RANKED AMONG THE WORLD'S TOP 10 THINK TANKS
CEPS Liberty and Security in Europe
CENTRE FOR EUROPEAN POLICY STUDIES

# Ignoring Dissent and Legality

## The EU's proposal to share the personal information of all passengers

**Evelien Brouwer**

**June 2011**

**Abstract**

In February 2011, the European Commission published a proposal for a new Directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes. This proposal replaces an earlier draft of 2007 for a Framework Decision on the use of PNR data for law enforcement purposes. The new proposal does not seem to allay the earlier concerns of important stakeholders with regard to the 2007 proposal. Its content contradicts not only important principles of data protection as described by the Commission in November 2010, but also the principle of proportionality underlying EU law. This paper examines the extended purpose and (lack of) added value of this proposal. It also considers its relation to the Directive on advanced passenger information and PNR agreements between the EU and third countries, the lack of harmonisation and the consequences for the fundamental rights of individuals.



ISBN 978-94-6138-109-5
Available for free downloading from the CEPS website (http://www.ceps.eu)

# Contents

# Ignoring Dissent and Legality
## The EU's proposal to share the personal information of all passengers

**Evelien Brouwer***

**CEPS Paper in Liberty and Security in Europe, June 2011**

## 1. Introduction

In February 2011, the European Commission published a proposal for a new Directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.[1] This proposal follows and replaces an earlier draft of 2007 for a Framework Decision on the use of PNR data for law enforcement purposes.[2] The draft Framework Decision, the primary goal of which was the fight against terrorism and organised crime, was critically received by the European Parliament, the European Data Protection Supervisor (EDPS), the EU Agency for Fundamental Rights, the Article 29 Working Party and other organisations. In their comments, these organisations criticised in particular the lack of evidence on the necessity and proportionality of the proposed measure, the insufficient level of data protection, and the risks of profiling and transfer of data to third countries. With regard to the new proposal by the Commission, the EDPS, the Article 29 Working Party and the European Economic and Social Committee repeated many of their earlier criticisms.[3]

The new proposal does not seem to allay the earlier concerns with regard to the 2007 proposal. Its content contradicts important principles of data protection as described by the Commission in November 2010 in the Communication on a comprehensive approach to personal data protection in the European Union.[4] Furthermore, the proposal does not meet the general principle of proportionality, which is the basis of EU law.

---

* Evelien Brouwer is Associate Professor, Utrecht University. This paper is based on an earlier commentary on the PNR proposal written by the author on behalf of the Meijers Committee. The author would like to express her gratitude to Elspeth Guild and Sergio Carrera for their comments.

[1] European Commission, *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32, Brussels, 2 February 2011.

[2] European Commission, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654, Brussels, 6 November 2007.

[3] See EDPS, Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, adopted on 25 March 2011; Article 29 Data Protection Working Party, Opinion 10/2011, adopted on 5 April 2011 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf); European Economic and Social Committee, Opinion, SOC/414, Passenger Name Record data/terrorist offences, 5 May 2011; and Committee of the Regions, Opinion, Council Document No. 10169/11, 13 May 2011.

[4] See European Commission, Communication on a comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, Brussels, 4 November 2010.

This paper addresses the following subjects:

- the extended purpose and (lack of) added value of this proposal,
- its relation to the Directive on the use of advanced passenger information (2004/82/EC),
- lack of harmonisation,
- consequences for fundamental rights of individuals, and
- its relation to the PNR agreements between the EU and third states.

## 2. Purpose and necessity of the PNR proposal

Comparing the current proposal with the earlier draft of 2007, the Commission took into account some criticisms of the aforementioned stakeholders. With respect to the data retention periods, the original time limit of 13 years has been reduced to 5 years. Furthermore, in response to the criticism of the European Parliament and EDPS on the differentiation between the pull and push methods in the 2007 proposal (applying the push method to EU carriers, and a combination of push and pull for third-country carriers) the Commission proposal now provides for an exclusive use of the push method.[5] Still, despite these improvements, the new proposal does not really narrow the scope of its application, nor does it provide extra safeguards. On the contrary, instead of limiting the goals for which member states may use PNR data, the current proposal extends the purpose of this instrument further. Whereas the earlier draft Framework Decision on the use of PNR data was limited to the purpose of "preventing and combating terrorist offences and organised crime", this has been changed in the new PNR proposal to "the prevention, detection, investigation and prosecution of terrorist offences and serious crime". Especially in the definitions of "prevention, detection and investigation" and "serious crimes" the national authorities are left with a wide margin of discretion, which will result in large differences among the member states implementing this Directive.

For the definition of serious crime and serious transnational crime, the proposal refers to the Framework Decision on the European Arrest Warrant (2002/584/JHA), which could be considered a positive delimitation of crimes for which PNR data may be processed. Yet the list of offences in Art. 2(2) of the Framework Decision still includes the possibility for divergent practices in the member states, including on interpreting general definitions of such terms as "terrorism", "participation in a criminal organisation", "corruption", "computer-related crime" "facilitation of unauthorised entry and residence" or "sabotage". According to the explanatory memorandum, member states may also exclude minor offences if their inclusion would not be proportionate, which implies that in general PNR data may be processed for minor offences as well. This possibility of exemption will likewise result in divergent implementation of this Directive by the member states. Finally, consideration 28 of the preamble provides that the possibility remains for member states to oblige air carriers to transfer PNR data for purposes other than those specified in the Directive.

