Air Passenger Lists in Civil Aviation

Olga Mironenko

Olga Mironenko, LLM, is a PhD candidate at the Norwegian Research Center for Computers and Law, and is writing about data protection and security in civil aviation. She has a background in the civil aviation industry from Russia. She graduated from the University of Oslo in 2009 and the State University – Higher School of Economics in Moscow in 2002.

1 Background: Development of Passenger Name Records (PNR) Systems

The right to privacy and data protection belongs to the fundamental rights and freedoms of the individual. It is also believed that effective security must be ensured in the civil aviation sector. But new surveillance and control measures being enforced under the motto of combating terrorism, specifically the collection of air passenger personal information, have a serious impact on these fundamental rights. As the result, a conflict arose between the use of personal data for security purposes and the protection of such data. Along with the threat of potential terrorist acts, the concurrent threat to privacy became a matter of public concern. The principal objective of this article is to examine, discuss and analyze the legal problems, issues and disputes deriving from this conflict with reference to the main sources of the air passenger personal data – the air passenger lists of the airlines.

The initial purpose of collecting passenger data by the airlines is generally to document commercial air transportation. In most cases this process includes flight reservation from the place of origin to a destination and back. This information is registered in the airline reservation system. In addition, the passenger might have some special or extra service requests, and these are also registered. A frequent traveler can also become a member of the airline’s loyalty program, which again requires some additional personal information enabling the airline to supply the passenger with all the benefits that the customer is qualified to receive.

But apart from airlines and passengers, there is another category of major participants in air traffic control, namely the State. States are concerned with ensuring compliance with applicable laws and policies. Among other things, States introduce and implement different air traffic
measures for the purpose of immigration and customs control, public and state security and defense, etc.

Initially, international mechanisms of surveillance in this area were quite general and limited. Article 29 of the Chicago Convention (1944) requires every aircraft engaged in international navigation to carry certain documents, including, for passengers, “a list of their names and places of embarkation and destination”. But due to dramatic events such as politically motivated acts of terrorism on an aircraft (which first occurred in 1968), various anti-terrorist and anti-crime security measures in civil aviation were adopted worldwide, and air passenger data became one of the most important sources for surveillance in the context of air traffic.

At first, many countries introduced measures such as pre-flight and luggage controls. In the late 1990s, the Computer Assisted Passenger Prescreening System (CAPPS) was created in the USA, which allowed the automatic singling out of certain passengers and putting them through stricter controls. After the terrorist attacks on 11 September 2001 in the US, security measures increased greatly. Inter alia, the first Passenger Name Records (PNR) system was implemented in the US.¹ All international airlines had to provide the US government with complete electronic access to detailed airline passenger data on all travelers registered in the airline's computer system. Furthermore, the US government issued a warning to airlines, namely that as of 5 March 2003 failure to provide the requested data would lead to a fine and withdrawal of landing authorization.

The CAPPS was redesigned and expanded to CAPPS II in 2003, entailing extended passenger checks. In 2004, the latter was replaced by the passenger-prescreening scheme Secure Flight, which is designed to compare passenger information against watch lists (so-called “selectee” and “no fly” lists, i.e. lists of individuals who “pose a threat”) maintained by the federal government

¹ According to the US Aviation and Transportation Security Act of 19 November 2001 (Pub. L. 107 – 71), all airlines flying to or from the US must disclose to the US Bureau of Customs and Border Protection (CBP) and the Transportation Security Agency (TSA) personal data contained in the PNR of air passengers. Not only the US Customs, but all US federal agencies can have access to these data.
in the Terrorist Screening Database.\textsuperscript{2} The goal is “to vet 100 percent of passengers on all
domestic commercial flights by early 2010 and 100 percent of passengers on all international
commercial flights by the end of 2010”\textsuperscript{3}.

Recent developments have shown that other countries’ security policies are greatly influenced
by the US policies. The European Union (EU) and the US tried to reach an agreement on PNR
transfer in a series of bilateral agreements.\textsuperscript{4} In 2007, after several terrorist attacks in Europe, a
European PNR system was proposed in the EU.\textsuperscript{5} The arrangements, having an international
dimension, provoked widespread privacy and security concerns.

Moreover, agreements for the transmission of PNR already exist between the EU and
Australia, and the EU and Canada, respectively.\textsuperscript{6} According to ICAO, several European states
have enacted primary legislation for the gathering of PNR data from air carriers, and other
countries worldwide are also now considering the use of the PNR, most notably Korea and
Australia.\textsuperscript{7}

\textsuperscript{2} The Intelligence Reform and Terrorism Prevention Act of 17 December 2004, DHS’ Notice of
See also: http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm.
\textsuperscript{3} Transportation Security Agency. TSA’s Secure Flight Enters First Public Phase.
\textsuperscript{4} Will be considered in section 5 hereafter.
\textsuperscript{5} Will be considered in section 6 hereafter.
\textsuperscript{6} Agreement between the European Community and the Government of Canada on the
processing of Advance Passenger Information and Passenger Name Record data. 21.3.2006.
(L 82/15). Agreement between the European Union and Australia on the processing and
transfer of European Union-sourced passenger name record (PNR) data by air carriers to the
\textsuperscript{7} ICAO, FALP/5-W/26. Recommendations Relating to ICAO’s Best Practices Relating to
Passenger name Record (PNR). 31/03/08.
The problem, however, is that PNR contain personal data about air passengers which is protected by law nationally and internationally. Since the security measures have a serious impact on the right to data protection, they need to be accompanied by strong and adequate safeguards. To what extent and how do the legal norms provide such safeguards for personal data circulating in civil aviation? Is it possible to find an appropriate balance between the need for surveillance and privacy-related interests? Due to the article’s format, I will analyze the applicable international instruments, citing the EU\textsuperscript{8} and the US regulations as the principal sources.

