“The Effectiveness of the Exchange of Passenger Name Records (PNR) in Europe”

Dissertation submitted to obtain the academic degree of Master of European Criminology and Criminal Justice Systems
by (00905707) Wim Geluykens

Academic year 2009-2010

Promoter:
Prof. dr. Gert Vermeulen

Commissioners:
Prof. dr. Patrick Hebberecht
Prof. dr. Paul Ponsaers
Foreword

In order to write about the effectiveness of the exchange of Passenger Name Records in Europe, a lot of importance needs to be given to the practice. It is for that reason that a big part of my dissertation is based on interviews and contacts I had with practitioners.

My sincerest gratitude therefore goes out to everyone who has helped me with their answers to my questions and with their advice. More specifically the following people should be mentioned. Tony Verachtert, head of the federal judicial police at Brussels Airport, for his cooperation both with the interview and by giving advice concerning documentation. Monique Lebersorg, Director Passenger & Cargo Charter Services for TNT Airways, for making time to talk to me about how they deal with passenger data. Danny Rits, Security Manager for JetairFly, for taking the time to respond to my questions. Member of the European Parliament Sophie in't Veld and her Policy Advisor Sophie Bots, for their kind and helpful advice. Jacquelyn Aron Bednarz and Hylko Oosterloo of the U.S. Missions to the European Union, for the useful documents they have sent me.

Despite the fact that it eventually wasn’t possible to conduct interviews with people of the police at the airports in the Netherlands and the UK, I would nevertheless like to thank those that tried to make it work.

Furthermore I would like to thank my promoter Prof. dr. Gert Vermeulen for his suggestions on how to handle this topic.
Abstract

The ever-growing globalization our world is the subject of doesn't only have positive effects. As a consequence we have seen a rise in terrorism and organized crime over the last decades. In this dissertation we investigate whether the exchange of PNR data as we see it in Europe is an effective way of countering both of these forms of crime. We do this by comparing PNR with API and by talking about the proposal for a Council Framework Decision on the use of PNR for law enforcement purposes. We then take a look at how PNR is used in practice on the basis of interviews that were conducted with practitioners. There we see that the exchange of PNR indeed is effective, especially when it is used for profiling and when it is integrated into a nodal-oriented type of policing. The privacy issues that are linked to the exchange of PNR are also addressed and special attention is given to the agreements between the EU and the USA on the transfer of PNR. We conclude that the exchange of PNR is effective but that crucial amendments have to be made to the EU PNR system as it is proposed. Both privacy- and organisational aspects need to be changed in order to realise the full potential of PNR for law enforcement purposes in a way that also respects the rights of the passenger.
# Index

1. Introduction p. 5

2. What are PNR? p. 6
   a. Difference with API p. 8
   b. The EU’s PNR initiatives p. 11

3. PNR in practice and the potential of profiling p. 16
   a. Practice p. 16
   b. Profiling and nodal-oriented policing p. 19

4. Privacy and the issue of the EU-USA PNR transfers p. 24
   b. The proposal for a PNR Council Framework Decision’s privacy aspects p. 26
   c. Council of Europe and privacy p. 27
   d. Council Framework Decision of 27 November 2008 on the protection of personal data p. 28
   e. Criticism towards the proposed exchange of PNR and privacy p. 29
   f. The EU-USA PNR agreements p. 33
   g. The future and what we can learn from all of this p. 38

5. Recommendation p. 41

6. Conclusion p. 43

Annex: List of PNR data p. 45

Bibliography p. 47
1. **Introduction**

From the beginning of the previous century until now, our world has been the subject of an ever-growing globalization. The speed of communication, the ease of travel and the rapid movement of capital have meant a shrinking of space and a shortening of time. These evolutions underlie the transformation of our world into a global village. This has great advantages for all of us. We are able to get in contact with people living thousands of miles away within a second and we can follow important events as they occur on the other side of the world. But of course, there are also downsides to such a transformation.¹

For if travel becomes easier, not only bona fide people will make use of this possibility, but also people with far less good intentions will. Therefore we see a rise in transnational crime. Drug trafficking, terrorism and all sorts of organized crime have been facilitated by these bigger societal evolutions. One of the most painful confrontations with this drawback of globalization are the 9/11-attacks. These showed that globalization is definitely not a solely happy story and that there is a dying need for effective measures that counter some of the possibilities globalization creates.²

And indeed, after the attacks a lot of counterterrorism measures were taken. Not all of them were effective though. Some were implemented a bit too hasty in a sphere of revenge and have proven not too be useful and/or detrimental to human rights. Also concerning organized crime many initiatives have been taken. However not all of them have shown to be equally effective and organized crime still is ever-present in our society. What we will investigate in this dissertation is whether the exchange of PNR data as we see it in Europe is an effective way of countering not only terrorism, but also organized crime.

We will start by giving an explanation of what PNR data actually are. We will talk a bit about the differences with Advanced Passenger Information (API) and how the future of PNR will look like according to the EU. Then we will discuss the use of PNR in Europe and its effectiveness as it is already being used. This part will mostly be based

---

² Ibid., 102-106.
on interviews with people from the police force at the airport and with people from the air carriers. After this, attention will be given to the privacy aspect of the exchange of PNR data. In this part, we will also discuss the agreements between the EU and the USA on the exchange of PNR. Then we will make a recommendation on what the PNR system in the EU should or could look like, taking into account what we have discussed before. We will end the dissertation with a conclusion wherein the key findings will be highlighted.

Like this we will have succeeded in using a double threefold structure that tries to cover every main aspect of the issue. We will not only talk about how it is, how it will be and how it should be, but by making use of the interviews we will also try to see things from the position of the police and the air carriers. The passenger’s viewpoint is represented by the part on privacy. Hence we will discuss every main actor involved in the exchange of PNR.

2. What are PNR?

Passenger Name Records are the data that are kept in the automated reservation and departure control systems of air carriers. These Passenger Name Records hold information about the itinerary of a client plus information about the client himself. Which data exactly these records hold can be the subject of discussion, which we will see further on, but there are some basic things whereon consensus exists. These are identification data such as a name, first name, date of birth and telephone number. The date of reservation, the travel agent if there is one and financial data like credit card number, expiry data and invoice address are also included. Further elements are the itinerary, the flight and seat number and frequent flyer information.\(^3\)

Every time someone makes a reservation, a Passenger Name Record is created. Even if that person eventually doesn’t show up for the flight, doesn’t pay or if he cancels the reservation, his PNR is still kept. Every adaptation that is made to a

reservation is also traceable in the PNR. Each entry into a PNR is registered in the PNR’s history with the date, the place and the time. The user ID and any other information of the airline staff, travel agent or automated system that made the entry is also logged. Even the name of the person who requested the change, who doesn’t necessarily need to be the traveller himself, is stored. Like this we get an enormous amount of information for every reservation.4

Therefore air carriers usually don’t store all this data themselves. Rather it is stored in Computerized Reservation Systems (CRS), which are also known as Global Distribution Systems (GDS). Worldwide there are three major CRS companies. Amadeus deals with the data of airlines such as Air France, KLM, Iberia, American Airlines and Qantas. Another big player in this market is Sabre, which delivers services to over 300 air carriers. The last one of the big three is Galileo. This system has a lot of experience in dealing with PNR and is still used by a lot of European airlines.5

The fact that there are so many different systems means that the various actors in the process of the reservation need to work together closely. When you, for example, book a trip on an airline that uses Amadeus through a travel agent (who also work with PNR) that uses Galileo, there has to be some kind of communication between the two of them. What will happen is that the travel agent will create a PNR in Galileo after which this CRS will send a message to Amadeus through a bilaterally agreed upon standard of communication such as AIRIMP. Amadeus will then create a PNR for the airline based upon the portions of the travel agency’s PNR that it has received. The same goes for when you book a trip that includes taking planes of two different airlines that make use of different systems. If then later changes are made to one of the

---

flights, these changes will not always be communicated to the other system. Therefore we see that there can be different PNR with different data for one single reservation.6

When combining the data of the different systems, you get information on everyone who has ever made a reservation regardless of the fact whether they eventually went on the trip or not. Add to this that due to the massive amount of information, PNR can show you things like who travelled when, whereto, with whom, for how long and who paid for the ticket and it becomes pretty clear that PNR can be a quite important research tool for law enforcement authorities.7

a. **Difference with API**

As it is shown above, Passenger Name Records were initially created to help airlines in exchanging flight information. Herein it shares the same goal with Advanced Passenger Information (API). However it is important to clearly distinguish the two concepts from each other.