The reasons for the (extended) use of PNR data are not clarified. In the explanatory memorandum, the Commission refers to trafficking in human beings and drug-related crime, and illustrates the human and economic costs of these crimes using rather random data from various sources, including data of the UK Home Office on costs incurred "in anticipation of crime" of 2003. Moreover, the Commission does not provide real evidence of the added value

[5] The 'push method' refers to carriers forwarding, by their own means, the PNR data to the national authorities of the arrival or departure state, whereas the 'pull method' implies that the national authorities obtain the PNR data by having direct access to the reservation systems of the air carriers. See also the Opinion of the European Union Agency for Fundamental Rights (FRA) on the PNR Proposal of 14 June 2011 (http://www.fra.europa.eu).

of using PNR data for the prevention or prosecution of these crimes. The European Commission only refers to examples in three countries (Belgium, Sweden and the UK) in which a substantial number of drug seizures would have been "exclusively or predominantly" due to the processing of PNR data. These data are not further specified, and surprisingly not mentioned at all in the impact assessment of this proposal. It also seems odd that according to the Commission, Belgium reported that 95% of all drug seizures in 2009 exclusively or predominantly stemmed from the processing of PNR data, while according to the same impact assessment Belgium would not have implemented any PNR scheme by that time.

## 3. Relation to the Directive on advanced passenger information

The Commission does not provide information on the implementation of the Directive on the use of advanced passenger information (API), which was adopted in 2004 and for which the implementation date was exceeded in September 2006.[6] This Directive concerns the obligation of air carriers to transfer API to border officials for immigration law purposes. Considering the added value for law enforcement and migration control purposes, it is important to differentiate between API and PNR data. Whereas API concerns data from the machine-readable zone of the passport – including name, date of birth, passport number and nationality – PNR data includes data that are registered by the airline companies or travel agencies when a traveller makes a reservation: including the person's name, seat number, travelling route, booking agent, credit card number, etc. These PNR data are collected for reservation purposes, and thus may differ for each air carrier organisation or may not always include the same categories of information. The most important difference between API and PNR is that the information that can be extracted from PNR data mainly depends on the data the passenger submits him- or herself to the ticket reservation system. Related to passport information, API data offer national officers more objective and permanently valid information, permitting the identification of individuals. Whereas PNR data (entailing diverse information on the passenger such as meal requests, contact information and travel agencies) may be useful for profiling, such data are less reliable, being dependent on what the traveller submitted him- or herself when making a reservation. In addition, as has been pointed out by the Association of European Airlines, with respect to the identification of passengers the PNR data are not always consistent with the persons actually on board the air carrier. Therefore, the inclusion of category (10) in the annex to the current proposal, concerning the PNR data to be collected, is rather pointless. Referring to the "travel status of passenger, including confirmations, check-in status, no show or go show information", this includes data that are by definition not included in the PNR data, because this information will only be available when the passenger has (or not) checked in for his or her flight.

During negotiations on earlier drafts of the API Directive, the use of API was originally planned for immigration control purposes alone. Shortly before the final adoption of the Directive, however, a provision was added according to which member states may use the passenger data for law enforcement purposes (Art. 6). One would have expected an evaluation by the Commission of the current use of the API Directive, together with the existing large-scale databases in the EU, before proposing new measures of data collection. Although Directive 2004/82/EC does not include a sunset clause or obligation for the Commission to evaluate this instrument itself, it is in line with the general policy of the Commission to assess "the initiative's expected impact on individuals' right to privacy and personal data protection and set out why such an impact is necessary and why the proposed solution is proportionate to the

[6] Council of the European Union, Directive 2004/82/EC of 29 August 2004 on the obligation of carriers to communicate passenger data, OJ L 261/24, 6.8.2004. In June 2010, the Commission started an infraction procedure against Poland for failure to adopt the necessary laws implementing the Directive, Case C-304/10, OJ C 246/22, 11.9.2010.

legitimate aim of maintaining internal security within the European Union, preventing crime or managing migration".[7] This failure to first identify the security gaps of existing systems and methods of cooperation has similarly been pointed out by the Article 29 Working Party in its opinion of April 2011.[8] According to the Working Party, if any gaps exist, then the next step should be to analyse the best way to fill these gaps by exploiting and improving the present mechanisms, without necessarily introducing a whole new system.

## 4. Lack of harmonisation

According to the European Commission, the PNR proposal would be necessary to harmonise national legislation on obligations for air carriers, preventing the creation of 27 "considerably diverging systems", which could result in "uneven levels of data protection across the Union, security gaps, increased costs and legal uncertainty for carriers". The goal of the current proposal is to guarantee "a uniform standard of protection of personal data under any proposal, and provide legal certainty for individuals, commercial operators and law enforcement authorities".[9]

First, it seems justified to question the claim of the Commission that this proposal is necessary to prevent 27 diverging systems in the EU. At this time only three member states provide legislation for the use of PNR.[10] This means that rather than harmonising existing rules, this proposal will result in forcing a large majority of the EU member states to adopt a new law enforcement measure. Second, with regard to important issues on the collection and use of PNR, the current proposal does not provide for harmonisation at all. As mentioned above, the purpose of using PNR data has not been narrowly defined and the proposal leaves the member states a wide margin of interpretation by referring to "serious crime" and "serious transnational crime" and by including the aforementioned preamble 28. In the next sections, it will become clear that the proposal does not offer harmonised rules with regard to other important subjects either, including

- time limits,
- extension to internal flights,
- the functioning of PIUs,
- the authorities entitled to request or receive PNR data, and
- transfer of data to third countries.