2 Overview of the main legal privacy framework
The right to privacy is protected by a number of international instruments.\textsuperscript{9} The EU legislation provides strict requirements for personal data processing: personal data must be (i) collected for

\textsuperscript{8} As a member of European Economic Area (EEA), Norway is bound by EU legislation incorporated in the 1992 Agreement on the European Economic Area. In the security field, a great part of Norwegian legislation is connected to its participation in the Schengen area cooperation. The data protection standards and security measures against terrorist acts in Norway are almost exclusively implemented as a consequence of international regulations. There are few independent Norwegian initiatives on anti-terrorist security measures (See: Transport Security and the Protection of Privacy. TØI report 914/2007). More detailed references will be given below.

\textsuperscript{9} The following international instruments are applicable: Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (applicable in the EU); the Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (not self-executing: it obliges members of CoE to incorporate its principles into their national legislation. It is open for ratification by states other than members of CoE); 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 data (it is binding for EU/EEA member states); the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal
specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (ii) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (iii) accurate, relevant, kept up to date; and (iv) stored only as long as necessary for the given purpose. Moreover, there are other requirements, such as the data subject’s right to be informed of the data processed, purposes of such processing, etc. and the right of access. The transfer of personal data from the EU/EEA\textsuperscript{10} to the countries lacking adequate level of protection is prohibited.

Protection afforded by the US law\textsuperscript{11} differs greatly. While the EU has historically enacted broad legislative protection of personal data, the US treats personal information as a commodity and the right to privacy is protected by common law mechanisms.\textsuperscript{12} There are, nevertheless, some statutes that limit the use of data, for example the Privacy Act of 1974. But the Privacy Act only protects personal information when it is processed by the federal government. The US has no general law protecting the privacy of “commercial” data. Thus air passenger personal data has

\begin{flushleft}
\textit{matters of 27 November 2008 (EU member states should take necessary measures to comply with this Framework Decision before 27 November 2010); the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23.09.1980 (not legally binding for OECD members); United Nations Guidelines Concerning Computerized Personal Data Files of 14.12.1990 (not legally binding).}
\end{flushleft}

\textsuperscript{10} The Directive 95/46/EC was incorporated on 25 June 1999 into the 1992 Agreement on the European Economic Area (EEA). Thus EEA member states which are not members of the EU (Norway, Lichtenstein and Iceland) are legally bound by the Directive. In Norway, the Directive is implemented by the Act of 14 April 2000 No. 31 relating to the processing of personal data. (LOV 2000-04-14 nr. 31: Lov om behandling av personopplysninger).


\textsuperscript{12} Patryk Pawlak. Made in the USA? The Influence of the US on the EU’s Data Protection Regime. Center for European Studies, November 2009.
been considered the “property” of airlines, over which travelers have no control. The airlines could allow the US government agencies to look at the data without the knowledge or consent of the data subjects. There is no comparable privacy law requiring disclosure to passengers of how their travel records are used.

Thus, after the introduction of the new security measures in the US, the European airlines found themselves in a difficult situation: to fly from the EU to the US, they could either refuse to transmit the data, thereby becoming subject to US authorities’ sanctions, or they could deliver the data in violation of the EU law.

3 Advanced Passenger Information (API)

Passenger data are typically categorized as Advanced Passenger Information (API) and Passenger Name Record (PNR). In this section I will discuss API requirements. PNR requirements will be dealt with in section 4.

The key difference between API and PNR is as follows. The collection of API is carried out by airlines on behalf of governments and serves immigration purposes. The collection of PNR has never been imposed by the governments; airlines have developed the PNR system according to their own commercial needs. API, deriving from travel documents information, offers more objective and permanently valid information, permitting the identification of individuals, while PNR include all the information that the passenger submits him or herself to the reservation system of the airline. PNR lists contain, therefore, not only “any collected API information”, but much more, including data of a sensitive nature.

According to Guidelines of June 2003, jointly agreed by the World Customs Organization (WCO), the International Air Transportation Association (IATA) and the International Civil Aviation Organization (ICAO), API involves the capture of a passenger's biographical data and other flight details by the carrier prior to departure and the transmission of the details by electronic means to the Border Control Agencies in the destination country. API can also act as a

13 The first international Guidelines on API were adopted in 1993 by the World Customs Organization (WCO) and International Air Transportation Association (IATA).

14 The lists are available in Annex 1 here.
decision making tool that Border Control Agencies can employ before a passenger is permitted to board an aircraft.

The recommended practice entails the electronic interchange of data elements and does not include manual preparation of lists, teletyped messages or documents. The API should be limited to the data contained in the machine readable zone of travel documents or obtainable from existing government databases, such as databases containing visa issuance information.

The purpose of API is not solely to provide the authorities with a complete manifest of passengers on board a flight. Article 22 of the Chicago Convention obligates States to facilitate international air navigation and adopt all measures to prevent unnecessary delays, especially in administration of the laws relating to immigration, quarantine, customs and clearance. ICAO states that use of an API system would reduce the costs incurred by aircraft delays due to inordinately long passenger clearance times, and it would also substantially reduce or eliminate the time-consuming data entry and computer processing required during the examination of each passenger from a flight for which data was not transmitted. It is essential also that the authorities have procedures and resources in place for such pre-arrival screening of passenger information.\footnote{ICAO. Specifications and Guidance Material (SGM) Section. Advance Passenger Information (API). http://www.icao.int/icao/en/atb/sgm/Api.htm}

At the same time, Article 13 of the Chicago Convention requires the aviation community to comply with a State's laws and regulations related to entry, clearance, immigration, passports, customs, and quarantine. ICAO states that the API system can be justified if it serves to improve productivity of operations and if it improves compliance with the above-mentioned laws and/or enhances aviation security.