First of all are API's a lot more limited in their extent. They include identification details from the passport and basic flight information. Therefore it consists of the name and first name, date of birth, sex, nationality, passport number, country where the passport was issued and country were the passport-holder is living plus flight details.8

By sending this information to the customs service of the country of destination, the airlines can be of help to said services. These can namely start checking the information they receive against their databases while the flight is still in the air. Like this they are better prepared to start their actions upon the landing of the plane.9

In theory this technique holds quite some benefits. First of all it has a positive effect for the traveller. Because of the fact that the information is already sent to the services at

---


7 Ibid.


the airport of arrival, the formalities at that very airport will be far less lengthy for the passenger who isn’t targeted. For the carrier it has the positive effect of reducing its chances of being fined because the people it carries don’t have the proper documentation on them. Because of the obligation to transfer said data, the carriers need these documents hence obligating the passenger to bring them in order to be allowed on the plane. Furthermore the use of electronic communications in this field allows the handling of a bigger amount of passengers thus meaning more revenue for both air carriers and airports.\textsuperscript{10}

On the other hand some downsides can be spotted as well. First there is a need for solid databases against which the received information can be checked. If none such databases exist yet, initial efforts can be costly. For the air carriers too some costs are implied. They need to have the right systems up and running in order to communicate with the services at the airport of arrival and they will have to spend a bit more time and effort on checking-in in order to get the information and send it out.\textsuperscript{11}

Because of the fact that API only consists of the basic set of information on a passenger it is easy to check it against a set of databases in a fast manner. This makes it suitable for basic border controls and also gives it a role in the fight against illegal immigration and human trafficking. It is in this respect that the Spanish saw the need for an obligation on carriers to communicate passenger data in 2003. In its initial initiative the data that had to be transferred by the air carriers to the authorities responsible for carrying out border checks in the country of arrival were the number of the passport or of any other travel document that was used, the nationality, the first name and family name and the date and place of birth. This information was not only needed for all people the carriers were preparing to convey, but also for third country nationals that were carried into a Member State by them but that had not returned to their country of origin or hadn’t continued their journey to a third country on the date that was stipulated on the travel ticket. Providing severe sanctions for the air carriers that didn’t comply with the obligations placed on them, the Spanish initiative for a

\textsuperscript{11} Ibid., 9-10.
directive was especially tough for those very carriers, even more than for the Member States.\textsuperscript{12}

The European Parliament had strong doubts about the whole initiative and formulated quite some criticism. The Committee on Regional Policy, Transport and Tourism mostly flayed the initiative for its one-way obligations on the air carriers. If the Member States require such information, recompense should be given to the carriers. The Committee was also of the opinion that it is not the air carrier’s job to monitor and transmit whether someone has or has not taken his flight home or to a third country. Rather this is seen as a job for the police and border control authorities. Over the months following up to the Spanish initiative, the document was heavily adapted and despite ongoing criticism from the European Parliament that was definitely not in favour of the draft documents, the directive was adopted in April of 2004.\textsuperscript{13}

The eventual directive entitled “Council Directive on the obligation of carriers to communicate passenger data” omitted the stipulations about the third country nationals who didn’t return to their country of origin or didn’t continue their journey. The resulting obligation for the air carriers was to communicate a basic set of data elements (the same as the ones cited above as API, hence explaining that the directive is also referred to as the API-directive) of the passengers they are carrying to an authorized border crossing point through which these persons will enter the territory of a Member State, by the end of check-in to (and at the request of) the authorities responsible for carrying out checks on persons at external borders. These authorities have to delete the data within 24 hours after transmission unless they still need it afterwards to execute their functions. The data can also be used by the Member States for law enforcement purposes. Furthermore it should be noted that

\textsuperscript{12} Council of the European Union, Initiative of the Kingdom of Spain with a view to adopting a Council Directive on the obligation of carriers to communicate passenger data, 7161/03 FRONT 22 COMIX 139.

sanctions for non-complying air carriers were kept rather strict.\textsuperscript{14} The directive also stated that the Member States had to comply with it by 5 September 2006 at the latest. This however wasn’t the case. When we look at Belgium for example, we see that there is a Royal Decree of 18 December 2006 that concerns the implementation of the directive in Belgian law. There however never was any real executing decision that stated the concrete obligation for an air carrier to provide the API to the border control authorities. In other Member States as well, the execution of this directive didn’t go the way the European Union had envisioned it.\textsuperscript{15}

The practical impact of this directive can therefore be seen as rather minimal.

\textbf{b. The EU’s PNR initiatives}

The EU however has not been standing still in the field of exchanging passenger data. Already during the negotiations about the API-directive it came with a global EU approach for the transfer of air passenger name record data in the form of a communication from the Commission to the Council and the Parliament. This document came about in an atmosphere of heightened awareness of the possible benefits of exchanging passenger data. In the wake of the 9/11-attacks the USA wanted to make more use of the Passenger Name Records of air carriers for law enforcement purposes. Therefore it needed to negotiate an agreement with the EU in order to be in line with the data protection requirements for the data they receive from European air carriers. Later, countries such as Canada and Australia also asked access to this PNR data. Because of this, the EU found that the time was there to bring forward an approach that should be the basis of a multilateral solution for the issue of improving aviation and border security and fighting terrorism and international organized crime through the exchange of PNR.\textsuperscript{16}

The main elements of this approach are a legal framework for the PNR transfers from

\textsuperscript{15} KB 11 December 2006 betreffende de verplichting voor luchtvervoerders om passagiersgegevens door te geven, BS 22 December 2006.
the EU to the USA, accurate information for the passengers about PNR, replacing the pull method with the push method, developing an EU position on the use of PNR and creating a multilateral framework for PNR data transfer. Both the transfers to the USA (including the informing of the passengers) and the distinction between the pull- and push method will be discussed later on in this dissertation. For now let’s go deeper into the other aspects of this global approach. The multilateral framework the EU talks about is to be seen within the structure of the International Civil Aviation Organization (ICAO). For this reason, the Commission sent out a paper to the ICAO to discuss this framework. In this paper the EU makes clear that the data elements to be transferred should be kept to a minimum. Therefore it would be not in line with the principle of proportion for the public authorities of a state to request elements that don’t appear on the individual PNR. As a consequence, airlines shouldn’t go out to retrieve these “missing” elements. Furthermore the EU prefers that sensitive data such as information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life is not shared with the public authorities. The EU also set forward some guiding principles in this paper. These principles include transparency, purpose limitation, limited storage periods, respect for the rights of the passenger and redress mechanisms.\(^\text{17}\)

So it is within this context that the EU started with the preparations for its own regulation concerning the use of PNR. In November of 2007 the Commission then came with a first proposal for a Council Framework Decision on the use of PNR for law enforcement purposes. Unlike with the API-directive, where the information was exchanged to improve border controls and to combat illegal immigration and human trafficking, the goal of the PNR-proposal was to prevent and combat terrorist offences and organized crime. The scope of this proposal was limited to international flights. These are defined as “flights scheduled to enter the territory of at least one Member State of the European Union originating in a third country or to depart from the territory of at least one Member State of the European Union with a final destination in a third country”. In the most recent draft, it is also explicitly stated that this includes transit or

transfer flights.\(^{18}\)

The system proposed is one where every Member State has a Passenger Information Unit (PIU). This is a Unit that is responsible for the collection of PNR data from the air carriers or intermediaries for said international flights.\(^{19}\) In this proposal the PIU is also given the task of analyzing the data and carrying out risk assessments of the passengers so they know who requires further examination. In doing so it may check the PNR data against various national or international databases and risk criteria. These risk criteria are to be created in compliance with national law and taking into account the recommendations for common general criteria which will be made after the entry into force of the Framework Decision. In any case these criteria may not be based on any sensitive data elements like the ones we have referred to already. The Units will then, after the analysis and assessment, send the information regarding the passengers who are seen as a risk, to the so-called “competent authorities”, for every Member State has to make a list of authorities that are allowed to receive PNR data. These can only be authorities that are responsible for the combating of terrorism and the fighting of serious (initially only organized) crime.\(^{20}\)

Up until the last proposal for a Council Framework Decision the system of the PIU is still the same. The general scope however has been changed from preventing and combating terrorist offences and organized crime towards preventing, detecting, investigating and prosecuting terrorist offences or serious crime. This was done because merely terrorism and organized crime were seen as being too narrow. Therefore serious crime is defined by referring to article 2 of the Council Framework Decision on the European Arrest Warrant and the surrender procedures between

---


\(^{19}\) It should be clarified that there is a possibility for the air carriers to choose an intermediary through which they will make the PNR data available to the PIU instead of doing it directly themselves. When we hereafter refer to the air carriers transferring their data to the PIU please bear in mind that can also mean that there is an intermediary who does it on behalf of the air carrier.