### 4.1 Time limits

Despite the shortening of the data retention periods from a maximum of 13 years to a maximum of 5 years, the 2011 proposal still includes some questionable provisions extending the use of PNR data. The proposed Art. 9 differentiates between a period of 30 days after the transfer of PNR data, in which they are retained in a database of the national Passenger Information Unit

[7] European Commission, Communication on Overview of information management in the area of freedom, security and justice, COM(2010) 835, Brussels, 20 July 2010, p. 25.

[8] Article 29 Data Protection Working Party, Opinion 10/2011, op. cit.

[9] European Commission, *Impact Assessment accompanying document to the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, Staff Working Paper, SEC(2011) 132, Brussels, 2 February 2011 – see pp. 15 and 20.

[10] These are the UK, France, and Denmark, with the remark that it is still unclear whether the UK will decide to opt in to this proposal. See the European Commission's Staff Working Paper on Impact Assessment (SEC(2011) 132) of 2 February 2011, *supra*.

(PIU). After this period, the data will be stored for a further 5 years by the PIUs. In principle, during this period, all elements serving to identify persons will be 'masked', meaning that 30 days after the transfer of their data, passengers can no longer be identified on the basis of these data. But during the period of 5 years access to full PNR data will remain possible for "a limited number of personnel of national PIUs" specifically authorised to carry out analysis of PNR data and to develop assessment criteria according to Art. 4(d) of the proposal. This latter provision allows the analysis of PNR data for the purpose of updating or creating new criteria for carrying out assessments in order to identify persons who may be involved in a terrorist offence or serious transnational crime. In other words, during these 5 years, personnel of PIUs may use non-anonymised data for the purpose of setting up new profiles. Meanwhile, during the same period of 5 years, each head of the national PIUs may have access to the full data "where it could be reasonably believed that it is necessary to carry out an investigation and in response to a specific and actual threat or risk or a specific investigation or prosecution". The descriptions of both "limited number of personnel" and "specific investigation or prosecution" are too vague and allow disproportional use of passengers' data.

The proposed Directive allows the aforementioned time limits of 30 days and 5 years to be set aside by the member states. Art. 9(3) of the proposal includes an exception to the obligation to delete PNR data after 5 years, where they have been transferred to national competent authorities and are used "in the context of specific criminal investigations or prosecutions, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State".

Finally, Art. 9(4) allows the PIUs to keep the results of matching based on PNR data for an indefinite period, namely "as long as necessary to inform the competent authorities of a positive match". An important provision is that which obliges the PIUs to keep data on so-called 'false' positive matches: these data should be kept for a maximum period of three years to avoid future false matches. Yet the proposal does not provide safeguards on the further retention of these data or on how other national authorities will be informed there has been a false match.

## 4.2 International or internal flights, or both?

On the basis of the proposed Art. 6, member states will have the choice between whether the obligation on air carriers applies only to international flights arriving in their territory or also to departing flights. Currently, the member states are negotiating the (optional) extension of this Directive to internal flights. This will mean that air carriers will have to deal with divergent rules applying in each member state. This will result not only in high costs for each air carrier organisation, but also in the different treatment of travellers within or coming to the EU.

## 4.3 The functioning of the PIUs

The draft Directive does not offer harmonised rules on the functioning of the national PIUs. The PNR proposal allows variations among the member states with regard to the assessments carried out on passenger data, the use and new creation of "pre-determined criteria" for the PNR assessments, and the further transfer of data to law enforcement authorities, other member states or third parties. As set out below, the use of profiling and the assessment of individual behaviour solely based on PNR data imply risks to the fundamental rights of travellers. The lack of harmonised criteria will increase these risks.

## 4.4 Authorities entitled to request or receive PNR data

Art. 5(1) of the proposal obliges member states to adopt a list of competent national authorities entitled to request or receive PNR data or the results of processed PNR data by the PIUs. The

Directive does not give any further specifications, however, other than that these authorities should be "competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime". A comparable mechanism has been identified in the Data Retention Directive (2006/24/EC).[11] The list of authorities having access to telecommunications data, published in the European Commission's recent evaluation report on the implementation of the Data Retention Directive, reveals many differences among the member states.[12] These differences concern in the first place the scope of 'competent national authorities'. According to this evaluation, 14 member states include security and intelligence services, 6 member states list tax or customs authorities (or both) and 3 list border authorities. Second, the list makes clear many differences with regard to the procedure for gaining access to the telecommunication data. Among the member states, 11 require judicial authorisation for each request for access to retained data and 3 require judicial authorisation in "most cases". In 4 member states the authorisation of a senior officer is required but that not of a judge, and in 2 member states the only condition is that the request is made in writing. In the evaluation report, the Commission states that it is necessary to assess the need for a greater degree of harmonisation with respect to the authorities having access and the procedure for obtaining access to retained data. In our opinion, the adoption of comparable mechanisms with regard to PNR data or other proposals granting national law enforcement authorities access to personal data (for example Eurodac) should wait for the outcome of such an evaluation.

## 4.5 Transfer of PNR data to third countries

Art. 8 of the 2011 proposal allows member states to transfer PNR data and the results of the processing of PNR data, only on a case-by-case basis and if

- it is in accordance with the conditions Art. 13 of the Framework Decision 2008/977/JHA;
- the transfer is necessary for the purposes of this Directive specified in Art. 1(2); and
- the third country agrees to transfer to third states only when necessary for the purpose of this Directive, and only with the express authorisation of the member state.