Although the number of countries requiring API is increasing, the guidelines have not yet been agreed to by all governments that have, or are considering, API requirements. The problem is that many national API systems differ substantially. Many of these API systems appear: i) to have been established hastily; ii) to impose data transmission requirements on air carriers with minimal (sometimes 2 or 3 weeks’) notice; and/or, iii) to be set up apparently without consideration of the technical, financial and operational aspects of such systems. Air carriers are required to comply with diverse requirements from different states. This lack of uniformity leads
to tremendous operational and economic inefficiencies for airlines and possibly even for the States themselves. Therefore, according to ICAO, there is a need to ensure that present and future national API programs are standardized and are globally uniform.\textsuperscript{16}

In the EU, the API transfer is regulated by the Council Directive 2004/82/EC,\textsuperscript{17} which was adopted after the terrorist attacks in Madrid and aims at improving border controls and combating illegal immigration.

It provides that EU member states\textsuperscript{18} must oblige the carriers to transmit at the request\textsuperscript{19} of the authorities responsible for carrying out checks on persons at external borders, by the end of

\begin{center}
\begin{tabular}{l}
\hline
\textsuperscript{18} Directive 2004/82/EC is also applicable to EEA member states. According to Recital 14, as regards Iceland and Norway, this Directive constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter’s association with the implementation, application and development of the Schengen acquis, which fall within the area referred to in Article 1, point E, of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement. Norway has been associated with the Schengen Agreement since 19 December 1996. The agreement on Norway’s association with the implementation, application and development of the Schengen acquis, as based on the Council Decision 1999/439/EC of 17 May 1999, was signed between Norway and the EU on 18 May 1999. \\
\hline
\end{tabular}
\end{center}
check-in, information concerning the passengers they will carry. The sanctions imposed by member states on carriers deemed negligent in failing to transmit data or in having transmitted incomplete or false data, can vary from EUR 3000 to EUR 5000 for a journey. Other sanctions can also be adopted by the member states. API comprises: the number and type of travel documents used, nationality, full names, dates of birth, the border crossing point of entry into the territory of the member states, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport, the initial point of embarkation.

According to Directive 2004/82/EC Article 6, after passengers have entered the EU, the authorities shall delete the data within 24 hours after transmission. But the same article contains an exception: “unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders.” This contravenes with the EU data protection principle of strict purpose limitation.

One more exception which significantly extends the purpose of Directive 2004/82/EC, is another provision of Article 6 stating that “In accordance with their national law and subject to data protection provisions under Directive 95/46/EC, Member States may also use the personal data referred to in Article 3(1) for law enforcement purposes.”

With reference to the US, American authorities currently request the following: name, date of birth, gender, citizenship, country of residence, travel document type, its number, expiration date, country of issuance, foreign registration number (if applicable), address while in the US, passenger contact information (phone), any other data deemed necessary to identify the persons traveling. 20

19 The fact that data must only be transmitted in response to a prior request constitutes an important difference with the proposed EU PNR system which includes the systematic transmission of data (will be considered below).

Demands for additional information, such as passenger address while staying in the US and phone numbers, exceed the Guidelines’ recommendations (these items are not in the machine readable zone of a passport; see above).

According to IATA, the expanded list of required data elements constitutes the most critical and problematic issue. Moreover, IATA stated that the actual costs for both the program’s initial implementation and data collection and airport operations will rise significantly higher than the estimated cost of $164 million, which is “a staggering financial imposition for an industry”. 21

In addition, a number of countries do not have passports that are machine readable. This requires manual input, which is costly and slows down passenger handling at check-in. 22 In spite of the ICAO requirement for all countries to start issuing machine readable passports by April 2010, 23 a number of countries face the consequences of not having met this deadline.

4 Passenger Name Record (PNR)

According to the ICAO PNR Data Guidelines of 9 June 2005, a PNR, in the air transport industry, is the generic name given to records created by aircraft operators or their authorized agents for each journey booked by or on behalf of any passenger. The data is stored in the airlines’ reservation and departure control databases and is used by operators for their own commercial and operational purposes in providing air transportation services. 24


24 The Industry Standards related to PNR creation are detailed in IATA’s Passenger Services Conference Resolutions and in the ATA/IATA Reservations Interline Message Procedures (AIRIMP) Manual.
PNR allows all the different agents within the air industry to recognize each passenger and have access to all relevant information related to his/her journey: departure and return flights, connecting flights (if any), changes to requested seating, additional services, etc. Through special service codes, PNR reveal details of travelers’ physical and medical conditions; through special meal requests, they contain indications of travelers’ religious practices, i.e. a category of data typically referred to as “sensitive information”. The number and nature of fields of information in a PNR system will vary from airline to airline. There are approximately 20–25 possible fields of PNR data, some of which include subsets of information, expanding the total to approximately 60 fields and sub-fields.  

A PNR is created every time a traveler makes a reservation and cannot be deleted: once created, they are archived and retained in computer reservation system (CRS), and can still be viewed, even if a person never bought a ticket or cancelled the reservation. Each entry in each PNR, even for a solo traveler, contains identifiable information on at least two people, and often others: the traveler, the travel arranger or requester, the travel agent or airline staff person, and the person paying for the ticket. The PNR system contains all passenger data of the whole airline company, thus, the system is not restricted to a specific flight. Most travel agencies also use the CRS as their primary customer database and accounting system and store all customer data in CRS profiles. Thus PNR also contain data on individuals who never travel by air at all, since lots of travel services, such as car rental and hotel reservations, are made through CRS.