\(^{20}\) COM (2007) 654 final; Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/2/09 CRIMORG 7 AVIATION 3 DATAPROTECT 2.
Member States and its list of 32 offences and to article 2 of the Council Framework Decision on the fight against organized crime. For the definition of terrorist offences reference is made to the offences in article 1 to 4 in the Council Framework Decision on combating terrorism. The Member States however wanted to go even further and thus chose for an intermediate option, meaning that the purpose limitation (terrorism and serious crime) only applies for the risk indicators against which the PNR data are checked. In case the use of this data reveals other offences, then the data can also be used for the investigation and prosecution of those other offences without being bound by the scope of the PNR Framework Decision in general.\(^\text{21}\)

It is up to the Member States to take the necessary measures to get the air carriers to share their PNR data for the international flights that land in and depart from their territory. The last draft of the proposal foresees a time schedule to come to the complete collection of the data. During the first three years after the implementation of the Framework Decision the Member States have to get PNR data for at least 30% of those international flights. During the next three years this percentage has to be minimum 60 in order to come to a situation wherein the Member States get the data for all of the flights after a period of six years. Furthermore it should be noted that Member States have to put in place a set of sanctions for air carriers that do not comply with the obligations that are imposed upon them by national law adopted in the execution of the Framework Decision (for instance not sending the required data or

doing so but not in the desired format).\textsuperscript{22}

The timing of the transfer of the PNR data from the air carriers to the PIU is twofold. The first transfer will take place 48 hours before the scheduled time for flight departure. The second transfer follows immediately after flight closure i.e. after the passengers have boarded the aircraft and it is no longer allowed for other passengers to get on the plane. In specific and urgent cases, deviations from this time schedule can be made so that the PIU has the information earlier than 48 hours before the scheduled time for flight departure or somewhere between the moment of the first and the second transfer.\textsuperscript{23}

All the carriers have to make use of the push method after an initial period of two years after the implementation of the Framework Decision wherein carriers who don’t have the technical possibilities to apply the push method have to make use of the pull method. The difference between the two is that the push method implies that the air carriers transfer the information to the PIU. By making use of computer-based filter systems in combination with the push method, it becomes possible to only send the data that is required without transferring superfluous data, thus not (further) “damaging” the privacy of the passenger then needed. Using the pull method on the other hand means that the PIU is allowed to take the data itself from the air carrier’s database. Giving preference to the push method therefore seems understandable. However this implies quite some costs for the carriers in order to adapt their systems to this way of working. Consequently thorough checks of whether the air carriers comply with this obligation after two years are recommended.\textsuperscript{24}

When it comes to data retention, the Framework Decision foresees a system wherein the data is kept in the database of the PIU for three years. After these initial three, the PNR data can be archived at the PIU for a period no longer than seven years. In this

\textsuperscript{22} Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/2/09 CRIMORG 7 AVIATION 3 DATAPROTECT 2.
\textsuperscript{23} The Member States however can also allow the air carriers to let the first transfer take place somewhere between 48 and 24 hours before the scheduled time of departure. The second transfer can be limited to updates of the first and its timing can be forwarded to half an hour before flight closure; \textit{Ibid.}
\textsuperscript{24} \textit{Ibid.}; COM (2003) 826 final.
period, wherein the data is kept in a “sleeping” database, it can still be accessed, processed and used, but only by specific members of the PIU who have been formally granted such access in their functional description. The latest proposal describes that this access is allowed, “only in response to a specific and actual threat or risk or a specific investigation or prosecution or for analytical purposes related to the prevention, detection, investigation and prosecution of terrorist offences or serious crime”. This however doesn’t really seem to be a limit to the access. Moreover it just comes down to the same purposes as to why the PNR data is exchanged in the first place. In any way, the maximum total retention period of the data thus is ten years. After this period the data has to be deleted from every PIU database.25

3. PNR in practice and the potential of profiling

This chapter will focus on how Passenger Name Records are already used in practice. It is mostly based upon interviews with Tony Verachtert, head of the federal judicial police at Brussels Airport, Monique Lebersorg, Director Passenger & Cargo Charter Services for TNT Airways and Danny Rits, Security Manager for JetairFly.

a. Practice

The interviews showed, like we said before, that PNR is used a lot more than API. In Belgium for example there isn’t even any implementing legislation on API.

PNR on the other hand is used a lot. The federal judicial police at Brussels Airport for instance uses it for almost 25 years now. First, they used it under the approval of the Federal Public Prosecution Service and now they do so after getting the authorization of the magistrates in Brussels in the context of the pro-active criminal investigations. This PNR data is mostly used in the fight against terrorism and organized crime, with a focus on human smuggling and human trafficking.

Not only do they get data for the international flights as they are defined in the

---

25 Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/2/09 CRIMORG 7 AVIATION 3 DATAPROTECT 2.
proposal for the Framework Decision, they also get Passenger Name Records for intra-EU flights. The issue of whether or not to include intra-EU flights in the proposal for a Framework Decision was decided in favour of the latter. The Commission thought that it would be disproportionate at this stage to include such flights in the scope of the Framework Decision. This opinion was seconded by the ECTAA, which is the group of European Travel Agents’ and Tour Operators’ Associations. The Member States have however been given the option to include intra-EU flights in their national PNR systems. In this light, there is a stipulation in the last draft of the proposal for a Framework Decision to let the cost-benefit impact of the inclusion of said flights in the scope of the Framework Decision be analyzed by the Commission. This analysis will then mostly draw upon the experiences of the Member States that have chosen to include those flights within their own system. It seems rather strange and inefficient not to include flights within the EU. Since the scope of the proposal when it comes to modes of transport is limited to air carriers, you have a lot of transportation options that are left uncovered. If then you decide to limit your geographical scope to international flights, it becomes quite easy for criminals to dodge the application of the Framework Decision and to move around in the EU relatively unknown. They just have to make sure to enter the EU by car, boat or train or so and then they could take the plane to go to the country where they need to be to unfold their criminal plans.  

For the moment the police at Brussels Airport receives the PNR data through agreements that are made with the air carriers. Although, not all air carriers are willing to enter into such an agreement. German and UK carriers for example are rather reluctant to do so and will mostly redirect the police forces to the respectively German and UK authorities, which often is the start of a very lengthy procedure. The way to get the PNR data directly from the air carriers in situations like these is to make use of a sort of court order that obligates the carrier to disclose the data. This is something that will change in a positive way once the Framework Decision has entered into force, for then there will be an obligation for all carriers to share this data. The need for this

26 SEC (2007) 1422; Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, 12360/08 CRIMORG 124 AVIATION 162 DATAPROTECT 55; Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/2/09 CRIMORG 7 AVIATION 3 DATAPROTECT 2.
compulsion also showed in the interview I had with Monique Lebersorg of TNT Airways. They, as an air carrier that mostly operates charter flights, only have the names of the passengers and nothing more. What they do is sending the Passenger Name Lists (PNL) to the outstations (located at the airport of destination). This is done by the handling agents who have the best view on who checked in and who didn’t. Since the sharing of passenger data isn’t mandatory (yet), they do not share their information with police services. The only situation wherein this does happen is when they get a specific request through a court order like we said before. Since they themselves do not have anything more then the passenger names, it is the tour operator who buys the seats in the plane who has all the passenger data. These tour operators however also do not share their data with the police. Like this you have a series of flights for which there is no PNR data with the police services, apart from the occasional situation where there is a court order. The same situation can be seen with JetairFly who also don’t have any agreements with police services for the systematic exchange of PNR data. What they do get is that customs, police services or the Belgian State Security Service asks them for data on specific passengers. Most of the times this concerns flights from Brussels to a non-EU country or the other way around, while there has hardly been any such inquiry related to intra-EU flights. So what we see is that these airlines aren’t really confronted with the issue of PNR and that they mostly see it as something for international flights from and to the USA.