The inclusion of the condition of "case-by-case basis" prohibits the systematic transfer to third countries; however, to ensure its effective application, this provision will need close supervision. Whereas the 2007 proposal only provided for the further transfer of PNR data, this draft also allows for the transfer of the results of the PNR analysis by the PIUs or national authorities. The reference to Art. 1(2) of the proposal excludes the transfer of PNR data for "other purposes" as mentioned in the preamble, but it does include the very wide definition of purposes as provided in Art. 4(2) of the Directive.

Whereas the 2007 proposal explicitly stated that transmission to third countries may only take place in accordance with the national laws of the member state concerned and any applicable international standard, the 2011 proposal only refers to the Framework Decision 2008/977/JHA.[13] This Framework Decision includes data protection rules in the field of police

[11] See Art. 4 of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54, 13.4.2006.

[12] European Commission, *Evaluation report on the Data Retention Directive*, COM(2011) 225, Brussels, 18 April 2011 – see pp. 9-12.

[13] Council of the European Union, Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.

and judicial cooperation. From the perspective of a uniform scheme of data protection law in the EU, it seems illogical to refer in this Directive on the transfer of passenger data to the rules of a former third-pillar instrument, when the Commission is expected to replace this instrument (and Directive 95/46/EC) with a new general instrument on EU data protection law in the near future. Furthermore, Framework Decision 2008/977/JHA does not guarantee a harmonised approach by the EU member states.

Art. 13 of the aforementioned Framework Decision allows the transfer to competent authorities in third countries or to international bodies if

a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

b) the receiving authority in the third state or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

c) the member state from which the data were obtained has given its consent to transfer in compliance with its national law; and

d) the third state or international body concerned ensures an adequate level of protection for the intended data processing.

The Framework Decision allows transfer without prior consent in accordance with paragraph 1(c) if the transfer of the data is essential for "the prevention of an immediate and serious threat to public security of a member state or a third State or to essential interests of a member state and the prior consent cannot be obtained in good time".

The adequacy of the level of protection referred to in paragraph 1(d) must be assessed "in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations". According to the Framework Decision, "particular consideration" must be given to

> the nature of the data, the purpose and duration of the proposed processing operation or operations, the State of origin and the State or international body of final destination of the data, the rules of law, both general and sectoral, in force in the third State or international body in question and the professional rules and security measures which apply.

This provision will also result in a differentiated approach by the member states.

In addition, Art. 13(3) of the Framework Decision provides a very wide derogation from the aforementioned conditions and allows transfer of personal data if

(a) the national law of the member state transferring the data so provides because of
  i) the legitimate specific interests of the data subject; or
  ii) the legitimate prevailing interests, especially important public interests; or

(b) the third state or receiving international body provides safeguards that are deemed adequate by the member state concerned according to its national law.

Finally, the draft Directive allows the further transfer of personal data from the third state to other third countries. Even if this requires the explicit consent of the member state concerned, it does not give other member states, national supervisory authorities, the EDPS or the Commission any power to control this further dissemination of passenger data.

## 5. PNR, profiling and the fundamental rights of individuals

According to the explanatory memorandum, the draft PNR Directive is aimed at achieving information on "unknown criminals or terrorists". Unlike other databases, such as the Schengen Information System (SIS) or Visa Information System (VIS), which provide information solely on identified persons regardless of whether they are being reported for specific goals (arrest warrants or refusal of entry), the transfer and especially analysis of PNR data should assist national authorities of the member states in identifying criminal offenders or associates or persons suspected of terrorist or serious crimes. The Commission distinguishes among three possible ways PNR data can be used: "re-active", "real-time" and "pro-active" use. "Re-active" use refers to use of the data in investigations, prosecutions and the unravelling of networks after a crime has been committed. With "real-time" use, the Commission refers to national authorities using data prior to the arrival or departure of passengers in order to prevent a crime, watch or arrest persons before a crime has been committed or because a crime has been or is being committed. In such cases PNR data may be used for running such data against predetermined assessment criteria to identify persons who were previously "unknown" to law enforcement authorities, or for running the data against various databases. Finally, "pro-active" use concerns the use of the data for analysis and the creation of (new) assessment criteria, which could then be used for a pre-arrival and pre-departure assessment of passengers.

Dealing with both the 2007 proposal and the current draft of February 2011, stakeholders expressed their concerns about the impact of using PNR data for profiling on the fundamental rights of individuals. Profiling can be understood as an automatic data processing technique that consists of applying a 'profile' to an individual, particularly for taking decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.[14] According to the Fundamental Rights Agency in its report on ethnic profiling of 2010, "profiling involves categorising individuals according to their characteristics, whether these are 'unchangeable' (such as gender, age, ethnicity, height) or 'changeable' (such as habits, preferences and other elements of behaviour)".[15] As discussed below, the rights at stake include the rights to privacy and data protection, non-discrimination rights, and the right to free movement. With regard to the latter right, it is important to distinguish between the right to freedom of movement as a human right protected in Art. 2 of the 4th Protocol to the European Convention on Human Rights (ECHR) on the one hand, and the freedom of movement as one of the fundamental rights of EU citizens and their family members, based on Art. 20 of the Treaty on the Functioning of the European Union (TFEU) and Directive 2004/38/EC.

## 5.1 Profiling and the right to non-discrimination

Art. 14 ECHR and the12th Protocol to the ECHR prohibit discrimination on any ground, such as gender, race, colour, language, religion, political or other opinions, national or social origin, association with a national minority, property, birth or other status.[16] According to the case law of the European Court of Human Rights (ECtHR), a difference in treatment is discriminatory, if it "has no objective and reasonable justification", that is if it does not pursue a "legitimate aim" or if there is not a "reasonable relationship of proportionality between the means employed and

[14] This definition is used in the Council of Europe Recommendation CM/Rec(2010)13 of the Committee of Ministers of the Council of Europe adopted on 23 November 2010, at the 1099th meeting of the Ministers' Deputies.