Besides CRS, which was initially created and run by the airlines themselves, there are now large Global Distribution Systems (GDS) which book and sell tickets for multiple airlines. There are four major GDS platforms in the world; Amadeus is the only one of these that is based in the EU rather than the US. Each of them has a website that gives anyone access to PNR data, very often with no password at all, but merely by reference to the reservation number printed on every ticket.

---


26 Amadeus, Sabre, Galileo and Worldspan.

27 Edward Hasbrouck. What’s in a Passenger Name Record (PNR)?
http://hasbrouck.org/articles/PNR.html
By contrast with API, PNR provides a comprehensive and extremely detailed record of every entry and includes data from which aspects of the passenger’s history, conduct and behavior can be deduced. Thus PNR can be used in profiling, offering national authorities information on the background of the individuals and their possible relationship to other persons being investigated. There is therefore a growing interest in the use of PNR worldwide for anti-terrorism and law enforcement purposes.

But since the rules governing PNR data provision are unclear, particularly with regard to data protection, the ICAO proposed the inclusion of some additional key principles, inter alia: 28

1. Where the existing laws of the state of departure prevent a carrier from complying with the requirements of the destination state, the latter should suspend the requirement for PNR data until the conflict is resolved, and no action should be taken against a carrier who is not able to supply data under these circumstances. Where a state requiring PNR data is not proven to have adequate data protection measures in place, states should enter into bilateral or multilateral negotiations in order to reach an agreement on data protection measures, before commencing a PNR program. According to ICAO, this should enable the carriers to continue operating to the country requiring PNR and avoid the problems encountered in 2003 by the EU airlines flying to the US.

2. PNR should not be required by a state until the state has the necessary data transfer protocols and appropriate automated systems in place to access or receive the data in a manner consistent with the guidelines. Otherwise an unacceptable burden will be placed on carriers to meet ad-hoc or manual processing requirements.

3. States should not require an operator to provide PNR data that is not already collected or held in the operator’s Reservation or Departure Control systems. States should require PNR data only from carriers who directly operate flights that are scheduled to enter, depart or transit through airports situated in their territory. States should not require data from any agent or third party marketing or selling tickets on such flights, including carriers operating in a code-share arrangement.

28 Recommendations Relating to ICAO’s Best Practices Relating to Passenger name Record (PNR), FALP/5-WP/26, 31/03/08.
4. The timing and frequency of data transfer should be limited to what is strictly necessary for law enforcement purposes. States should routinely request data on a scheduled basis, with a maximum of two iterations of data per flight. In exceptional circumstances and where States identify a specific threat, data for a given passenger or PNR may be requested on an ad-hoc basis.

5. Since operators cannot verify the accuracy or completeness of PNR data, the operator should not be held legally or financially responsible for errors or omissions in the data provided by the passenger or his representative. The only context where sanctions might be applied would include failure to transmit data when required or in instances where intentional modification of the data by the air carrier prior to transmission is proven.

But how can the recommendations be enforced? This question is still open. There appear to be some financial concerns as well. To date, according to IATA, the cost of transferring API to authorities is approximately US$14 per flight or more than US$100 million annually. Providing the PNR data in addition to API would make the expenses, as well as the amount of $164 million mentioned in section 3, even higher. Apparently, these costs, imposed on the airlines and other agents within the air industry, would ultimately have to be borne by travelers.

5 Agreement on PNR transfer between the EU and the US

As mentioned above, the US’ request for PNR transfer came into conflict with the EU data protection requirements. Firstly, the data controller can process personal data only if processing is compatible with the original purposes of data collection. Transfer of passenger personal data by airlines to the US government agencies can hardly be seen as a fulfillment of airlines’ contractual obligations towards their passengers. The airlines did not originally intend to collect data for the transfer of this to the US Customs (although one may argue that without such transmission airlines would fail to carry their passenger to the US).

29 IATA. Fact Sheet: Security.

Secondly, the transfer of personal data from the EU to the countries lacking an adequate level of protection is prohibited.\textsuperscript{31} With reference to the US there exists the Safe Harbor system,\textsuperscript{32} which is considered to provide an adequate level of protection.\textsuperscript{33} But the Safe Harbor principles apply only if the data recipient is an American enterprise that has signed up with Safe Harbor, and it cannot apply for data transfers to government authorities.\textsuperscript{34} Thus air passenger data transfer lies outside this system, and additional guarantees should be established which could ensure adequate protection. Namely, the problem of the lack of an adequate level of protection in the USA could be resolved by concluding a bilateral EU-US agreement, where adequate safeguards could be provided. But what is actually meant by “adequate protection”? According to Article 29 Working Party\textsuperscript{35} Opinion 12/98,\textsuperscript{36} analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for

\textsuperscript{31} Directive 95/46/EC, Article 25.

\textsuperscript{32} See: Safe Harbor Privacy Principles issued by the US Department of Commerce on 21.07.2000, Annex I. The Safe Harbor principles are intended for use solely by US organizations receiving personal data from the EU for the purpose of qualifying for the safe harbor and the presumption of “adequacy” it creates.


\textsuperscript{35} Working Party on the Protection of Individuals with regard to the Processing of Personal Data established pursuant to Article 29 of the Directive 95/46/EC (Article 29 Working Party). This organ consists of representatives from each EU Member State’s data protection authority. It acts independently of the Commission and other EU organs, but has advisory competence only.

ensuring their effective application. With regard to a contractual solution, therefore, the substantive data protection rules stipulated by the Directive 95/46/EC shall apply. In some situations additional principles relating to sensitive data, direct marketing and automated decisions must be applied. The contract should set out the detailed way in which the recipient of the data transfer should apply these principles (i.e. there should be specified purposes, data categories, time limits for retention, security measures, etc.). The Opinion stresses that detail is imperative where the transfer is based on a contract.