The Belgian police forces however already get the data from other airlines. This happens continuously from the moment there is a reservation list until flight closure. This is quite important since otherwise you run the risk of working with old and thus false information. Let’s for instance say you only get information every 12 hours and in the data from the first transfer you’ve spotted someone you are looking for. Now if this person has cancelled his flight an hour after the first transfer, you will only notice this 11 hours later. By this time, there’s a big chance that that person has already taken another flight and thus is on the move or maybe even already has arrived somewhere else without you knowing so. Like this it is clear to see that only being fed with information sporadically can really have big consequences for entire investigations and thus also for police operations. The question now is of course whether the two
transfer-system as described in the proposal for the Framework Decision will be effective enough. Of course it still leaves room for the Member States to choose to obligate the carriers to share data more frequently, but it might have been better to make this option the norm.

b. **Profiling and nodal-oriented policing**

The Belgian police at the airport does not use the data in an automated way. Instead of just automatically running the data against various databases, they analyze the date through profiling. This is a very important aspect since it is exactly here where the potential of the exchange of PNR lies. This kind of profiling can be defined as a specialized technique of the authorities, a specific kind of operational analysis, that, with respect for human rights, makes use of objective criteria to compare specific ‘aviation data’ with the information of the authorities in an intelligent and effective way so the authorities can execute their legal responsibilities, including the prevention and detection of crime and the apprehension and prosecution of the perpetrators. It is needless to say that PNR data play a crucial role in the act of profiling. These data elements allow to check for certain risk criteria. The presence of these criteria might imply that the passenger in question is involved in any form of organized crime or terrorism. These are criteria such as: paid his ticket with cash money, bought the ticket less than 24 hours prior to departure, the ticket was paid by someone else, etc.\(^\text{27}\)

What is important to point out here is that profiling in itself is not really to be labelled as a police technique since it isn’t recognized as such by law. There is no specific legal framework on it, so it shouldn’t be seen as being on the same level as for instance observations, infiltrations and telephone tapping. In fact it somehow originated and further evolved out of practice in the 80’s. This was a time wherein we saw various terrorist attacks on planes (the Lockerbie bombing, Air India Flight 182, …), which has led police to gradually monitor the passengers of flights more and more

---

until it became the true example of intelligence led policing that it is nowadays.  

In order to do the profiling in a proper way, you need people that are specialized in this and that know how to work with the software wherein the data is generated. Like we said before you have different systems such as Amadeus and Galileo. Bearing in mind that for instance airlines that are part of the Star Alliance work with different systems than the airlines that are part of the SkyTeam alliance, you need people with a workable knowledge of all those different systems. Good thing here is that we see that the EU is setting the goal of making them all use the same interface so it also becomes a bit easier for the police forces who are working in this field.

What these people do is they look for certain things. They don’t really make use of watch lists, but what can happen is that after a while, they create a sort of manual watch list built out of the experience of profiling. The most effective way to do this profiling is by looking at multiple reservation lists and comparing and analyzing them. By doing this and checking against the criteria like the ones we cited above, you can make a sort of risk assessment of the passengers and you get to see certain patterns. These patterns also give you a view on potential criminal organizations. An example might help to clarify this way of working. When a criminal organization has 200 kg of cocaine and they want to transport this they have two options. Either they move it all at once, which would mean that they are sure that it will go undetected. This option might suggest that they have someone on the inside. The other, and most probable, option is that they split the 200 kg up because they know that police will never be able to catch everything. What they will do is split the 200 kg into 200 packages of one kg, so they will need 200 flights to transport the whole load. They will make use of couriers that will be going via different flights and different Member States, since the criminal organization obviously wants to spread the risk. However there won’t be 200 different couriers. Instead it will be 20 different couriers doing those 200 flights. What police then does is check the reservation lists and look for the criteria. If they find something, they will compare it with other reservation lists and by thorough criminal analysis of said data they will have a bigger chance of getting a view of at least a

---

portion of the criminal organization. This will then help them to start their actions upon arrival of the assumed couriers.

Another thing that might help in catching these guys and their drugs is a nodal orientation. This means that police focuses on certain points or places where there is a lot of traffic in a sense that these places will be checked more thoroughly. It are these nodes, such as for instance airports, that play a large role in our society and thus also offer great opportunities for criminals. Pointing back at our example, it is rather easy to indicate that a nodal orientation can be helpful. If you know that you need three people to catch one guy and that those three people equal 12 working hours, you see that it becomes vital to intervene as soon as possible before you need more people. Therefore it is much easier for the police to try to grab hold of the 200 kg of cocaine when it still is 200 packages of 1 kg that all pass through the airport before they become 200 000 packages of 1 gram that are spread all over the country. Even more so when you are situated at certain criminal hubs.29

A criminal hub is defined by Europol as “a conceptual entity that is generated by a combination of factors such as proximity to major destination markets, geographic location, infrastructure, types of OC groups and migration processes concerning key criminals or OC groups in general”. In Europe there are five criminal hubs: the North West hub (which is equal to Belgium and the Netherlands), the North East hub (consisting of the Baltic countries), the South East hub (close to the Black Sea), the Southern hub (equal to Italy) and the South West hub (which is the Iberian Peninsula). Now, sticking to our cocaine example, what happens is this. Cocaine is produced in countries such as Columbia, Peru and Bolivia. From these countries, the cocaine is moved to other countries like Venezuela, Costa Rica and Panama. This is done in an attempt to circumvent the extra strict controls and checks at airports and seaports for things that come out of the cocaine producing countries. So from these “secondary” states the goods are moved to places in West and North Africa and Turkey. From these locations the drugs are then brought into the EU and more specifically to the five

criminal hubs. Lastly, from these hubs, the drugs spread out over the whole EU. The North West hub is one of the main ones in Europe. The market at this hub is mostly defined by organized crime groups from Belgium, the Netherlands, Ireland and the UK. Lately we also see more and more West and North African and Eastern European organized crime groups doing business in this hub. Because of the tough competition some groups have also taken the effort of getting in direct contact with the suppliers so they can skip the level of both the secondary and tertiary distribution and get an advantage in comparison with the other groups. However, it is not only for cocaine that this hub is important, cannabis products are also brought in from Spain and Morocco by Moroccan organized crime groups. The rise of local cannabis plantations also plays a role as a catalyst for crime. Chinese or Vietnamese illegal immigrants and Bulgarian victims of human trafficking often have to pay for their transportation by working in and taking care of those plantations. The proximity of the UK obviously also is a big pull factor for illegal immigration and human trafficking. 

Like this we get a hub where there is a variety of drug crimes, human trafficking and illegal immigration. It is here that a nodal orientation of police work including the use of PNR data can help. Transnational cooperation is something that is of big importance in this matter. If the criminals are able to work together regardless of borders, then why shouldn’t police forces be able to do the same thing? Moreover, with the internationalization of crime, this cooperation becomes a necessity for effective crime fighting. The minimum of this cooperation should be the sharing of information seeing as how the pro-active collection of movements within the nodes and hubs becomes crucial. By doing this, the police can get a view of the broader patterns of criminal organizations, so not only of their air travel routes, but also of their movements outside of the airports. In this view, the PNR data are integrated into the bigger whole of nodal-oriented policing. 

