this information. PNR data is protected under the U.S.

Privacy Act and the Freedom of Information Act, among other laws, as well as the robust oversight provided through the U.S. Congress, American courts, and internal controls such as the Department of Homeland Security's Privacy Office, Inspector General, and Government Accountability Office. In addition, our policies ensure that records pertaining to foreign nationals are properly protected.

PNR data is also used in strict accordance with U.S. law. Our officers make determinations based on relevant criteria developed from investigative and intelligence work. PNR data does not alone tell us who is and who is not a terrorist. It simply helps our officers make a more complete and informed assessment at the border to decide who warrants further scrutiny prior to entry. And PNR data is not used to create a "risk score" that remains with an individual or automatically adds a person to a terrorist watch list.

One of the central lessons of the 9/11 attacks, and subsequent attacks in Europe and elsewhere, is that we must break down barriers to information sharing. That same lesson must extend to our use of PNR data. We must not take this valuable counterterrorism tool away from border law enforcement professionals by limiting or restricting the kind of information sharing and analysis that has already proven effective.

I appreciate the time you have given me today to address the Committee, and I look forward to working with you as we seek new ways to strengthen international cooperation in our fight against terrorism while protecting the fundamental rights and liberties we all cherish.

Sincerely,  


Michael Chertoff



## ANNEX 2

---

**Personal Letter to Mr. Franco Frattini by Ms. Meg Hillier**



**Home Office**

**Meg Hillier MP PARLIAMENTARY  
UNDERSECRETARY OF STATE**

2 Marsham Street,  
London SW1P 4DF

[www.homeoffice.gov.uk](http://www.homeoffice.gov.uk)

**Vice President Franco Frattini European Commission  
B-1049 Brussels**

20 NOV 2007

### **EU PNR PROPOSALS**

We welcome the Commission's proposal for an EU PNR system and I look forward to discussing it with you in the future. This is a key opportunity to share data in the fight against criminality targeting our borders. We need a

permissive framework at the EU level which sets a basis for collection and sharing of PNR and enables our authorities to use this data to maintain the security and integrity of all of our borders.

Such passenger and crew information is key to a fundamentally more effective, efficient and secure border. Stronger cooperation in the EU will increase the effectiveness of our domestic programme and provide wider benefits for us all, while ensuring that we strike an appropriate balance between the right to security and other fundamental values, including the right to privacy.

There were over 200 million passenger movements across the UK border in 2006 and these are rising rapidly. The EU as a whole is faced with similar increases in international travel which brings us great economic and social benefits. However, mass migration also poses challenges of illegal immigration and cross border crime and terrorism.

In the UK, we have run a pilot project, Project Semaphore, for three years to assess the value of using both API and PNR data. This has had many significant successes and demonstrated the value of passenger information for border control and law enforcement purposes and in the protection of the vulnerable. This includes over 1300 arrests for crimes including murder, rape and assault, the offloading of passengers who would not qualify for entry to the UK and seizure of many false documents, tobacco, and drugs.

Since the project started, it has covered 38 million passenger movements, and issued over 17,000 alerts. As you can see from these figures, the system only flagged a very small proportion of travellers (1 in 2200) for further intervention, but of those nearly 1 in 12 were arrested. This shows the extent to which using this data safeguards and enhances the rights of legitimate travellers who do not need to be subject to detailed scrutiny, while detecting successfully the small proportion of travellers breaking the law. PNR also allows the detection of crime that would not have been found using other data sets.

Some examples include:

- Chinese non-documented arrivals. On the basis of PNR data we have offloaded a number of passengers who were subsequently arrested all with forged documentation.
- A two week Semaphore trial on outbound passengers on a ferry route to France identified three suspected facilitators, two tobacco smugglers, one convicted sex offender and one individual under investigation by Kent police. Two forged documents were also identified.
- A passenger was matched by HMRC against one of their drugs courier profiles using essential PNR elements. An alert was sent to the Airline

Liaison Officer who intervened at embarkation. His reasons for travelling to the United Kingdom lacked credibility and he was referred to the local police who on searching his baggage discovered 25kgs of marijuana.

- Location of a murder suspect overseas by linking him to an associate's PNR record.
- Offloading of passengers attempting to smuggle (swallowed) drugs to the UK through **PNR** profiling.
- Identification of a significant number of facilitators and those using falsified documents through **PNR** profiling alerts.

We have of course run this pilot project in conformity with UK and EU data protection rules, and with involvement of our Information Commissioner.

Following the success of Semaphore, the UK intends to continue to implement our new borders system. We have this week signed the contract with a technology supplier to deliver the UK's e-Borders system. This will enable the routine acquisition and analysis of both API and PNR data, using our Joint Border operations centre. I would be more than happy to accommodate you or your officials if you wanted to see this technology first hand. I intend to send further examples of the successful use of **PNR** data, showing in more detail exactly why the **PNR** element in particular was crucial, in the coming months.

I'm copying this letter to Members of the JHA Council and to members of the LIBE Committee of the European Parliament.

**MEG HILLIER**



## ABOUT THE AUTHOR

---

**Frank Kuipers (MA)** is research assistant at the Security and Conflict Programme of the Netherlands Institute of International Relations 'Clingendael'. He focuses on the nexus between counterterrorism efforts and data analysis.