[15] European Union Agency for Fundamental Rights (FRA), *Towards more effective policing: Understanding and preventing discriminatory ethnic profiling, a guide*, FRA, Vienna, 2010, p. 8.

[16] The right to non-discrimination is further protected in the Convention on Elimination of Racial Discrimination, Arts. 2 and 26 of the International Covenant on Civil and Political Rights, and the Racial Equality Directive (Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180, 19.7.2000).

the aim sought to be realised".[17] With regard to discrimination based on race, gender or nationality, very weighty reasons have to be submitted. In *Timishev v. Russia*, the ECtHR found that no difference in treatment based exclusively or to a decisive extent on a person's ethnic origin is capable of being objectively justified in a contemporary democratic society built on the principles of plurality and respect for different cultures.[18] In this case, concerning the refusal by Russian authorities to allow a national of Chechen ethnicity to pass administrative borders within Russia, the ECtHR found a violation of the right to non-discrimination with regard to the right to liberty of movement as protected in Art. 2 of the 4th Protocol to the ECHR.

Investigative or law-enforcing powers are often based on profiling, using generalised criteria such as nationality, country of origin, religion, etc.[19] Profiling on the basis of PNR data may expose passengers to risks of discrimination, resulting in a differential treatment that includes search or stop measures, or extra surveillance based on the aforementioned pre-selected criteria.[20] Such differentiation or discrimination should be limited to situations where an objective and reasonable justification exists, and when based on gender, race or ethnic origin, should only take place on the basis of very weighty reasons. A decision to stop and search an individual that is motivated solely or mainly by virtue of a person's race, ethnicity or religion can be described as discriminatory ethnic profiling and is therefore unlawful.[21]

According to the Commission, the proposed use of PNR data has the advantage that it enables national authorities to perform "a closer screening only of persons who are most likely, based on objective assessment criteria and previous experience, to pose a threat to security". This would facilitate the travel of all other passengers and reduce the risk of passengers being subjected "to screening on the basis of unlawful criteria such as nationality or skin colour which may wrongly be associated with security risks by law enforcement authorities, including customs and border guards". The Commission addresses an important problem of current border controls and the risk that these controls are led by discriminatory considerations. It nonetheless seems questionable whether the aforementioned use of "pre-determined criteria" will actually result in less discrimination at the borders or whether it just changes the moment of screening by the PIUs. Both methods will have the same result, namely that a person may be refused entry

[17] Refer to the case *Gaygusuz v. Austria*, 16 September 1996, Application no. 17371/90.

[18] See the case *Timishev c. Russia*, 13 December 2005, Application nos. 55762/00 and 55974/00, paras. 58-59.

[19] See the definition of the Open Society Justice Initiative on "ethnic profiling" in *Ethnic Profiling in the European Union: Pervasive, Ineffective and Discriminatory*, Open Society Foundations, New York, NY, May 2009: "the use by law enforcement of generalizations grounded in ethnicity, race, religion, or national origin – rather than objective evidence or individual behavior – as the basis for making law enforcement and/or investigative decisions about who has been or may be involved in criminal activity".

[20] See the aforementioned Recommendation of the Council of Europe (CM/Rec(2010)13), op. cit. See also Olivier de Schutter and Julie Ringelheim, "Ethnic Profiling: A Rising Challenge for European Human Rights Law", *Modern Law Review*, Vol. 71, No. 3, 2008, pp. 358-384; and András Pap, *Ethnicity and Race-based Profiling in CounterTerrorism, Law Enforcement and Border Control*, Study for the Directorate-General of Internal Policies of the LIBE Committee of the European Parliament, November 2008; and Evelien Brouwer, *The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?*, CEPS Working Document No. 320, CEPS, Brussels, September 2009 (www.ceps.eu); and the Office of the High Commissioner of the United Nations for Human Rights (OHCHR), *Report of the Special Rapporteur on the protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, OHCHR, Geneva, 29 January 2007.

[21] FRA (2010), op. cit., p. 64.

or subjected to further investigation measures on the basis of "pre-determined criteria", or in other words, the use of profiling.

Art. 5(6) of the current proposal provides that competent authorities may not take any decision that produces an adverse legal effect on a person or significantly affects a person "on the basis of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life". Although this general prohibition of discriminatory decision-making is to be welcomed, it does not exclude that the analysis or assessment of PNR data by the PIU may be based on one or more of the aforementioned criteria. This means that indirectly, on the grounds of this Directive, decision-making by competent authorities based on one of these discrimination grounds is still possible. Furthermore, the reference to "decisions" does not make clear that this prohibition also applies to the measures of national authorities, including physical measures such as searches or preventing persons from entering the territory.

## 5.2 The right to privacy

The systematic collection and storage of personal data by national authorities may fall within the scope of the right to privacy as protected in Art. 8 ECHR, irrespective of the use that is effectively being made or the sensitivity of the data.[22] In the case *Marper v. United Kingdom*, the ECtHR referred to the stigmatising effect of the long-term, systematic storage of fingerprints and DNA samples of individuals, including minors, who were suspected of having committed criminal offences, but not convicted.[23] In this judgment, the ECtHR found that the applicable UK law violated Art. 8 ECHR, particularly on the grounds that these data were stored for indefinite periods and concerned non-convicted persons, and was thus disproportional. Considering both the stigmatising effect of being selected repeatedly on the basis of "pre-determined criteria", and the lack of sufficient safeguards and legal remedies for the individual in the current proposal, it is not unlikely that the systematic transfer and storage of PNR must be considered a disproportional infringement of the right to privacy.