In practice, for an airport, it could look like this. As a result of profiling, which is based

---

on the PNR data that police receives, a person can be labelled as potentially dangerous or, more in general, involved in criminal activities. What police for the moment still cannot do that easily in this situation is refuse someone to board a plane. In a lot of cases, it can also just be more interesting to let the passenger board in order to keep him unaware of the fact that you are keeping an eye on him. Taking this into account, they can do an extra check of his luggage and they can watch him closely as his plane arrives and as he leaves the airport by making use of CCTV. Furthermore they can also track him down by making use of the signal of his cellphone and maybe even monitor his conversations and e-mails since both the telephone number and e-mail address are part of the list of 18 PNR data elements (see annex). After getting enough of incriminating material by making use of classic police techniques and when the time is right, the police can then do an intervention which might dismantle an entire criminal organization, or at least an important part of it.\footnote{V. BEKKERS, A. VAN SLUIS and P. SIEP, o.c., 38-39.}

Besides the potential the use of PNR and profiling have in a nodal-oriented type of policing, it also has other advantages. For instance, practice has proven that police forces don’t need sensitive data when they are profiling based on the PNR data. Like this it can also be a safeguard against racial profiling. What the policemen do is they look for the criteria that might indicate that someone is potentially dangerous in a criminal sense. The name of someone is not a criterion, on the contrary it is the result of the analysis. It is only in last instance that the profilers get the name, after they have labelled someone as a potential threat, so they can take further action. If we compare the use of PNR with other, more classical police techniques like observation we see that the former scores better in this aspect. When people go out on the street and they are visually confronted with someone, they will be more inclined to, be it unconsciously, stigmatize. On the other hand, when they only face some facts and characteristics of a person, of which name and race are not a part, it becomes a lot more difficult, if not impossible, to do so.

PNR data is thus mostly used pro-actively. However it can also be used reactively.
When for instance you have the situation wherein someone is suspected of murder and he claims that he was abroad at the time of the event, the PNR can confirm or contradict this. Then again, most of the times, after the police has done its profiling work and its subsequent actions, the data lives on in the working files and reports that are kept in the context of a criminal investigation.

Over the years, the exchange of PNR, contrary to that of API, has proven to be very effective for the police at Brussels Airport. In a lot of cases this has meant a breakthrough and it has assisted police forces in offering a basis to build further police work on. These were all cases involving either organized crime, terrorism or other serious crime. Police forces in Switzerland and the UK make sort of the same use of PNR like they do in Belgium. Other countries such as the Netherlands and France however are still not really adept at it. The new Framework Decision on the use of PNR for law enforcement purposes might play a big role in helping all the Member States of the European Union to see and make full use of the potential of the exchange of PNR.33

4. Privacy and the issue of the EU-USA PNR transfers

In this part we will talk about the privacy aspects of the exchange of PNR in Europe. Extra attention will also be given to the EU-USA PNR agreements as an example of the difficulty of finding the right balance between privacy and security.

a. Directive 95/46/EC

The first document that is of importance in this aspect is the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Directive however is mostly of importance for the air carriers and the commercial processing they undertake of the data. This is so because art. 3,2 of the Directive clearly states that the Directive doesn’t apply to processing operations

concerning public security and the activities of the State in areas of criminal law. Keeping in mind that the PNR are to be exchanged under the future Council Framework Decision in order to prevent, detect, investigate and prosecute terrorist offences or serious crime it becomes clear that the Directive wasn’t meant to apply to this Council Framework Decision. This is also why the latest draft of the proposal clearly states that in case the Member States decide to install a system for the collection of PNR for other purposes than those stipulated in the proposal, the Directive of ’95 will apply, without making any further reference to it regarding the proposal itself. Consequently it does apply to the transfer of API, which, like we discussed already, focuses on illegal migration and human trafficking, matters that are not regarded as concerning public security.\footnote{Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.95, 31-39; Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/2/09 CRIMORG 7 AVIATION 3 DATAPROTECT 2; Council directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004, 24.}

The Directive itself consists of general principles such as that Member States have to make sure that personal data is processed fairly and lawfully and that it is collected only for specified, explicit and legitimate purposes. Furthermore it states that sensitive data cannot be processed, followed by a list of exceptions of which consent of the data subject is one. In the specific case of PNR (and API) the purchase of an airline ticket holds with it the permission for the air carrier to process the personal data that has been given to him in the course of the purchase.\footnote{Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.95, 40-41.}

We will come back to this Directive and more specifically to art. 3,2 when we discuss the agreements between the EU and the USA on the transfers of PNR.
b. The proposal for a PNR Council Framework Decision's privacy aspects

The most recent proposal for a Council Framework Decision on the use of PNR for law enforcement purposes naturally also has some data protection aspects. Article 11, 1a of that last proposal states that all processing of personal data in light of this Framework Decision both by the PIU and the competent authorities has to be in line with national law on the protection of personal data which has to comply with the standards of two documents. These are the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters and the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to the automatic processing of personal data, taking into consideration the Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector. With this as a background, the proposal goes on to state that PNR data can only be processed for the specific purposes set out in its earlier articles (see supra). Furthermore the processing must at all times be legitimate, adequate, relevant and not excessive. Some general data security measures must also be taken so that only authorized personnel of the PIU can reach the PNR data.\(^{36}\)

Processing sensitive data is prohibited in general but is still possible when meeting three conditions. First of all there has to be an automated risk assessment first, secondly it has to be necessary with regard to the purposes of the Framework Decision and lastly there is a need for domestic law that provides adequate safeguards.\(^{37}\)

In order to be able to check the lawfulness of the processing of all the PNR data, every transmission of and request for the data shall be logged. This control of the data protection will be done by the National Supervisory Authority. This is a public authority

\(^{36}\) Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/2/09 CRIMORG 7 AVIATION 3 DATAPROTECT 2.  
\(^{37}\) Ibid.
that is made responsible by the Member State for advising on and monitoring the application of all things data protection-related in light of the Framework Decision. It is also this Supervisory Authority that hears claims from persons who feel that their rights and freedoms concerning personal data are infringed. The Supervisory Authority is then able to start legal proceedings or bring the alleged infringement to the attention of the judicial authorities. In addition it can also give opinions about the use of the data, order the blocking or erasure of it and impose temporary or definitive bans from processing PNR data.\(^{38}\)

The proposal also states that the Member States have to make sure that every passenger is duly informed by the air carrier that their PNR are being transmitted to the PIU and that they might be used in the fight against terrorism and serious crime. Information about the passenger’s rights should also be given for he has the right of access, the right to rectification and erasure and the right to compensation. More specifically he has the right to compensation by the Member State for damage suffered by unlawful processing of the data and he has the right to compensation by the air carrier for damage that he suffered by a PNR transmission that was in violation of the national law adopted as a consequence of the Framework Decision.\(^{39}\)

c. Council of Europe and privacy

As we made clear above, the proposal for a Council Framework Decision on the use of PNR for law enforcement purposes explicitly refers to the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to the automatic processing of personal data and the Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector as being applicable to the processing of PNR by the PIU and competent authorities of the Member States that ratified the Convention. Since actually all of the EU Member States have ratified that Council of Europe Convention, it is worth mentioning here as well.\(^{40}\)

\(^{38}\) Ibid.  
\(^{39}\) Ibid.  
\(^{40}\) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG.
Concerning the content of the Convention, we can to a great extent refer to what has been said about the content of the Directive of ’95 since the latter was clearly influenced by the former. Noteworthy however is what is stated in the Recommendation of 1987 on the use of personal data in the police sector and which also became a part of the Convention after a protocol was added to it in 2001. This concerns the establishment of supervisory authorities in every Member State that are responsible for ensuring the adherence to the general principles as they are set out in the Convention, Protocol and Recommendation. This supervisory authority hears claims of people that feel that their rights and freedoms with regard to the processing of personal data have been infringed. Furthermore it has the power to investigate and intervene as well as to engage in legal proceedings when according to it, action has been taken without respect for the earlier named principles. In this aspect, they are quite reminiscent of the National Supervisory Authorities as they are described in the proposal for a Council Framework Decision (see supra).41

d. Council Framework Decision of 27 November 2008 on the protection of personal data

The Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters is, according to the latest draft of the proposal for a PNR Council Framework Decision, applicable to the transfer of PNR data by the PIU or competent authority of one Member State to the PIU or competent authority of another Member State. The same goes for future transfers of PNR data from a Member State to a third country.42

Content wise this Council Framework Decision talks about the same topics as the

---


42 Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/2/09 CRIMORG 7 AVIATION 3 DATAPROTECT 2.
other privacy-related documents do. Principles of lawfulness, proportionality and purpose are discussed just as time limits for data retention and the rights of access, rectification and erasure. Again we also see stipulations about a national supervisory authority with the same powers as the ones we cited above. Interesting as well is that the Council Framework Decision specifically notes that it is “without prejudice to any obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements with third States existing at the time of adoption of this Framework Decision”. This will be of importance for the agreement between the EU and the USA as we will see further on in the dissertation.43

e. Criticism towards the proposed exchange of PNR and privacy

The system as we have described it above and its privacy aspects have been the subject of quite some criticism.