In order to render the substantive rules effective, a contractual solution must deliver a good level of compliance with the rules, provide support and help to individual data subjects in the exercise of their rights and provide appropriate redress to the injured party in the event of noncompliance with the rules.

But was the US in the position to provide data protection guarantees which would satisfy such requirements?

The first PNR Agreement between the European Community and the USA\(^\text{37}\) was subjected to substantial criticism from different institutions such as the European Parliament, Article 29 Working Party and privacy advocacy groups. The “weakest points” of the Agreement concerned both the substantive data protection rules and requirements for making them effective. Inter alia, the purposes for which the data might be used did not satisfy the purpose limitation principle (not only for fighting terrorism, but also for fighting “serious crime”). The list of 34 data elements to be transferred was excessive and not proportionate.\(^\text{38}\) The data retention periods were not proportionate either (3.5 years in an active database, then 8 years before the record is destroyed, etc.).


\(^{38}\) The full list is available in Annex 1 hereto.
and in certain cases much longer, with no verification mechanism for the deletion of the data at the end of the agreed storage period). A “pull” instead of a “push” system was used, meaning that the US does not have to ask for the data but has immediate access to it. The “detail” requirement was not followed, especially concerning data quality and data subjects’ rights, and there was a lack of mechanisms for redress, access and rectification, and provision of information to the passengers. Finally, sensitive data which normally should not be transmitted could be submitted in some cases. Furthermore, the US promised that the arrangement would not cover CAPPs II, but later, the US confirmed that the PNR data would be used for testing CAPPs II. The US promised not to pass the data on to other agencies. There was, however, no verification mechanism for this promise.

39 Paragraph 15 of Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data of 9 July 2004 states that this schedule of 3.5 and 8 years would not apply to PNR data that is linked to a specific enforcement record (such data would remain accessible until the enforcement record is archived).

40 As mentioned above, the PNR system is not restricted to a specific flight. Thus, allowing full access to PNR means that the US agencies also get full access to data of passengers who do not fly to the US at all.

41 See, for instance, Paragraph 11 of Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data of 9 July 2004 which states that prior to CBP's implementation of automated filters, if "sensitive" data exists in a PNR which is the subject of a non-discretionary disclosure by CBP as described in paragraph 35 hereof, CBP will make every effort to limit the release of "sensitive" PNR data, consistent with US law.

42 Computer Assisted Passenger Prescreening System II.

Moreover, this agreement was ruled invalid by the European Court of Justice,\textsuperscript{44} and on 6 October 2006, an “Interim Agreement”\textsuperscript{45} was signed. In contrast to the previous arrangement, it requested more data: “The Undertakings authorize Department for Homeland Security (DHS) to add data elements to the 34 previously set forth in Attachment ‘A’ of the Undertakings, if such data is necessary to fulfill the purposes set forth in paragraph 3”. Data was also allowed to be shared with additional and unspecified agencies: “The DHS will be allowed to share (without providing unconditional direct electronic access) PNR data freely with other US government authorities exercising a counter-terrorism function that need PNR for the purpose of preventing or combating terrorism and related crimes in cases (including threats, flights, individuals, and routes of concern) that they are examining or investigating.” The purposes, therefore, were widened. Along with other features such as undefined retention periods, allowing for more frequent and earlier pushing of data, unclear protection of personal data of EU citizens, it can be assumed that the scope of the agreement was widened substantially. Thus, the new deal looked weaker with reference to the passenger data protection level.

The new PNR Agreement was signed on 23 July 2007.\textsuperscript{46} According to the agreement, DHS uses EU PNR strictly for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any


\textsuperscript{45} 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, 2006 O.J. (L 298) 29. This agreement was valid until 31 July 2007.

\textsuperscript{46} Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) of 29 June 2007. 4.8.2007. (L 204/18).
criminal judicial proceedings, or as otherwise required by law. The list of purposes again is not limited at all.

The dataset was apparently reduced from 34 to 19 elements. But the reduction is largely cosmetic due to the merging of data fields instead of actual deletion. See, for example, line 7: All available contact information (including originator information). Previously this constituted four separate data items: 6. Address, 9. Contact telephone numbers, 17. E-mail address and 28. Received from information. The same concerns lines 8, 10, 14, 16 and 17. Thus the number of the elements in the list in fact remained the same (34).

With regard to sensitive data, it is stated that “DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information.” But at the same time the sensitive data can be accessed “if necessary, in an exceptional case where the life of a data subject or of others could be imperiled or seriously impaired”. In addition, the filtering of sensitive data continues to be done by DHS even with a “push” system. Apart from “exceptional cases”, sensitive data can be contained within the mandatory 19 fields of data. Line 17 (“OSI, SSI and SSR information”) can include such items as special meal requests, which can give an idea about sensitive data such as the religious beliefs of the passenger.

Moreover, Agreement 2007 comprises the following elements: (i) the Agreement signed by the parties; (ii) US DHS letter to EU giving assurances on the way it intends to protect PNR data; and (iii) a letter of reply from the EU to the US. Formally the Agreement is a treaty. But the letters are not actually legally binding. It is more accurate to say that they have an indirect legal force, since the EU has entered into the treaty on the basis of the assurances in the DHS letter explaining its safeguarding of PNR.

All three above-mentioned EU-US PNR agreements, in addition, had neither legal force nor effect in the US. To be binding and enforceable in the US, an international agreement must be

47 The full list is available in Annex 1 hereto.

48 Undertakings 2004, Attachment “A”.

49 Other Service Request, Special Service Information and Special Service Request respectively.


signed by the President, and ratified by the Senate as a treaty, or be enacted into US law. As of today, none of these requirements have been met.