Of relevance with regard to the indiscriminate transfer and use of PNR data is the consideration of the ECtHR in the *Marper* case. More specifically, the Court states that it is struck by "the blanket and indiscriminate nature of the power of retention in England and Wales" and the fact that "the material may be retained irrespective of the nature of gravity of the offence with which the individual was originally suspected or of the age of the suspected offender" (para. 119). The ECtHR concluded there was a violation of Art. 8 ECHR also because of limited possibilities for the individual to have the data removed from the nationwide database or to have the materials destroyed and because of the lack of independent review.[24] Moreover, as the ECtHR has pointed out repeatedly in its judgments, to fulfil the requirement that the breach of privacy is in accordance with the law, including the principle of foreseeability, the law must be sufficiently clear in its terms "to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures".[25] As

[22] See ECtHR in the case *Amann v. Switzerland*, 16 February 2000, Application no. 27798/95 and *Rotaru v. Romania*, 4 May 2000, Application no. 28341/95.

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

[24] A report by the Dutch National Ombudsman of 2008 illustrates the devastating effects for a Dutch businessman, who as a result of identity theft and incorrect information in different files, including the Schengen Information System, was searched and arrested for more than ten years, at Schiphol airport among others. The main cause for this ongoing problem was the impossibility of obtaining the correction of his data in the different files at stake. See the report of 21 October 2008, 2008/132 (only in Dutch) (www.nationaleombudsman.nl).

[25] See the case *Copland v. United Kingdom*, Application no. 62617/00, 3 April 2007, para. 45.

discussed above, the current proposal does not offer harmonised criteria and leaves the different member states wide discretionary powers with regard to the use, retention and further dissemination of passenger data. Therefore, the current proposal does not meet the criterion "in accordance with the law" of Art. 8(2) ECHR.

Aside from Art. 8 ECHR, the right to privacy has been included in Art. 7 of the EU Charter on Fundamental Rights. According to Art. 52 of the Charter, in so far as the Charter contains rights guaranteed by the ECHR, the meaning and scope of these rights shall be the same as those laid down by the ECHR, including the determination of these rights by the ECtHR in its case law.[26] This means that when adopting new measures like the PNR proposal, the EU legislator is bound by the aforementioned interpretation of Art. 8 ECHR by the ECtHR. Taking into account Art. 6 of the Treaty on the European Union (TEU), which aside from the provision on the accession of the EU to the ECHR, also confirms that the fundamental rights in the ECHR constitute the general principles of EU law, it is safe to assume that the Court of Justice of the European Union (CJEU) will follow the same approach of the ECtHR when it is requested to assess the lawfulness of the current proposal in the light of Art. 8 ECHR.

## 5.3 The right to data protection

Art. 8 of the EU Charter on Fundamental Rights safeguards the right of everyone to protection of personal data concerning him or her. According to Art. 8(2), such data must be processed "fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law". Further safeguards are provided in Directive 95/46/EC on the protection of personal data.[27] In November 2010, the European Commission adopted a Communication on "a comprehensive approach on personal data protection in the European Union", including proposals and an approach for the review of the EU legal system on the protection of personal data.[28] In this Communication, the Commission defined general principles and guidelines for the future structure of EU data protection law. The content of the current PNR proposal is difficult to reconcile with these general principles. In the first place, the Commission advocates the further harmonisation of data protection law, which as we have seen, is not provided in the PNR proposal. Second, the Commission calls for enhancing control over one's own data, for example by harmonising law on the individual's right of access, correction and deletion of his or her data, and strengthening the principle of data minimisation. It also calls for clarifying the so-called 'right to be forgotten' – the right of individuals to have their data no longer processed and deleted when the data are no longer needed for legitimate purposes.

The PNR proposal does not incorporate an explicit right of access, correction or deletion of the individual. It only includes an obligation for member states to ensure that the private organisations involved (air carriers, agents or other ticket sellers) will inform passengers at the time of booking a flight and at the time of purchasing a ticket "in a clear and precise manner" about the provision of PNR data to the PIU, purposes of processing, period of data retention, possible further use and exchange of such data, and their data protection rights (Art. 11 of the proposal). For this purpose, one could refer to the right to information as formulated in

[26] This provision does not prevent more extensive protection.

[27] 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, OJ L 281, 23.11.1995.

[28] See European Commission, COM(2010) 609 final, op. cit. These principles have been further developed by EU Justice Commissioner Viviane Reding in her speech to the Privacy Platform, "The Review of the EU Data Protection Framework", SPEECH/11/183, Brussels, 16 March 2011.

paragraph 4.1 of the Recommendation of the Committee of Ministers of the Council of Europe (the text is presented in the Appendix to this paper).[29]

Another measure announced by the Commission in the aforementioned Communication is to make remedies and sanctions more effective. According to the Commission, the power to bring an action before the national courts, to data protection authorities and to civil society associations, as well as to other associations representing data subjects' interests, should be extended. The Commission also proposed to assess whether existing provisions on sanctions can be strengthened, for example by explicitly including criminal sanctions in cases of serious data protection violations, in order to make them more effective. It is a positive step that, unlike the 2007 proposal, the current PNR proposal includes a provision obliging member states to impose "effective, proportionate and dissuasive penalties" in case of infringements of the provisions adopted pursuant to this Directive (Art. 11(7)). Yet these sanctions are not further specified and it is not clear against which authorities or organisations they may be imposed. Art. 12 of the proposed Directive obliges member states to ensure that national supervisory authorities are responsible for "advising and monitoring" the application of this Directive, without supplying these organisations with binding or coercive powers. What is more, the proposal does not include any direct reference to individual data protection rights or legal remedies.