One of the stipulations of the proposal for a Council Framework Decision that is criticized is article 11d,2 that sums up the reasons for which the right of access can be limited. These reasons are kept rather broad, so that the fear is real that the Member States might render this right mute. The question remains what the Member States will do with this in practice.44

The European Data Protection Supervisor (EDPS) has already claimed not to be in favour of the system of PNR. Regardless of the privacy aspects that are present, it is of the opinion that there is no necessity for such an infringement of privacy since other instruments that also focus on monitoring the movements of individuals within the EU have not been given due consideration and evaluation prior to coming up with the PNR proposal. Another issue is the impact the different legal regimes of the Member States might have on the exercise of the passenger’s rights of access, rectification, erasure and compensation. It can indeed turn out to be quite confusing for the passenger to know whom to turn to with his complaints or inquiries. Furthermore the

EDPS perceives the proposal as being too vague, especially when it comes to the identity of the PIU and the competent authorities and what exactly they can do under the proposal.\textsuperscript{45}

Some also fear that the use of PNR data in combination with profiling might mean a breach of the right to non-discrimination as protected by art. 14 ECHR. They fear that the PIU and the competent authorities might focus on certain ethnic or religious groups leading to stigmatization and a possible breach of art. 8 ECHR. However practice already has proven that this doesn’t necessarily has to be the case (see \textit{supra}).\textsuperscript{46}

Nevertheless, the European Union Agency for Fundamental Rights (FRA) has written a pretty interesting opinion about the relation between the PNR proposal and the right to privacy and data protection and the prohibition of discrimination. Since the processing of personal data such as the elements that are included on a PNR (see annex) is an interference with the right to privacy, some conditions have to be fulfilled. First of all, the objective of this interference has to be legitimate and meet objectives of general interest that are recognized by the EU or the need to protect the rights and freedoms of others. Since the objective is to fight terrorism and serious crime there is no real discussion on the legitimacy criterion. The second requirement is that the conditions under which the interference is imposed have to be described by law in such a way that it is accessible for those whom it affects and protects those people from arbitrariness by means of among other things precision and foreseeability. This criterion is subject to quite a lot of discussion since it implies that not only the persons who can consult the data should be explicitly made clear but also the nature of the files and the use that can be made of such information. Concerning the people who can access the data we can refer to what has been said about the vagueness of the PIU and the competent authorities. When it comes to the nature of the files we should look at what is being stipulated in the list of PNR data (see annex). Under number 12 on the list we see “General remarks”. It says that it includes information about a minor


\textsuperscript{46} E. BROUWER, o.c., 21-25.
travelling alone, however like this it leaves the door open for every other kind of information that can be seen as a general remark to be included. The FRA initially also criticized the fact that the earlier versions of the proposal talked about identifying persons who are or may be involved in terrorism or organized crime, as well as their associates without further specifying what they meant with “associates”. This could have led to situations wherein the term was interpreted very broadly so that the use to be made of the PNR would become rather unclear as well. In the later drafts of the proposal the term was left out and to remove any vagueness in this aspect the draft now only mentions identifying persons who themselves may be involved in a terrorist offence or serious crime. The last criterion is that the interference has to be proportionate to the end that is pursued. The FRA comes to the conclusion that as long as there is no evidence of the fact that the processing of PNR is effective in fighting terrorism and organized crime, the measure is disproportionate. As we have shown in the part about PNR in practice though, we can say that the processing is indeed effective. Therefore the measure should be seen as proportionate. 47

Taking all of this into account we can say that the proposal as it is now still isn’t totally in line with art. 8 ECHR. Further adaptations will have to be done in this field in order for it to be able to live up to the requirements.

Concerning the protection of personal data the FRA opinion is a bit obsolete since most of the problems it had with the proposal on this aspect have been taken care of. Like this specific stipulations have been added on the right of access, rectification and erasure and the National Supervisory Authorities. Other issues arise however. As art. 5,b of the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to the automatic processing of personal data reads, personal data should only be stored for specified and legitimate purposes and should not be used in a way incompatible with those purposes. Since the purpose of the exchange of PNR is to fight terrorism and serious crime, the provision in art. 4,5 of the proposal that the data can also be used for other offences when they are detected in the course

of law enforcement action following up to the processing of it is remarkable. Although rather logical as such, it is not in accordance with the requirements of clarity. This could however be remedied quite easily by limiting the other offences to those punishable with a certain minimum in sentence. Like this both the goals of clarity and further use of the data can be achieved.\footnote{EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, o.c., 7-10; E. BROUWER, o.c., 19-20; Art. 8 Charter of Fundamental Rights of the European Union.}

The Article 29 Data Protection Working Party (Art. 29 WP), together with the Working Party on Police and Justice, has also given its opinion about the proposal. Apart from pointing out issues like the ones we already cited above, it also casted its opinion on other topics of interest. It for instance drew attention to the fact that the list of PNR data elements to be transferred by the air carrier to the PIU might be a bit too extensive for the purposes of the exchange. When taking a close look at the list (see annex), this however doesn’t necessarily seem to be the case. Apart from the already talked about vagueness of the “general remarks” which might lead to the transfer of unnecessary information, nothing seems to be superfluous. Especially keeping in mind what we already talked about in the part about PNR in practice, it is really not that hard to see the law enforcement potential of every single data element on the list.\footnote{ARTICLE 29 DATA PROTECTION WORKING PARTY and WORKING PARTY ON POLICE AND JUSTICE, 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, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp145_en.pdf, 2007, 9-10.}

All of these issues are little aspects of the broader debate about the balance between privacy and security. In a response to not only terrorism, but also increasing international crime the first reaction is to concentrate on (re)creating a safe environment for your citizens. However by solely focusing on the security side of the equation that safe environment might turn out not to be as cosy as it was expected to be. People’s most personal rights might be infringed heavily thus rendering the freedom they can enjoy in that secure setting seriously limited. Such a world, reminiscent of the one described in 1984 by George Orwell, is not a world we want to live in, for really living would simply not be made possible. Too much emphasis on privacy on the other hand would not be liveable either. The constant threat of imminent danger would lead to a restless existence wherein the feelings of insecurity
would work paralyzing. The art then is to find a way in between. A way wherein people can feel secure and can still make use of a freedom that name worthy. Finding this way is one of our world’s biggest contemporary challenges. In order to have a decent chance of success, it is required to think every aspect of a (partial) solution to this problem through. Hysterical and hasty responses are therefore not always appropriate and will have to be adjusted and improved over time, when it is easier to get a broader and better view of the issue. A good example of the difficulty of trying to find the right balance between security and privacy is the case of the agreements between the EU and the USA on the exchange of PNR.

f. The EU-USA PNR agreements

Shortly after the attacks of 9/11, the USA adopted the Aviation and Transportation Security Act. This act requires all airlines entering the territory of the USA to transfer passenger data to the US Customs Service (later renamed to Bureau of Customs and Border Protection or CBP). Airlines that didn’t comply with this obligation were subject to large fines and possibly even revocation of their landing rights. European airlines were really between two fires since on the other side there was also EC law they had to be in line with in order not to be prosecuted. More specifically Directive 95/46/EC required that personal data was only to be shared with third countries who ensure an adequate level of data protection. Since the Art. 29 WP was of the opinion that the European airlines’ compliance with the US Aviation and Transportation Security Act would lead to infringements of their obligations under the data protection Directive of ‘95, there was a need to come to a negotiated agreement. 50

Until a joint statement was released by the EU and the USA in February 2003, the EU airlines were discharged from having to comply with the US Aviation and

Transportation Security Act. This joint statement had the function of an interim agreement. In the document, the EU agrees to not take any enforcement action against airlines that fail to comply with their duties under the data protection Directive of ’95 when they act in accordance with the US law. They refrain from such action because of the apparent good faith that the US has shown in providing the EU with enough undertakings and information about their use of the PNR data, the purpose with which they process it, how they will protect it, etc. Upon receiving this information, the European Commission will then be able to adopt a decision under art. 25,6 of Directive 95/46/EC stating that the US ensures an adequate level of data protection.51