With reference to the EU member states, the PNR Agreement 2007 is binding for them, but before it is ratified and incorporated, the PNR transfer can be governed only by national law and is generally prohibited. On 23 July 2007 eleven member states indicated that, in order for the Council to conclude the Agreement, they would have to comply with the requirements of their constitutional procedures. According to the information of the EU Council, by 19 March 2009 only five of the EU member states have finalized the ratification/incorporation process.\(^{51}\) Norway is not bound by the EU-US Agreement.\(^{52}\)

Furthermore, the US DHS, while accessing PNR and secretly keeping copies of some of them in the Automated Targeting System (ATC), violated the US Privacy Act of 1974 which requires prior notice in the Federal Register, in specific form, of the existence, content, and usage of each system of records of personal information maintained by a US Federal agency. It was not until 2006, after years of illegal operation outside the Privacy Act and EU laws and regulations, that the DHS confirmed the existence of the ATS and US government retention of PNR data.\(^{53}\) The DHS Privacy Office also reported that requests for PNR data have typically taken more than a year to answer — many times longer than the legal time limits in the Privacy Act and Freedom

\(^{51}\) Council Decision 5311/1/09 of 19 March 2009 on Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) - Declarations made in accordance with Article 24 (5) TEU – State of Play.

\(^{52}\) See: Gunnel Helmers. ”Passasjerdata – minst 15 års lagring” [Passenger Data – storage for at least 15 years]. 24.08.2007. http://www.datatilsynet.no

\(^{53}\) DHS admits problems in disclosing travel surveillance records. Identity Project (US human rights association).

of Information Act.\textsuperscript{54} The US human rights association Identity Project (IDP) published a condemnation on its website listing a series of violations of the PNR Agreement 2007, in particular the enormous difficulties encountered by citizens wishing to exercise their right to access stored data concerning them.\textsuperscript{55}

An example of such violations was the request in 2007 from a member of European Parliament Sophia In ’t Veld to receive PNR information pertaining to her. At first she received a claim from DHS that they did not have any record of her trip. The PNR data was finally received after American lawyers filed a lawsuit\textsuperscript{56} on her behalf, but the data was “late, clearly incomplete, and inconsistently and inappropriately redacted”.\textsuperscript{57}

Thus it can be concluded that the EU-US agreement failed to offer an adequate level of data protection and left many problems open. The US demands still violate EU data protection law. The agreement will undoubtedly need further negotiations and revisions.

Another problem is that the US is still trying to dictate tougher restrictions and get additional data transfer from EU member states by pressuring them individually. For example, the US takes advantages of the situation that “old” and “new” EU member states are unequal with regard to American visa policy. Within one year after the signing of PNR Agreement 2007, a group of new EU member countries\textsuperscript{58} signed their own Memorandum of Understanding with the US in regard


\textsuperscript{55} DHS admits problems in disclosing travel surveillance records. Identity Project (US human rights association).


\textsuperscript{56} The full complaint: http://www.eff.org/files/int_veld_complaint.pdf.

\textsuperscript{57} Edward Hasbrouck. Can you really see what records are kept about your travel? 30.12.2008.


\textsuperscript{58} Czech Republic, Estonia, Latvia, Lithuania, Hungary and Slovakia.
to visa waivers which could potentially jeopardize the protection of passenger data collected in those countries and extend even further the data required to be provided under the PNR Agreement 2007.\textsuperscript{59}

6 Proposed European PNR System

In November 2007, the EU announced a project containing anti-terrorism measures, including the creation of a European PNR system.\textsuperscript{60} The plan is to have a decentralized system of data collection.\textsuperscript{61} According to the proposal, airlines must make available to the member states\textsuperscript{62} 19

\textsuperscript{59} See, for instance, Memorandum of Understanding between the US and the Czech Republic of 26 February 2008.

\textsuperscript{60} Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, Brussels, 28 November 2007. The recent version of the Proposal: Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes 5618/2/09, 29 June 2009.

\textsuperscript{61} Although the (dis)advantages of a centralized vs. a decentralized scheme are still under discussion among the member states.

\textsuperscript{62} As for the EEA members, at the current stage, while the Proposal is under discussion, they have limited possibilities to participate. According to EEA Agreement Article 99, the EEA members have access to participation in the phase when the European Commission’s task is to prepare a proposal for new regulation, formally in expert panels. When the proposal is prepared, it is forwarded to the European Parliament and the EU Council which are entitled to ratify framework decisions. The Council then arranges hearings for the EU member states. If the Parliament and Council do not agree on the proposal, several attempts to reach agreement can be made. The EEA Agreement does not authorize the EEA members to participate when decisions are made. If the EU decision is relevant to the EEA Agreement, it can be discussed and incorporated into the EEA Agreement. After that the EEA members must implement it in national law.
PNR data elements on their passengers.\textsuperscript{63} Such data must be made available only for flights to and from the EU, excluding intra-EU and domestic flights. EU carriers will be required to “push” the data to the member states authorities and there will be two data transmissions, one 48 hours before the flight takeoff and one when the flight has completed boarding, with a Passenger Information Unit (PIU) as recipient of the data in each member state. PIU will conduct a “risk assessment” of the traveler, which could lead to questioning or even refusal of entry. PIU will share the results of such assessments with other PIU where necessary\textsuperscript{64} and retain the data for three years in an active database and for a “further period of [not more than seven] years” in a dormant database. Airlines refusing to provide the requested data before take-off will face withdrawal of their landing authorization.