## 5.4 Freedom of movement of EU citizens, their family members and third-country nationals under EU law

Aside from non-discrimination, privacy and data protection rights, it should also be emphasised that the current proposal raises problems from the perspective of the fundamental freedoms of Union citizens and their family members as protected in Art. 20 TFEU and Directive 2004/38/EC.[30] Art. 27 of Directive 2004/38/EC provides that every measure restricting the freedom of movement and residence of EU citizens and their family members must comply with the principle of proportionality and "be based on their personal conduct representing a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society". Stop and search measures on EU citizens and their family members at the airport of a member state that are solely based on an analysis of PNR data of his or her flight cause an unlawful limitation of their freedom of movement. In the case *Heinz Huber v. Germany*, the CJEU made clear that the systematic and strict monitoring of EU citizens may infringe the right of non-discrimination of EU citizens in relation to the proportionality principle to be observed on the basis of Directive 95/46/EC on the protection of personal data.[31] In this case, the CJEU found that the practice of the German central aliens administration of including data on EU citizens violated their right to non-discrimination on the basis of a strict application of the condition of necessity as laid down in Art. 7(e) of Directive 95/46/EC. Among others, the German legislator had failed to justify the necessity of the centralised nature of the database, the storage of individualised personal data in the AZR for statistical purposes, and the possible use of the personal data on EU citizens for law enforcement purposes.

[29] See the Recommendation of the Council of Europe (CM/Rec(2010)13), op. cit.

[30] Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC, OJ L 158, 30.4.2004.

[31] See Case C-524/06, *Heinz Huber v. Germany*, 16 December 2008.

Furthermore, search measures grounded on PNR analysis on the basis of this Directive may also infringe the freedom of movement of EU citizens and third-country nationals, whose rights are guaranteed by EU legislation (for example the EU–Turkey Association Agreements, Directive 2003/86/EC on family reunification and Directive 2003/108/EC on long-term resident third-country nationals). Therefore, any measure on the large-scale collection and use of personal data should include a clause taking into account the freedom of movement and rights of EU citizens and third-country nationals. A comparable clause has been included in the Schengen Borders Code and the Returns Directive (2008/115/EC).[32]

## 6. Negotiations on PNR agreements with third countries

The discussion on the current PNR proposal cannot be considered separately from the negotiations underway between the Commission and third countries on the transfer of PNR data to these third countries. Here as well, one wonders whether the negotiators have learned from the past and taken into account the earlier comments with regard to the content of these agreements. Despite the intense and long-term discussions between the Commission, the European Parliament and other stakeholders on the level of protection in earlier agreements, the current texts of the PNR agreement with both the US and Australia still include many gaps with regard to the rights of passengers.[33] These gaps concern among others the long data retention periods, the wide discretion for US authorities to use the PNR data and the power to transfer these data to other third countries.[34]

When negotiating with third countries on the transfer of passenger data, whether with the US, Australia or South Korea, it is even more necessary to take into account the above comments on the protection of fundamental rights. Because these agreements concern the transfer of personal data to third countries – outside the legal order of the EU – the European Commission, data protection authorities or passengers will have few or no powers to control the lawfulness or security of the storage and further use of these data. As underlined by the European Parliament in its Resolution of May 2010, legal certainty for both EU passengers as well as airlines require a coherent approach and harmonised standards.[35] The standards applying to the transfer of data to third countries should not be below the level of the EU's PNR system.

## 7. Conclusion

Considering the risks of violation of the fundamental rights of passengers, including EU citizens and third-country nationals, and the expected high costs for individual member states and air

---

[32] See for example, Art. 3 of the Schengen Borders Code: "This Regulation shall apply to any person crossing the internal or external borders of Member States, without prejudice to: (a) the rights of persons enjoying the Community right of free movement; (b) the rights of refugees and persons requesting international protection, in particular as regards non-refoulement." See also Art. 4(2) of the Returns Directive (2008/115/EC of the European Parliament and of the Council of16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348/98, 24.12.2008): "This Directive shall be without prejudice to any provision which may be more favourable for the third-country national, laid down in the Community acquis relating to immigration and asylum."

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

[34] The most recent version of the EU–US PNR agreement includes a data retention period of 15 years, and the Agreement with Australia includes a retention period of 5.5 years. The texts are available on the Statewatch website (www.statewatch.org).

[35] European Parliament Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, P7_TA(2010)0144.

transport organisations, the proposed PNR Directive should not be adopted. The Commission has not provided real evidence of the added value of the current PNR proposal for the prevention or prosecution of terrorist offences or serious crimes. Without further information on the added value of the dissemination of passenger data of every traveller flying from and to the 27 member states, one must conclude that this proposal does not meet the principles of necessity and proportionality. This principle of proportionality, as reaffirmed by the Court of Justice of the European Union in a case dealing with the dissemination of personal information on the Internet, is one of the underlying principles of EU law. This principle "requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it".[36] Earlier criticisms of the European Parliament, the EDPS and other stakeholders with regard to the 2007 proposal for a Framework Decision on PNR have not or only partially been taken into account. The new proposal does not offer clear rules with regard to the powers of national authorities to use PNR data or to transfer these data to other countries, nor does it include sufficient safeguards to protect the fundamental rights of individuals. The proposal lacks in particular harmonised rules on the following subjects:

- purpose limitation,
- data retention,
- individual rights,
- powers of supervisory and judicial authorities, and
- transfer of data to third countries.