The blatant way in which the Commission went along with the US’s plans raised more than one eyebrow. The European Parliament was one of the biggest critics stating among other things that the Commission failed to assume its responsibilities as guardian of the treaties and community law with the necessary diligence. This critique was based upon the fact that the Commission set aside community law for US law without even having thoroughly checked whether it provides sufficient data protection. Not only does this create a problem in this specific case, it also sets a bad example towards the Member States as to what the value is of community law.52

In response to the critique of the European Parliament, the US, as promised, gave more information about how it was planning to use the PNR data. In the undertakings the CBP for instance said it would only make use of the data in relation to terrorist offences and serious crime. Furthermore it was made clear that it would install automatic filters so that sensitive data would not be visible and that it would only use the pull method until the air carriers were able to push the information. The CBP would also implement certain security standards so that the data would not be compromised.53

For the Commission these proposals were adequate safeguards so they initiated the

process to issue an adequacy decision. In this process the Art. 29 WP needs to be heard. This Working Party was less positive as the Commission itself. It still saw some issues remaining. For instance it thought the 34 PNR data elements the US requested were a bit too much and out of proportion. It was also of the opinion that the data could be held too long and that in general the undertakings were not enough in a sense that they were not legally enforceable. The Commission however was dying to come to a definitive solution for the issue and it was with this in mind that Commission-member Frits Bolkestein addressed the European Parliament. Referring to the improvements the US had already made, he stated that it was in everyone’s best interest to come to an agreement and thus to decide that the data protection in the US was adequate. By calling this a political judgment, he implicitly admitted that the protection in fact wasn’t adequate yet but that deciding it was, was the only way forward.54

Despite the fact that the European Parliament rejected the Commission’s adequacy determination, the Commission went on and entered into an agreement with the US that had the support of the Council and had more or less the same content as the undertakings. As the European Parliament was furious with this, it started a legal procedure before the European Court of Justice (ECJ) seeking confirmation that the adequacy determination and the international agreement were both invalid. The Parliament claimed this invalidity since, in their eyes, the Commission acted ultra vires when it took the adequacy decision and because it was a breach of fundamental rights and the principal of proportionality.55

The ECJ however did not respond to the fundamental rights and proportionality-related claims. Instead it ruled that the adequacy decision was something that fell outside of the scope of what the Commission could do and that the agreement was based upon the wrong legal basis. More specifically the Court followed the Parliament in its reasoning that Directive 95/46/EC doesn’t apply here. Article 3,2 of that Directive states, like we already said before, that the Directive doesn’t apply to processing operations concerning public security and the activities of the State in areas of criminal law. The Court judged that in this case it specifically was an operation concerning public security since the exchange takes place in the framework of fighting terrorism and serious crime. Consequently the adequacy decision falls outside of the scope of the Directive. Since the Directive itself was based upon art. 95 EC (now art. 114 TFEU), which concerns the internal market (first pillar), the agreement dealing with terrorism and serious crime (third pillar) couldn’t have been validly adopted based on that Directive. The ECJ however did state that since both the adequacy decision and the agreement are so closely linked, it was in the interest of legal certainty opportune to not let the annulment of the decision take direct effect but to preserve it for the same 90 day-period that was due before the agreement would cease to have effect. Like this it allowed the EU to take the necessary measures to comply with the judgment.56

As a result of this, the EU and the US made work of a new temporary agreement. In this document the pull method was kept as a basis until a satisfactory push system was in place and reference was made to the undertakings. Furthermore the agreement simply stated that the Department of Homeland Security was considered to ensure an adequate level of data protection for the transfer of PNR data in the context of it. Ironic is that although the European Parliament got what it wanted with the ECJ decision, namely the annulment of both the adequacy decision and the agreement, it saw its role in the discussions seriously limited since the issue was moved from the

1-7; I. TUKDI, l.c., 606-607.  
first to the third pillar wherein the Parliament had far less to say.\textsuperscript{57}

This is why the permanent agreement of 2007, which still is in force, was reached rather smoothly. Herein some changes were made in comparison with the past agreements. First of all the Department of Homeland Security stated it would transition to the push method by the 1\textsuperscript{st} of January 2008 at the latest for all air carriers that had implemented this method in compliance with the Department’s technical requirements. Furthermore the requested PNR data elements were brought down from 34 to 19 (these 19 are the same as the ones in the proposal for a Council Framework Decision on the use of PNR for law enforcement purposes, see annex). This however shouldn’t really be seen as a concession of the US authorities since a close comparison of those 19 data elements with the 34 cited in the undertakings teach us that those 34 are just regrouped into 19 categories. The US thus still asks for exactly the same data. Really new was that the agreement granted access to the PNR data by individuals, regardless of their nationality or country of residence. Like this passengers can seek information about or correction of their PNR.\textsuperscript{58}

Nonetheless this agreement too was criticized by some of the EU’s data protection authorities. The EDPS expressed his concern over the very long retention period of 15 years in total, consisting of seven years in an active database and eight more years in a “dormant” or “sleeping” database. The fact that the PNR data can be shared with a high number of US authorities of which the identity isn’t sure yet also puts the European data protection rights at risk. Striking is also that the US deliberately chooses to use letters to talk about how they will process the PNR data. Here again, a letter from the US Secretary of Homeland Security to the President of the Council


further specifies the general stipulations of the agreement. Like this the US tries to dodge specific, legally enforceable obligations. The Art. 29 WP shares this concern and repeated some of its earlier problems with the agreement. In addition it elaborated on certain aspects such as for instance the fact that it is the Department of Homeland Security itself that is responsible for filtering out sensitive data. According to the Working Party this is a very risky matter since like this they can for themselves decide on whether or not they want to use these data elements. The agreement indeed notes that sensitive data can be used “in an exceptional case where the life of a data subject or of others could be imperilled or seriously impaired”. The question then is of course how you define such situations and whether there is someone who controls the Department in exercising this discretion. Moreover the Art. 29 WP states that although there are some small improvements, the general level of privacy protection is even lower than that of the undertakings.\textsuperscript{59}

So despite all of these voices of protest, the EU deemed the agreement as ensuring adequate data protection safeguards, bringing us to the situation we are in today, wherein PNR data is transferred to the US on the basis of the 2007 agreement.

\textbf{g. The future and what we can learn from all of this}

It should be clear that the last word still hasn’t been said about the agreement(s) with the US. In December 2009, the Art. 29 WP claimed in a letter to the European Commission that the US was violating its obligations under the agreement of 2007. Apparently the US authorities are still using the pull method even for airlines that comply with the DHS’s technical requirements, although the agreement states that they would use the push method in these cases as of the 1\textsuperscript{st} of January 2008. For the Working Party this is a clear breach of the agreement and consequently a perfect

reason to terminate that very agreement.\textsuperscript{60}

This is perfect ammo for the European Parliament to use in the discussions now that its consent with the EU-US PNR agreement of 2007 is required after the entry into force of the Lisbon Treaty. An interesting effect of this prerequisite is that all of a sudden, the US now does appear to be willing to share some numbers about the effectiveness of the exchange of PNR data. In an attempt to convince the members of the European Parliament to approve the agreement, a member of the Department of Homeland Security said that the PNR agreement was useful in identifying a third of the terrorists or potential terrorists that the US has identified in 2009. The US also issued another report in advance of the 2010 joint review of the 2007 agreement. In this report the Privacy Office of the Department of Homeland Security comes to the conclusion that the CBP complies with the terms of the agreement. Apparently all problematic aspects have been tackled and the move from a pull to a push system seems to be going well too in a sense that compared to last year another ten European air carriers have been able to implement the push system. The European Parliament however has decided in a resolution of 5 May 2010 to postpone the vote. Before voting it wants to explore other options for arrangements for the use of PNR that are in line with EU law. Furthermore it invites the Commission to present a single set of principles that can serve as a model for all PNR exchange arrangements with third countries. In addition it notes certain minimum requirements for this model such as using binding international treaties for such transfers and only making use of the push method.\textsuperscript{61}