The proposal received criticism from, inter alia, the European Parliament, Article 29 Working Party, EDPS\textsuperscript{65} and the EU Agency for Fundamental Rights (FRA).\textsuperscript{66}

\textsuperscript{63} The list is identical to that from the EU-US Agreement 2007, thus the actual quantity of elements is still 34. Despite the fact that it is not mentioned, the proposal in fact uses the EU-US PNR scheme as a model.

\textsuperscript{64} The draft states that the processing of PNR data by competent authorities and the transfer of PNR data is subject to the data protection safeguards laid down in the Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

\textsuperscript{65} European Data Protection Supervisor (EDPS) is established by the European Parliament and European Council pursuant to Directive 95/46/EC. It is an independent supervisory authority that regulates the processing of data.

\textsuperscript{66} Resolution of European Parliament of 20 November 2008 on the proposal for a Council framework decision on the use of PNR for law enforcement purposes, B6-0615/2008; European Data Protection Supervisor, Opinion on the draft proposal for a Council Framework Decision on the use of Passenger name Records (PNR) data for law enforcement purposes, Brussels, 20 December 2007; Article 29 Working Party, Opinion 5/2007 of 17.08.2007 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
Although the proposal states that the use of PNR together with API in certain cases has added value in assisting member states in verifying the identity of an individual, no substantial evidence is actually given that the collection of passenger data is necessary and adds value to the fight against terrorist offences and serious crime. There are other measures (in practice or about to be implemented), such as ESTA, biometrics in passports, SIS, VIS and national border protection schemes, but there is no information on the added value of these measures. The States Department of Homeland Security concluded in July 2007; FRA opinion on the proposal for a Council framework decision on the use of Passenger Name Record (PNR), 3 November 2008.


68 The Electronic System for Travel Authorization (ESTA) is an automated system that assists in determining eligibility to travel to the United States under the Visa Waiver Program (VWP) and whether such travel poses any law enforcement or security risk. Upon completion of an ESTA application, a VWP traveler is notified of his or her eligibility to travel to the United States under the VWP. See: Frequently Asked Questions About ESTA – ESTA Site Help. www.cbp.gov/linkhandler/cgov/travel/id_visa/.../esta_faq.pdf

69 Schengen Information System (SIS) is an EU border-related database system established pursuant to the Schengen Agreement of 14.06.1985. It allows national border control and judicial authorities to obtain information on persons or objects. In its new SIS II generation, the system will allow the checking of identities on the basis of biometric information.

70 Visa Information System (VIS) is designed to hold biometric data to identify persons who have lodged a visa application for an EU Member State. See: Council Decision 2004/512/EC of 8.06.2004 establishing the Visa Information System (VIS); Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9.07.2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

relationship between them and the use of PNR is also unclear. Furthermore, the reports published by other agencies which had previous experience with PNR, such as the Government Accountability Office in the US,\(^7^2\) did not confirm the efficiency of the measures. FRA stressed that reports published on earlier measures of profiling in Germany and the UK do not confirm at all, at this stage, the efficiency of profiling based on or associated with ethnicity, national origin or religion. Thus the necessity and proportionality tests are not fulfilled within the proposal.

The proposal suffers from a lack of precise purpose limitation. In principle, the use of PNR is limited to member states’ activities against terrorist offences or serious crime. But the text leaves different possibilities for extending the aims of PNR processing; for example, via wording that PNR use is allowed for “preventing, detecting, investigating and prosecuting terrorist offences or serious crime” which extends the activities of national authorities during which PNR may be gathered and used. In addition, Article 4 (5) allows the use of PNR for “other offences, or indications thereof”, if they are detected in the course of enforcement action with regard to terrorist offences or serious crime. The definitions of “terrorist offences” and “serious crime” are not actually specified in the text; they refer to other instruments: Council Framework Decisions on combating terrorism, organized crime and on the European Arrest Warrant, thus creating extra risks for further extending of the aims. Finally, Article 8 allows transfer of PNR and analysis of PNR data to authorities of third countries. But which authorities and third countries will obtain access to PNR, and how can their PNR use be controlled? These questions are still open.

Rights of access and rectification of data by the data subjects would suffer due to many different competent entities (the airlines, PIUs, the law enforcement authorities) and different recipients of data (possible data transfer between different PIUs).

The large discretion left to the member states would lead to widely diverging interpretations. For instance, according to the Association of European Airlines (AEA), “Commissioner Frattini's

proposed decentralized system means that our carriers will have to comply with 27 different national data collection systems. We are talking about an operational and technical nightmare – and the Commission totally ignores the financial implications for the airline industry, which we haven't even started assessing yet.‖

There is a lack of detail concerning the quality and conditions with which PIUs must exercise their competence. In addition, law enforcement authorities of different states have different competencies as well, which can also create difficulties for the implementation of the PNR system. Both the amount of personal data collected and the retention period are unreasonable. The proposal allows use of profiling and further use of sensitive data. The filtering mechanisms and possible third-country data transfers appear inadequate.

The passengers’ opportunity to gain access to records kept by the US authorities has been discussed above. But what about the EU? Under the Data Protection Directive, the travelers have the right to see all of the records concerning them kept by companies, and to be told what data has been sent to other parties.

According to an American privacy advocate, Edward Hasbrouck, when he asked KLM Royal Dutch Airlines to see the records of one of his trips from the US to the EU and back, he was informed months later by KLM that they had outsourced the handling of his data to companies in the US; they did not know what data their contractors and agents had collected or retained, or with whom they might have shared the data; and they had no provisions in their contracts that would enable them to force their contractors to provide this information. When Edward Hasbrouck asked the Dutch Data Protection Authority to intervene, they admitted that they had no staff with the technical competence or sufficient knowledge of the industry to interpret the limited data that KLM had disclosed. Hasbrouck was informed that they could not

---


74 According to Article 11a of Proposal 5618/2/09, PIUs can collect, store and, if several conditions are met, fulfill any processing with the sensitive data as well.

help, and there was nothing to be done except hire a lawyer in the Netherlands to prepare and file a private lawsuit against the airline.