Before adopting new measures, the European Commission should be invited to evaluate current measures on the collection of personal data for law enforcement and migration control purposes, including VIS, SIS, the Prüm Treaty and the API Directive. Only on the basis of this information is it possible to identify the 'security gaps' in the fight against terrorism or serious crime.

Any new draft on the transfer of PNR data should include an extended impact assessment with reliable and up-to-date information on the efficiency, financial costs and consequences for the fundamental rights of individuals. Such a new impact assessment could be based on the recent *Operational Guidance on taking into account Fundamental Rights in Commission Impact Assessments*, published by the European Commission in May 2011.[37]

If the aforementioned requirements are met, any future proposal on the use of PNR data should entail precise criteria limiting the discretionary powers of national authorities, including PIUs, with respect to the collection and use of personal data. A new proposal should incorporate limitative rules on the grounds for which data may be collected, the authorities 'competent' to receive and use such data, time limits for data retention, and applicable safeguards and sanctions for misuse or incorrect use of data. For this purpose, the standards as included in the recommendation on the use of profiling in the public and private sectors adopted by the Committee of Ministers of the Council of Europe in November 2010 could be taken into account.[38] These standards, for example, concern the rights and legal remedies of individuals

[36] See Case C-92/09, *Volker and Markus Schecke v. Land Hessen* and Case C-93/09, *Eifert v. Land Hessen*, 9 November 2010, para. 74. See also Case C-58/08, *Vodafone and Others* [2010] ECR I-0000, paras. 51 and 86.

[37] European Commission, Commission Staff Working Paper SEC(2011) 567 final, Brussels, 6 May 2011.

[38] Recommendation of the Council of Europe (CM/Rec(2010)13), op. cit.

pertaining to the collection and use of their data, which should be formulated more precisely, including the rights to information and financial redress.[39]

Considering the risks to the protection of fundamental rights and freedoms, the conclusion of agreements with third countries on the systematic transfer of passenger data to third countries should be submitted to the same if not even more strict scrutiny as described above. If the individual rights of EU and non-EU passengers are not taken seriously now, it will only be a matter of time before the instruments at stake are denounced in either Strasbourg or Luxembourg.

[39] With regard to the right to information, a provision has been included in the Recommendation of the Council of Europe on profiling – see the Appendix of this paper.

## References

Brouwer, Evelien (2009), *The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?*, CEPS Working Document No. 320, CEPS, Brussels, September (www.ceps.eu).

De Schutter, Olivier and Julie Ringelheim (2008), "Ethnic Profiling: A Rising Challenge for European Human Rights Law", *Modern Law Review*, Vol. 71, No. 3, pp. 358-384.

European Union Agency for Fundamental Rights (FRA) (2010), *Towards more effective policing: Understanding and preventing discriminatory ethnic profiling, a guide*, FRA, Vienna, p. 8.

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

Office of the High Commissioner of the United Nations for Human Rights (OHCHR) (2007), *Report of the Special Rapporteur on the protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, OHCHR, Geneva, 29 January.

Open Society Justice Initiative (2009), *Ethnic Profiling in the European Union: Pervasive, Ineffective and Discriminatory*, Open Society Foundations, New York, NY, May.

Pap, András (2008), *Ethnicity and Race-based Profiling in CounterTerrorism, Law Enforcement and Border Control*, Study for the Directorate-General of Internal Policies of the LIBE Committee of the European Parliament, November.

Reding, Viviane (2011), "The Review of the EU Data Protection Framework", Speech to the Privacy Platform, SPEECH/11/183, Brussels, 16 March 2011.

## Appendix. Extract from Recommendation CM/Rec(2010)13 of the Committee of Ministers of the Council of Europe, 23 November 2010 – Paragraph 4.1

Where personal data are collected in the context of profiling, the controller should provide the data subjects with the following information:

a. that their data will be used in the context of profiling;

b. the purposes for which the profiling is carried out;

c. the categories of personal data used;

d. the identity of the controller and, if necessary, her or his representative;

e. the existence of appropriate safeguards;

f. all information that is necessary for guaranteeing the fairness of recourse to profiling, such as

- the categories of persons or bodies to whom or to which the personal data may be communicated, and the purposes for doing so;
- the possibility, where appropriate, for the data subjects to refuse or withdraw consent and the consequences of withdrawal;
- the conditions of exercise of the right of access, objection or correction, as well as the right to bring a complaint before the competent authorities;
- the persons from whom or bodies from which the personal data are or will be collected;
- the compulsory or optional nature of the reply to the questions used for personal data collection and the consequences for the data subjects of not replying;
- the duration of storage;
- the envisaged effects of the attribution of the profile to the data subject.

# ABOUT CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

## Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today,
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process, and
- Provide a regular flow of authoritative publications offering policy analysis and recommendations,

## Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts,
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach,
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals.

## Programme Structure

### In-house Research Programmes

Economic and Social Welfare Policies
Financial Institutions and Markets
Energy and Climate Change
EU Foreign, Security and Neighbourhood Policy
Justice and Home Affairs
Politics and Institutions
Regulatory Affairs
Agricultural and Rural Policy

### Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)

### Research Networks organised by CEPS

European Climate Platform (ECP)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)