As this shows, the negotiations between the EU and the US might have taken a different turn now with the entry into force of the Lisbon Treaty. This change has to be welcomed. For until now it is clear that these negotiations were constantly dominated by the US. Like this, the EU’s focus on fundamental rights has been set aside for the US’s focus on security. It really seems that every time the US made a proposal about how it was going to protect the data it received from the European air carriers, the EU immediately agreed with this and regarded this as ensuring an adequate level of data protection. This unequal relationship also resulted in the EU being inspired by the US for its own PNR system as it is proposed and as we have discussed it. The requested PNR data elements are almost exactly the same for instance. The use of active and “sleeping” databases also sounds very familiar. The fact that the EU used the US system as an inspiration should definitely not be seen as a surprise. As one Commission member supposedly stated, it would be difficult to explain to EU passengers that US authorities receive more information about them than their own national authorities. This however could be seen as a dangerous evolution. The risk being that US norms become global norms since the EU and the US are two of the most important actors in countering terrorism and organized crime. Caution and permanent close monitoring are due here. Then again it has to be pointed out that if it weren’t for all of these negotiations, an EU proposal for a PNR system would probably look worse than it does now. It seems as if the constant privacy issues hanging over the EU-US negotiations have led to a greater sense of awareness within the EU authorities. This will only increase now that the European Parliament has become more influential. Both indirectly, through the EU-US negotiations, and directly, with the discussions about the EU PNR proposal itself, the privacy aspects might gain more importance, thus making it likely that the proposal’s current privacy and data protection-related flaws will indeed be dealt with.62

---

5. Recommendation

Taking into account everything we have discussed it is possible to make a recommendation about what the European PNR system could or should look like.

As we saw, it is important that the people with the necessary expertise are the ones that do the profiling. They know what to look for, they know how to apply the risk criteria and they are capable of working with the different systems. Therefore it is important to invest in them. With the system as it is described in the proposal for a Council Framework Decision it is kind of unclear to see where these people can fit in when so much work is supposed to be done at the level of the PIU. Hence it might be better to see the PIU more as a database that gets the PNR data, for both international and intra-EU flights, from the air carriers that make use of the push method on a permanent basis. The profiling teams of the police forces then, can pull the information they need from the PIU. Like this the PIU becomes more of a collector that makes sure that the information is readable to the profiling teams. These teams can then completely focus on their profiling job based upon the information they need without being flooded with data. By making use of filters at the level of the air carriers, it is possible to keep the sensitive data there. Another option is to push the sensitive data along with the other elements to the PIU where it can be kept. In the rare case that profiling teams actually need the sensitive data elements, they can ask the PIU for them, bearing in mind that this is only possible in exceptional circumstances wherein they are necessary with regard to the purposes of the Council Framework Decision and when adequate safeguards are provided by domestic law.

Something that can still be done at the level of the PIU is running checks of the PNR against certain watch lists that include people that are wanted by law enforcement authorities. If there is a match, the PIU can then let those authorities know so they can take further action. This job doesn’t need any profiling or so and that is why it can still be done by the PIU. Like this, we keep the real analysis where it needs to be, namely, with the profiling teams. Besides of having the necessary expertise, they also have a better link with the practice. This allows a better connection between the profiling and the police work that naturally follows after it such as observations, controls, etc. In this
respect it furthermore facilitates the integration of profiling, and thus the use of PNR, in a nodal-oriented type of policing.

Seen as how profiling on the basis of PNR data for the moment is mostly done in Belgium and the UK, it might not be a bad idea to make use of the know-how of the police officers of said countries. More specifically they could assist police officers of other Member States in learning how to make use of PNR and how to do the analysis. Like this a common practice is set out for the whole of the EU and a certain level of proficiency is also achieved a lot faster as when those police officers are left on their own in getting acquainted with PNR.

Concerning the timing of the data transfer from the air carriers to the PIU, we have to plead for a system similar to the one being used between the air carriers and the police at Brussels Airport. This means transferring data from the moment there is a reservation list followed by updates until the moment of flight closure. The negative effects of working with outdated information are just too big, as we have indicated with the example in the part about PNR in practice.

The data retention periods as they are described in the proposal should be reduced. The data shouldn’t be kept longer than a year in an active database. Concerning the “sleeping” databases, practice has proven that a period between two and four years is already sufficient.

When it comes to privacy and data protection, the system as described in the proposal can be used as a basis. However some adaptations will have to be made. Regarding the right to privacy two things need to be done in order to comply with art. 8 ECHR. First of all, the vagueness of the notions “PIU” and “competent authorities” needs to be addressed. This can be done quite easily by attaching a list with the respective units and authorities for each country and where to find them to the Council Framework Decision. Fast communication between the Member States and the EU authorities is therefore needed. Secondly the issue of the “general remarks” needs to be taken care of. This can either be done by leaving it out completely or by specifying what other data elements are needed. It is recommended that the EU consults the practitioners in order to solve this question. Lastly an aspect of data protection also needs resolving.
This is the problem of the purpose specification. Since the purpose of the proposal is to fight terrorism and other serious crime, the stipulation that the PNR data can also be used for other offences when they are detected in the course of law enforcement action following up to the processing of said data needs further specification. This can be achieved by stating that the data can only also be used for offences that are punishable with a certain to be determined minimum in sentence.

6. Conclusion

In this dissertation we took a closer look at the use of PNR for law enforcement purposes in Europe. We started by explaining what PNR are and we talked about what makes them different from API. The API-directive can actually be seen as a first step towards the use of passenger data for law enforcement purposes. Its practical impact however wasn’t that big. This will probably be different with the PNR Council Framework Decision. Compared to the API-directive, its potential is a lot bigger. Not only does a PNR hold a lot more data elements, the proposal for a Council Framework Decision also appears to be more thought through. It can rely on the experience gained in the context of both the API-directive and the negotiations about the exchange of PNR between the EU and the USA. Especially the latter has had and still continues to have a big influence on the creation of a European PNR system. As we have shown, a lot of elements are directly taken from the US system. This has often been to the discontent of the European privacy and data protection authorities and the European Parliament. However also in the field of fundamental rights protection its impact can be noticed. The trials and errors made during the negotiations along with the criticism they were subject to can only be used to learn from and to come to a better system for Europe. Mistakes made on the transatlantic level shouldn’t be made anymore on the European level.

It is also in this field that the current proposal still has to be modified. Like we stated in the recommendation, both privacy and data protection elements need adaptation in order to be in line with European fundamental and human rights law. The system itself as it is described in the proposal is also susceptible of improvement. The emphasis on
automated risk assessment should be replaced by a focus on the “technique” of profiling as we have described it. This allows more of a case-by-case approach wherein attention can be given to certain particularities. This also means that investments have to be made in people with the right expertise and in creating that expertise for those who don’t have it yet.

If these requirements are met, the exchange of PNR might finally take place within a decent legal framework. The exchange has already proven its effectiveness, however it is this solid legal base that has been lacking. By taking into account the recommendations we made here, a balance between privacy and security might finally be found in this matter. It may not be the balance yet, but at least it is a workable way of paying due respect to both sides of the equation.
Annex: List of PNR data

(Source: Proposal of 29 June 2009 for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes)

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) 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 (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)

(13) Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields

(14) Seat number and other seat information
(15) Code share information

(16) All baggage information

(17) Number and other names of travelers on PNR

(18) Any collected API information

All historical changes to the PNR listed in numbers 1 to 18.
Bibliography

Legislation

Art. 8 ECHR.


Http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG.


Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.95, 31.

Art. 8 Charter of Fundamental Rights of the European Union.


European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights, OJ C 61 E, 10.3.2004, 381.


KB 11 december 2006 betreffende de verplichting voor luchtvervoerders om passagiersgegevens door te geven, BS 22 december 2006.


Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 7656/2/08 CRIMORG 49 AVIATION 77 DATAPROTECT 14.

Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes - State of play, 9514/08 CRIMORG 74 AVIATION 109 DATAPROTECT 27.

Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, 12360/08 CRIMORG 124 AVIATION 162 DATAPROTECT 55.

Art. 218 TFEU.


Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/2/09 CRIMORG 7 AVIATION 3 DATAPROTECT 2.

Case law


Doctrine


ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 5/2007 on the follow-up agreement between the European Union and the United States of
America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007,

ARTICLE 29 WORKING PARTY, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States,


Http://www.amadeus.com/airlinedisruption/customers/cus_1customers.html.


Http://www.sabreairlinesolutions.com/home/about.

Http://www.travelport.com/about/history.aspx.


VERACHTERT, T., Tickets en boarding passes: Nuttige doch niet (h)erkende elementen in een gerechtelijk onderzoek, unpublished, 11 p.


X, Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to