7 Conclusion

Air passenger data of the airlines has already become one of the most important sources for surveillance in the context of air traffic. As discussed, the problems generally derive from the conflict between the states’ demands for access to information and the data protection compliance obligations. Despite the fact that the majority of recent developments derive from the US, nowadays this concerns all the countries interested in public and state security and defense within the air traffic areas.

According to a number of surveys, there are actually doubts about whether the collection of passenger data is necessary or whether it adds value to the fight against terrorism and serious crime (in addition to other security measures which already exist or are planned to be implemented). Moreover, due to the fact that since 2001 the amount of API increased and their processing purpose was extended to include public security, the content of API became similar to PNR. Thus, privacy protection guarantees should be given accordingly to both API and PNR.

Another important problem is that, in spite of the existence of ICAO’s international guidelines both on the use of API and PNR, they are not obligatory for the member states and there are no enforcement mechanisms. Thus all endeavors to produce global standard approaches in this area are facing major challenges. The airlines, when required to provide passenger data to different state authorities, have to deal with numbers of different systems with different requirements and procedures. This creates technical and operational chaos for the airlines, with substantial financial consequences.

With regard to the passengers, real-world experiences undertaken to see if a person can really be informed of his or her records that are being kept and processed proved that no one can rely on existing compliance, enforcement, or oversight mechanisms (in the examples mentioned above, both in the US and the EU, for both US and EU citizens). According to the guidelines laid
down by the Article 29 Working Party,\textsuperscript{76} the airlines should provide a simple but efficient data protection guarantee – tell passengers that information about their travel will be transferred to state authorities. Of course, informing passengers about collected data may not in itself legalize the transfer, but would enable them to make a conscious decision, namely whether they wish to divulge personal, detailed information or not.

One of the explanations for the conflict between security and data protection rules may be the differences between the US and the EU legal systems and traditions. The negotiations between the EU and the US on the PNR agreement were pushy on the US side of the table, while the EU was forced to take several steps backward. Many of the weaknesses were discovered and discussed broadly in public before the agreement was entered into. But it must be remembered that the decision makers were under strong pressure from the US. Besides, the agreement was needed as soon as possible to avoid legal uncertainties for the EU member states, air passengers and air carriers, thus it was preferable to have an agreement with weaknesses and shortcomings, rather than not to have one at all. The agreement thus was more a political solution than a legal instrument.

In the meantime, the EU itself is establishing its own PNR system using the EU-US PNR Agreement 2007 as a model. The proposal therefore suffers, apart from its own weaknesses, many of the same shortcomings as the EU-US deal. From these undertakings we can see that the control and surveillance regime designed to uphold security and prevent terrorism and crimes will most likely prevail over the privacy issues. According to the European Commission's Eurobarometer surveys on data protection of January 2008, the majority of EU citizens (82\%)\textsuperscript{77} seem to be ready to give up some of their rights and agree on the monitoring of PNR when this is aimed at combating terrorism (but with the reservation that the monitoring must be restricted to terrorism suspects).

Unfortunately, the scope and purposes of such control may become broader and even less limited. After establishing European surveillance laws, the European Commission might also

\textsuperscript{76} Article 29 Working Party, Opinion 2/2007 of 15.02.2007 on information to passengers about transfer of PNR data to US authorities.

\textsuperscript{77} Eurobarometers are ad hoc thematical telephone interviews to measure public opinion. The survey results are available at: http://ec.europa.eu/public_opinion/flash/fl_225_sum_en.pdf
seek to create a global regime on passenger records surveillance, permitting all countries to gain access to this data. Thus, despite the fact that the EU is blaming the US for inadequate data protection standards, it may go even further than the US in establishing a global system of surveillance.

ANNEX 1

EU-US. PNR Data Elements Required by CBP from Air Carriers

(Undertakings 2004, Attachment “A”):

1. PNR record locator code
2. Date of reservation
3. Date(s) of intended travel
4. Name
5. Other names on PNR
6. Address
7. All forms of payment information
8. Billing address
9. Contact telephone numbers
10. All travel itinerary for specific PNR
11. Frequent flyer information (limited to miles flown and address(es))
12. Travel agency
13. Travel agent
14. Code share PNR information
15. Travel status of passenger
16. Split/Divided PNR information
17. Email address
18. Ticketing field information
19. General remarks
20. Ticket number
21. Seat number
22. Date of ticket issuance
23. No show history
24. Bag tag numbers
25. Go show information
26. OSI information
27. SSI/SSR information
28. Received from information
29. All historical changes to the PNR
30. Number of travelers on PNR
31. Seat information
32. One-way tickets
33. Any collected APIS information
34. ATFQ fields

**EU-US. Types of EU PNR Collected**

**(PNR Agreement 2007):**

1. PNR record locator code
2. Date of reservation/ issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Available frequent flyer and benefit information (i.e., free tickets, upgrades, etc.)
6. Other names on PNR, including number of travelers on PNR
7. All available contact information (including originator information)
8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information
12. Split/divided information
13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote
15. All Baggage information
16. Seat information, including seat number
17. General remarks including OSI, SSI and SSR information
18. Any collected APIS information
19. All historical changes to the PNR listed in numbers 1 to 18

EU. PNR data pursuant to Article 2

(Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes 5618/2/09, 29 June 2009)

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
(19) All historical changes to the PNR listed in numbers 1 to 18.